AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Pavel Kublitskii

Defendant

24-3632-MJ-GOODMAN

Case No. 8:24-mj-02157

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) Pavel Kublitskii

who is accused of an offense or violation based on the following document filed with the court:

❒ Indictment ❒ Superseding Indictment ❒ Information ❒ Superseding Information ☑ Complaint

❒ Probation Violation Petition ❒ Supervised Release Violation Petition ❒ Violation Notice ❒ Order of the Court

This offense is briefly described as follows:

Conspiracy, in violation of 18 U.S.C. § 371, to traffic in unauthorized access devices, in violation of 1029(a)(2), and to possess 15 or more unauthorized access devices, in violation of 1029(a)(3)

Date: 07/22/2024

Issuing officer's signature

City and state: Tampa, FL

The Honorable Amanda A. Sansone, U.S.M.J.
Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Pavel Kublitskii and
Alexandr Khodyrev

Defendant(s)

Case No. 8:24-mj-02157

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 29, 2017-present in the county of Hillsborough in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 371, 1029(a)(2)	Conspiracy to traffic in unauthorized access devices
18 U.S.C. §§ 371, 1029(a)(3)	Conspiracy to possess 15 or more unauthorized access devices

This criminal complaint is based on these facts:

See Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Greg Christopher, Special Agent, FBI
Printed name and title

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

Date: July 22, 2024

Judge's signature

City and state: Tampa, FL

HONORABLE AMANDA A. SANSONE, U.S.M.J.
Printed name and title

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR COMPLAINT

I, Gregory T. Christopher, being duly sworn, depose and state the following:

1. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed in this capacity since March of 2006. Prior to becoming a Special Agent, I served as an officer in the United States Marine Corps for approximately six years. During my time in the United States Marine Corps, I served as a platoon commander and participated in combat operations in Operation Enduring Freedom. I am currently assigned to the FBI Tampa field office in Tampa, Florida.

2. In my capacity as a Special Agent with the FBI, I have conducted a variety of national security and criminal investigations. I have investigated many different federal crimes, including those involving national security, computer intrusions, intellectual property rights, mail and wire fraud, and money laundering. In addition, I have drafted dozens of search warrants that resulted in valuable evidence collection and millions of dollars in seized assets. I am also in regular contact with law enforcement personnel who specialize in the area of cybercrime and criminal enterprises.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute search and arrest warrants issued under the authority of the United States.

4. I make this affidavit in support of an application for a criminal complaint charging Pavel Kublitskii ("**KUBLITSKII**") and Alexandr Khodyrev ("**KHODYREV**") with conspiring, in violation of 18 U.S.C. § 371, to violate 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices) (collectively, the "Target Offenses"), as well as associated arrest warrants.

5. Because this affidavit is provided for the limited purpose of establishing probable cause for the requested complaint and arrest warrants, I have not included all aspects of the investigation, but rather only information sufficient to establish such probable cause.

KEY TERMS DEFINED

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

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

8. *Blockchain*: The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

9. *Virtual Currency Exchange ("VCE")*: VCEs are trading and/or storage platforms for virtual currencies, such as Bitcoin. Many VCEs also store their customers' virtual currency in virtual currency wallets. These wallets can hold multiple virtual currency addresses associated with a user on a VCE's network.

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

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

11. *Distributed Denial-of-Service ("DDoS")*: DDoS attacks are malicious efforts to disrupt normal server or network activity by overwhelming the infrastructure with a flood of internet traffic.

12. *Dark net/dark web* is the hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity.

13. *Surface web/ clear web* is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines.

14. *Carding* is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards. Card forums are online shopping venues for stolen

credit and debit card information and criminal techniques. Carding is a third-party attack on an individual's financial information.

15. A *cookie* is information that a website puts on a user's computer to store limited information from a web browser session on a given website that can then be retrieved in the future. Common use cases for cookies include session management, personalization and tracking.

PROBABLE CAUSE TO BELIEVE THAT KUBLITSKII AND KHODYREV COMMITTED THE TARGET OFFENSES

Background

16. WWH Club ("WWH") is an internet message board and online marketplace—like a cross between Ebay and Reddit—that exists for the sole purpose of promoting and facilitating crime.

17. WWH is known for including members who specialize in different facets of the criminal underground and use the WWH platform to work together towards a common goal of generating ill-gotten gains. WWH members use the platform as a marketplace (like Ebay) where they communicate privately to buy, sell, and trade goods and services that are typical tools of the trade for cybercrime, including login credentials (usernames and passwords), personal identifying information ("PII") (dates of birth, addresses, Social Security numbers, etc.), malware, fake identification documents, bank account credentials, and PayPal credentials. In addition to WWH's marketplace function, WWH members use the forum features of the site (like Reddit) to promote themselves and the illegal goods

and services they can provide, as illustrated further below. Finally, WWH also provides online courses to train members on how to commit various crimes. In other words, WWH members conspire with, aid and abet, and train one and other in the commission of cybercrimes, including, but not limited to, wire fraud, access device fraud, identity theft, and other criminal offenses.

18. As described further below, there is probable cause to believe that **KUBLITSKII** and **KHODYREV** are two of the administrators of WWH, which means they help operate and manage the site/platform.

Obtaining and Examining the WWH Club Server

19. In or around July 2020, FBI agents determined that WWH's main domain, *wwh-club.ws*, resolved to IP addresses ultimately belonging to DigitalOcean, a United States cloud computing/web hosting company.

20. Pursuant to a federal search warrant, DigitalOcean provided investigators with a copy of the server used to run WWH. The data from DigitalOcean provided a wealth of information regarding the nature and extent of posts on WWH, as well as the transactions conducted via the site. The information from DigitalOcean made clear that the sole purpose and intent of WWH was to promote and facilitate criminal activity.

21. Using the server image provided by DigitalOcean, FBI computer scientists configured the data to enable investigators to view a copy of the forum as one with administrator access would have viewed it (the reconstructed server will hereinafter be referred to as the "Marketplace"). The entire WWH site is in Russian,

so investigators used the Google Translate function of Google Chrome to view and read the site.[1]

Examination of the Backend Database

22. Using the data provided by DigitalOcean, FBI computer scientists also reconstructed the site's SQL[2] databases and other stored information regarding the the Marketplace. That data—referred hereinafter as the "backend database"—was aggregated into a single searchable dataset. This dataset includes:

a. Email addresses registered to user accounts;

b. Registration dates for user accounts;

c. Secret word and password associated with accounts;

d. Privilege level of user (admin/moderator/staff/none); and

e. User activity, such as posts and messages.

23. Based on information obtained from the backend database, it appeared the Marketplace had nearly 170,000 registered users as of July 2020. Of the approximately 170,000 accounts, approximately 29 were assigned "moderator" privileges; 32 were assigned "staff" privileges; and 7 were assigned "admin" privileges. Based on the facts below, there is probable cause to believe that **KUBLITSKII** and **KHODYREV** are two of those administrators, and that

[1] Quotations included in this affidavit from the Marketplace and the current WWH Club forum are written in English as translated from the original Russian by Google Translate.

[2] A structured query language ("SQL") is a tool for connecting to many database systems that store data in tables organized into rows and columns. It is often used on the backend of business websites to provide access to user data.

KUBLITSKII also acted as a moderator.

24. From my training and/or experience, and my investigation to date, administrators (those with "admin" privileges) are the owners and creators of the site who determine the Marketplace's rules and regulations. The administrators also oversee the construction and maintenance of site infrastructure that is required to operate the Marketplace. Meanwhile, moderators oversee posts and chats on the forum to ensure that users adhere to the "chatting rules."

25. Based on rules displayed on the Marketplace, all discussions and transactions conducted on the site would be reviewed by moderators, staff, and administrators to ensure compliance. Users who disregard the rules are assigned a number of points for each infraction; users who accumulate too many points are banned from the site. The forum rules include topics such as Marketplace fees, chatting guidelines, advertising requirements, arbitration, and various communication restrictions.

26. In addition, the Marketplace rules forbid site users from conducting any work (*i.e.* crime) in Commonwealth of Independent States countries, which includes countries such as Russia (the home nation of **KUBLITSKII**), Kazakhstan (the home nation of **KHODYREV**), Armenia, Belarus, and Ukraine.

Criminal Activity Advertised, Facilitated, and Conducted on WWH

27. In March 2016, the owner of WWH posted a message to all members on the site that described "How wwh-club works":

> [WWH-Club was designed with] server protection with FastFlux technology . . . Fast-Flux networks are networks of compromised computer systems with public DNS records that are constantly changing, in some cases every 3 minutes. The ever-changing architecture makes it much more difficult to track and shut down criminal activity . . . Since January 2016, we have launched the decentralized work of WWH-CLUB . . . Over many years of work, a list of 13 people has been formed who will guarantee the operation of the project in any emergency . . . Guys from 7 countries . . . Instructions for restoring the project were developed (from the technical plan to notifying each participant), instructions for the development of the project (for three years with a full description of the actions), instructions for working with partner forums (8 forums with which we have operational communication) . . . Alert system, from the fall of the server, domains, to the loss of communication with any of the 13. (the system works on the basis of entering a special password once every three days).

Based on the referenced post, as well as my training and/or experience, I understand that the forum's server architecture was designed to operate off compromised computer systems to make it more difficult to shut down criminal activity. Furthermore, coconspirators from seven countries implemented a plan to keep the site operational in the event law enforcement attempted to disrupt and dismantle the ongoing criminal activity. Thus, it is clear to me that the owners and administrators of the forum were aware they were involved in criminal activity, and they took active steps to mitigate risk.

28. As of July 2020 (*i.e.* the date of the most recent capture of the WWH server, via the image provided by DigitalOcean), WWH was available on one darknet domain (*wwh-club.ws*) and four surface web domains. The sites are mirrors of each other, in that each URL leads users to replica sites that appear to be identical to

all of the other sites. Mirror sites are exact copies of a website that are placed at different URLs or domains. Mirror sites can be used for innocuous reasons, like reducing server traffic. Criminals also may use mirror sites to facilitate uninterrupted access to a particular site in the event that one of the site's domains is shut down.

29. After accessing WWH (whether through the surface web or darknet), the first thing a user sees is the homepage, which contains flashing banners advertising various criminal services and other darknet marketplaces. Each image contains a link to the associated post (or "thread"), which contains details about the advertised goods or services.

30. For example, some of the messages posted on or about July 31, 2020, the date of the most recent capture of the WWH server, included:

a. "Ddos attack on server sites!!! we will help to get rid of competitors !!!";

b. "Where to start carding?";

c. "We buy debit cards!!! We are looking for drop drivers!"; and

d. "Who can withdraw BOA[3] from the account."

31. Based on my training and/or experience, and my investigation to date, these messages were related to criminal activity, including DDoS attacks, credit and debit card fraud, and bank account takeovers. Based on my training and experience,

[3] Based on my training, experience, and knowledge of this investigation, I believe "BOA" to be a reference to Bank of America.

and my investigation to date in this case, I know that stolen PII is often used to commit a variety of crimes, including U.S. tax fraud, credit card fraud, unemployment insurance fraud, bank fraud, and stolen identity refund fraud.

32. The Marketplace also advertised that WWH offered its users training in how to commit credit card fraud via a banner that stated, "Quick start in shady business! Best carding training from WWH-CLUB." The banner advertisement linked to a page on the WWH site containing information pertaining to the Marketplace training material, which is discussed further below.[4]

33. Other similar advertisements on the Marketplace appeared to offer other criminal services, such as fraudulent ID printing or SMS- and phone-flooding services. From my knowledge and experience, I know that SMS- and phone-flooding is used by criminals as a means of blocking a victim's phone use by repeatedly sending a large volume of calls or texts to the phone. This DDoS attack is done in conjunction with fraudulent financial transactions so the victims cannot receive phone alerts from their financial institutions notifying them of the crimes in progress.

[4] Other advertisements on the site pointed WWH's users towards other avenues for criminal activity. For example, a large banner advertised a darknet marketplace called Joker's Stash. The advertisement stated that Joker's Stash was "The Biggest Darknet Marketplace." It also boasted that Joker's Stash had "Millions of CC+CVV, Dumps, SSN+DOB" and "Every Day Updates." From my knowledge and experience, I know that Joker's Stash was another large and well-known darknet market, like WWH, that sold stolen credit card information ("CC+CVV") and PII obtained during large-scale computer intrusions. After purchasing the stolen data through Joker's Stash, criminals used the data to conduct fraudulent transactions, just like on WWH.

34. At the top of each Marketplace page, there was a header with links that connected users to additional Marketplace pages. The main page was the "forum," and other pages had titles such as "members," "forum rules," "advertising," "duty," "raising rights," and "WWH.Radio."

35. The forum page included a list of Marketplace users that could be filtered. Each message displayed a title, date, and the user who submitted the message. Numerous messages were posted every day, and a review of message titles revealed that all of the reviewed titles pertained to some form of criminal activity.

36. The forum page included additional links organized by information type. For example, there were sections titled "Our Projects," "All About Carding," "Coding," "Cryptocurrency," "Trading Area," and "Paid Advertising."

37. The links pertaining to "carding" provided information and resources to assist individuals in using stolen credit card information and PII to make purchases and generate revenue. There was also information regarding online security, encryption, system masking, and anti-detection to enable carders to conduct their criminal activity without detection by law enforcement.

38. The "Trading Area" provided links to forum posts organized by topic. Such topics included hacking services, the sale of email databases, access to compromised bank accounts, DDoS services, fraudulent identification and document services, and numerous topics pertaining to carding.

39. In the "Our Projects" section, there were a number of links to Marketplace resources and training, such as previous lectures on topics such as carding, hacking, and "survival on the federal wanted list."

40. A link regarding carding brought users to a forum with thousands of posts and approximately two million views. On the forum, users could apply for membership to the Marketplace and apply to participate in trainings. The Marketplace administrator wrote:

> WWH-Club invites you to get a new profession, a new type of earnings, completely different kind of life! Which will not take away all your personal time, will help you reconsider your views on earnings, will show you how you can earn interestingly, intellectually, and amicably, and you will find progressive friends and a team! The basis of the WWH-Club project is: commodity carding is the purchase of goods in online stores at the expense of various means of payment of residents of the USA/EUROPE/ASIA/ with its subsequent implementation and profit. You will learn how to relax for free in the resorts of Europe, America or Asia.

41. The advertised cost of the Marketplace course was 60,000 rubles (approximately $775 U.S. dollars), with an additional $200 necessary for training materials. Answers to "popular questions" included:

a. "The work is completely anonymous;"

b. "Normal hours for carding: 10-12 hours a week to earn from $3,000/month. You can work on weekends;" and

c. "It is possible to build a work on any type of product. Clothing, electronics, digital goods and so on."

42. The first post on the training forum occurred in or around February 2014. Between the first post and in or around July 2020, there were approximately

7,700 individual posts combined from Marketplace administrators (who facilitated training) and individual users (who attended classes). Some of the student posts included a review of the training received, and others provided information and pictures regarding the students' personal success in using the training to commit fraud.

43. Also available on the Marketplace was a combined transcription of multiple lectures titled, "Public training manual V 3.0 WWH-CLUB 2019." The transcription was approximately 300 pages long and covered a number of instructional topics pertaining to fraud. For example, there were transcriptions of lectures on encryption and improving internet security to avoid detection by law enforcement and evade antifraud systems. There were also lectures on the best methods to conduct carding, such as which type of stolen credit card numbers to use, how to adapt to the purchasing habits of the actual cardholder, and how to find shops that are most susceptible to carding. For those who successfully purchased items with stolen credit card data, the training manual provided instruction on using re-shipping services to obtain the items or use other methods to immediately monetize the products.

44. To generate revenue, the Marketplace charged various fees to members who made posts regarding certain topics on the forum and/or who wished to participate in a training. The site provided a lengthy list of specific fees for approximately 35 "commercial topic[s]." The list included topics such as the sale of credit card information, PII, compromised bank accounts and debit cards; the sale of

services such as DDoS and hacking; and the sale of software and equipment such as credit card skimmers, scripts, and brute force programs. The fees appeared to range from approximately 10,000 rubles to 60,000 rubles (approximately $130 to $780).

45. To assure members that posting on the Marketplace forum was worth the mandatory fees, one of the site administrators (username: "*Reklama*," which is the Russian word for advertising) listed a summary of statistics regarding Marketplace traffic. As of 2020, the *Reklama* administrator stated:

> WWH-CLUB is the leader in terms of the number of active users of the shadow Internet. Over the last 5 years of the forum's existence, the average annual growth rate of active users is 60%. Setting up your business on our site means the stable growth of your project and confidence in its further growth. WWH-CLUB knows 80% of active users of the shadow Internet . . . The number of users on WWH-CLUB is 120,000 people, active in 72 hours – 39,000 people.

An administrator subsequently updated the 2020 post to indicate that the total number of members was 160,000 at that time, which aligns with the data FBI computer scientists found on the backend database (*see* paragraph 23). On March 26, 2023, the *Reklama* administrator posted that the forum had grown to 353,000 users, with 112,000 active users in a 72-hour period.

46. The *Reklama* administrator also advertised on WWH that the owners and administrators of WWH own additional criminal forums as well: Skynetzone, Opencard, and Center-Club. This was confirmed by a review of messages from the reconstructed Marketplace. For example, upon receipt of payment, one of the administrators told a user, "Done, the link from you was only required for approval.

Above, I wrote you full instructions on the topics. You can also stay on the sites wwh-club.net center-club.pw opencard.pw skynetzone.org." A review of the additional sites revealed they appear similar to WWH in layout and content, and the administrator usernames are the same across sites.

47. On or about July 19, 2024, an FBI agent logged on to WWH and confirmed that WWH still generally looks and operates as described above. In other words, it continues to function as a forum and marketplace for criminal activity related to the Target Offenses.

Undercover Purchases of Training and PII on WWH Club

48. In January 2023, an FBI online covert employee ("OCE-1"), who was physically located in the Middle District of Florida at the time, registered for an account on WWH using an undercover identity. OCE-1 subsequently paid approximately $1,000 in bitcoin to attend the WWH training described in paragraph 43. The training was conducted through a chat function on the forum to a class of approximately 50 students; the various instructors provided training in text format rather than audible instruction. The lectures were consistent with the aforementioned topics described in the WWH training manual, and it was apparent the purpose of the training was to educate individuals on how to obtain and use stolen credit card data and PII to generate fraudulent proceeds.

49. On multiple occasions during training, the instructors promoted various tools and services advertised on WWH that would assist users in conducting criminal activity. After approximately six weeks of lectures, OCE-1 completed the training

and was provided several promotional products by WWH that would assist students in their criminal endeavors.

50. In February 2023, while browsing WWH Club forums, OCE-1 observed an advertisement in the "hot threads" forum category on WWH wherein a user was selling stolen PII of United States persons and businesses. Buyers could choose how many people's PII they wished to buy and specify the particular U.S. state of residence, gender, age, and credit score of their desired victims. OCE-1 contacted the seller and arranged to purchase PII belonging to 20 victims located in Florida in exchange for $110, paid in Bitcoin. The WWH seller sent OCE-1 a folder containing 20 files, each of which contained the name, date of birth, Social Security number, state of residency, address, credit score, credit report, and account information from LendingTree.com for a United States person. All 20 of the victims had addresses in Florida, 13 of the victims had addresses in the Middle District of Florida ("MDFL"), and 7 of the victims had addresses in Hillsborough County.

51. I know, based on my training and experience, that the presence of account information from LendingTree.com suggests that this stolen PII derived from a February 2022 breach of LendingTree that compromised the data of over 200,000 customers.

Identification of WWH Administrators, Including *Makein* (*i.e.* KUBLITSKII and KHODYREV)

52. While it appears that WWH had over 350,000 users in March 2023, this investigation has largely focused on identifying the owner of WWH and those

individuals involved in the administration, management, and operation of the site.

53. The backend database, described above, lists certain users as administrators, staff, or moderators.

54. To date, investigators have determined that the owner and creator of the forum has two usernames with administrative functions: "*W.W.H.*" and "*Mans77.*" In addition to the forum owner and creator, it appears there are several other top administrators who operate the site and receive a portion of the generated revenue. One of those top administrators operates under the username "*Makein*." For the reasons described below, there is probable cause to believe that **KUBLITSKII** ***and*** **KHODYREV** both serve as administrators of WWH and share the *Makein* username.

55. On April 29, 2021, a United States Magistrate Judge sitting in the MDFL authorized four federal search warrants covering approximately 70 email accounts associated to administrators and staff who worked together to facilitate WWH. *See* 6:21-mj-1332 (TBS); 6:21-mj-1333 (TBS); 6:21-mj-1334 (TBS); 6:21-mj-1335 (TBS). Based on the information gathered from those warrants, on July 25, 2023, a different United States Magistrate Judge sitting in the MDFL authorized four follow-up federal search warrants covering 25 more email accounts associated with the main WWH Club administrators. *See* 8:23-mj-18 (SPF); 8:23-mj-19 (SPF); 8:23-mj-20 (SPF); 8:23-mj-21 (SPF).

56. As described below, the data returned from these search warrants revealed that many of these email accounts are linked to each other and used by **KUBLITSKII** and/or **KHODYREV** to administer WWH Club, as well as for other purposes, including personal ones.

57. WWH Club generates revenue by charging users for training, membership, and advertisement on the site. Most payments are made through Bitcoin, and site administrators often send users Bitcoin addresses to which payment should be made. Payment and blockchain records tied several e-mail addresses to *Makein*, and by extension **KUBLITSKII** and/or **KHODYREV**.

58. Based on backend data collected by law enforcement pertaining to Skynetzone, a sister marketplace to WWH Club maintained by the same administrators (per their own posts on WWH Club), *Makein* is the owner and primary administrator of Skynetzone. Investigators thus believe that same person(s) control(s) the *Makein* account on WWH Club and the *Makein* account on Skynetzone.

59. Based on a review of seized backend data pertaining to Skynetzone, in or around May 2019, *Makein* (on Skynetzone) sent a message advising a Skynetzone asking the user to send payment for an advertisement to a Bitcoin address ending in -qN2Z9. Blockchain analysis revealed -qN2Z9, as well as other Bitcoin addresses provided by *Makein* on Skynetzone, were clustered with over 100 Bitcoin addresses ("CLUSTER-2"). Between in or around July 10, 2015, and June 22, 2024,

CLUSTER-2 received nearly 4,000 individual deposits totaling approximately 152 Bitcoin, or approximately $961,000.

60. Meanwhile, between December 2, 2015, and September 7, 2022, CLUSTER-2 sent approximately 193 payments to various merchants through accounts at Bitpay, a company that provides online Bitcoin payment processing services. Bitpay records revealed at least 90 of the referenced payments were associated to five email addresses: superbuyer777@gmail.com, k.ostyanasonov.777@gmail.com, russellgoodwinmail@gmail.com, kelemenmitchell@gmail.com, and sadiehearnogr@aol.com. Records from Google revealed superbuyer777@gmail.com, k.ostyanasonov.777@gmail.com, russellgoodwinmail@gmail.com, and kelemenmitchell@gmail.com were connected by cookie; and sadiehearnogr@aol.com was registered as the recovery email for superbuyer777@gmail.com. Based on the common activity within CLUSTER-2 and the association of these five e-mail accounts, I believe that the same person controls all five accounts. For the reasons described below, each of those five e-mail addresses is linked to **KUBLITSKII**, and thus I believe **KUBLITSKII** controls all five accounts and therefore at least shares control of the *Makein* username on WWH Club and Skynetzone.

61. As described further below, two other e-mail addresses (Dducati@inbox.ru and Dducati777@inbox.ru) that are associated with **KHODYREV** were linked to different WWH-related payments made to *Makein* through a separate cluster of Bitcoin transactions.

62. Thus, there is probable cause to believe that both **KUBLITSKII** and **KHODYREV** received payments directed to *Makein* and therefore that both **KUBLITSKII** and **KHODYREV** control the *Makein* username and act as WWH and Skynetzone administrators.

KUBLITSKII E-mails Associated with Makein

a. superbuyer777@gmail.com

63. One of the e-mail accounts tied to WWH administrators and searched pursuant to the warrants discussed in paragraph 54 was 2013KPV@gmail.com. It appears that **KUBLITSKII** controls both 2013KPV@gmail.com and superbuyer777@gmail.com; at minimum, KUBLITSKII used 2013KPV@gmail.com to have conspiratorial contact with superbuyer777@gmail.com.

64. Google records for 2013KPV@gmail.com contained the account user's personal photographs, travel and identification documents, and online purchases sent. Those records revealed that the 2013KPV@gmail.com account is owned by **KUBLITSKII**.

65. The 2013KPV@gmail.com account contained multiple messages between 2013KPV@gmail.com and superbuyer777@gmail.com; some of the messages pertained to a vacation taken by **KUBLITSKII**; for example, in or around March 2018, superbuyer777@gmail.com forwarded 2013KPV@gmail.com an email string wherein superbuyer777@gmail.com was used to book a dolphin excursion in Punta Cana for **KUBLITSKII** and his family. Following the date of the excursion,

2013KPV@gmail.com received photos of **KUBLITSKII** and his family enjoying the excursion.

66. But some of the e-mails between 2013KPV@gmail.com and superbuyer777@gmail.com pertained to fraudulent activity. For example, in or around March 2017, superbuyer777@gmail.com forwarded to 2013KPV@gmail.com an apparent fraudulent contract to purchase Copper Isotopic Atomic Fractions using what appeared to be stolen PII and credit card information. Additionally, in or around May 2020, superbuyer777@gmail.com sent 2013KPV@gmail.com an access request to a Google spreadsheet.

67. Furthermore, based on backend data collected by law enforcement pertaining to Skynetzone, a sister marketplace to WWH Club maintained by the same administrators (per their own posts on WWH Club), *Makein* is the owner and primary administrator of Skynetzone, and a PayPal account registered to superbuyer777@gmail.com was listed within the administrator payment profile table for Skynetzone. Thus, it appears from a review of 2013KPV@gmail.com that, at minimum, **KUBLITSKII** had conspiratorial contact with superbuyer777@gmail.com, and at maximum it appears that superbuyer777@gmail.com is just another alias for **KUBLITSKII**.

68. Additionally, header records pertaining to superbuyer777@gmail.com revealed contact between superbuyer777@gmail.com and businesses with domains such as Crowncloud.net, FirstSSL.ru, Qiwi.com, Darkstore.biz, and Proxy-seller.ru. All of these domains are associated with businesses that provide services such as web

hosting, SSL certificates, online payments, compromised digital accounts, and proxies, all of which are services often used by cybercriminals to conduct their criminal activity, which suggests that the user of superbuyer777@gmail.com was also engaged in the operation and maintenance of websites, such as WWH Club.

b. k.ostyanasonov.777@gmail.com

69. Further review of 2013KPV@gmail.com revealed that k.ostyanasonov.777@gmail.com appears to be another alias/e-mail account used by **KUBLITSKII**. Indeed, **KUBLITSKII** used k.ostyanasonov.777@gmail.com to purchase software that enabled file transfers between iOS and Android phones. **KUBLITSKII** forwarded the purchase confirmation email from k.ostyanasonov.777@gmail.com to 2013KPV@gmail.com. Subsequently, **KUBLITSKII** used 2013KPV@gmail.com to communicate with the software provider to troubleshoot file transfers between his devices.

70. Header records pertaining to k.ostyanasonov.777@gmail.com revealed contact between k.ostyanasonov.777@gmail.com and businesses with domains such as Buycheaprdp.com, Voiptopup.com, Coinbase.com, and Firstdedic.ru. All of these domains are associated with businesses that provide services such as Remote Desktop Protocol, Voice Over IP, virtual currency exchange, and server hosting, all of which are services used to maintain websites and process payments, which suggests that the user of k.ostyanasonov.777@gmail.com was also engaged in the operation of websites, such as WWH Club.

c. russellgoodwinmail@gmail.com

71. As stated above, russellgoodwinmail@gmail.com was connected by cookie to superbuyer777@gmail.com, k.ostyanasonov.777@gmail.com, and kelemenmitchell@gmail.com, and all four email addresses were associated to Bitpay transactions through which payments were made from *Makein's* CLUSTER-2, which indicates *Makein* controlled all four accounts.

72. Additionally, financial records reveal that russellgoodwinmail@gmail.com made payments to multiple business that provide services used to maintain websites and process payments, which suggests that the user of russellgoodwinmail@gmail.com was also engaged in the operation and maintenance of websites, such as WWH Club. For example, a review of Bitpay transactions revealed payments associated with russellgoodwinmail@gmail.com were made to Dellmont, a VOIP provider. Similarly, header records pertaining to russellgoodwinmail@gmail.com revealed contact between russellgoodwinmail@gmail.com and Twilio.com, Cloudflare.com, Vanillacard.net, and Coinremitter.com. All of these domains are associated with businesses that provide services such as VOIP, reverse proxy protection, and virtual currency payments, all of which are services used to maintain websites and process payments.

d. kelemenmitchell@gmail.com

73. Kelemenmitchell@gmail.com registered superbuyer777@gmail.com as a recovery email address; in addition, kelemenmitchell@gmail.com was connected by cookie to superbuyer777@gmail.com, k.ostyanasonov.777@gmail.com, and

russellgoodwinmail@gmail.com. Based on a review of Bitpay records, kelemenmitchell@gmail.com was associated to Bitpay transactions through which approximately nine payments were made from CLUSTER-2.

74. The payments were made to Dellmont and Domains4Bitcoins, which is a merchant that allows customers to pay for domain registration with virtual currency. Multiple domains associated with WWH Club were registered through Domains4Bitcoins, which suggests that the user of kelemenmitchell@gmail.com was engaged in the operation and maintenance of the WWH Club website.

e. sadiehearnogr@aol.com

75. As stated previously, sadiehearnogr@aol.com was associated to Bitpay transactions through which payments were made from CLUSTER-2. A review of the Bitpay records revealed the payments were made to CrownCloud, a web hosting provider, as well Dellmont a VOIP provider. The administrators of WWH Club made payments through Bitpay to various web hosting providers to lease the servers on which WWH Club is hosted.

76. Furthermore, records from Google revealed sadiehearnogr@aol.com was registered as the recovery email for superbuyer777@gmail.com, suggesting these two accounts are used by the same person (*i.e.* **KUBLITSKII**).

KHODYREV E-mails Associated with Makein

a. Dducati@inbox.ru

77. In May 2020, a WWH user sent a message to *Makein*. In response, *Makein* sent a message with a Bitcoin address ending in -FxeWu. The user subsequently made the required payment and provided the transaction hash as confirmation. Blockchain analysis was conducted on the Bitcoin address provided by *Makein*. The address was clustered with 61 additional Bitcoin addresses ("CLUSTER-1") that received approximately 1.78 bitcoin (as of March 29, 2024, worth approximately $123,664) between in or around October 2019 and February 2021. On or around February 2, 2021, 0.65 bitcoin was sent from CLUSTER-1 to an address ending in -beYrU at Binance, a virtual currency exchange. The subscriber email address for the associated Binance account was Dducati@inbox.ru. The registered user of that Binance account was **KHODYREV**, which indicates that *both* **KUBLITSKII** *and* **KHODYREV** control *Makein*.

78. Additionally, as described above, the 2013KPV@gmail.com account controlled by **KUBLITSKII** contained multiple messages from 2013KPV@gmail.com to Dducati@inbox.ru (an account controlled by **KHODYREV**, as explained below) that contained evidence of an access device fraud conspiracy between **KUBLITSKII** and **KHODYREV**. For example, 2013KPV@gmail.com sent approximately ten messages to Dducati@inbox.ru between August 29, 2017, and December 24, 2017. The messages, nine of which had

attached files, contained stolen PII, bank account information, identification documents (such as scanned passports), bank server IPs, bank logon domains and server IDs, and apparent fraudulent contract documents. In total, the ten referenced messages contained more than 15 "unauthorized access devices," as that term is used in 18 U.S.C. § 1029(a)(3) and defined in 18 U.S.C. § 1029(e)(1), (3).

79. Meanwhile, Apple iCloud records for Dducati@inbox.ru revealed that the account was registered with a fictitious name, a common practice used by criminals to attempt to shield themselves from investigation and prosecution. The Apple records showed that the registered user for Dducati@inbox.ru was Максим Давидов (English: Maxim Davidov) with residence address 12467 Aviles Circle, Palm Beach Gardens, Florida. A review of law enforcement databases revealed there was no association between the referenced Florida residence and an individual named Максим Давидов (English: Maxim Davidov). The verified phone number registered with Apple was 77081989940, however, which is the same phone number registered to **KHODYREV's** Binance account.

80. Moreover, a review of IP logs associated with the Dducati@inbox.ru account revealed numerous IP commonalities between the Dducati@inbox.ru account and **KHODYREV's** Binance account. For example, approximately 13 different IP addresses were used to access both the Dducati@inbox.ru account and **KHODYREV's** Binance account, often on similar dates and times. (IP commonality between multiple accounts, particularly when the activity occurs at similar dates and

times, often indicates the accounts are used by the same individual or group of individuals.) In addition, there were also numerous IP commonalities between the Dducati@inbox.ru account and *Makein's* login activity on WWH Club, Skynetzone, and Center-Club, often on similar dates and times, further illustrating that *both* **KUBLITSKII** and **KHODYREV** were using the *Makein* username on WWH Club.

b. Dducati777@inbox.ru

81. In or around September 2018, in an effort to promote Skynetzone, *Makein* posted on WWH Club that Skynetzone was hosting a drawing through which a user could win a game console. *Makein* provided a bitcoin address ending in - 2AJTn to which participants were to send payment. Blockchain analysis revealed on or around September 3, 2019, - 2AJTn sent approximately 0.001 bitcoin to pay VOIP provider, Dellmont, through Bitpay. Records from Bitpay revealed the transaction was connected to Dducati777@inbox.ru.

82. Records from Apple revealed Dducati777@inbox.ru was registered to an iCloud account. The subscriber name and address registered on that iCloud account had similarities with information *Makein* had posted on WWH Club. For example, *Makein* stated in messages to WWH Club users that his Telegram handle was @maximov777; meanwhile, the Dducati777@inbox.ru iCloud account was registered to Alexandr Maximov. *Makein* also posted on WWH Club that his username (originally spelled "Maken") was in reference to the neighborhood where he grew up in Karaganda, Kazakhstan; similarly, the Dducati777@inbox.ru iCloud

account was registered to a residence address in Karaganda, Kazakhstan, and **KHODYREV** is a citizen of Kazakhstan (whereas **KUBLITSKII** is Russian). Furthermore, the verified phone number with Apple for the Dducati777@inbox.ru iCloud account was 77081989940, which is the same phone number registered to **KHODYREV's** Binance account and the Dducati@inbox.ru iCloud account.

83. Investigators compared the IP addresses used to login to several of the accounts above. That comparison revealed, for example, that between January 21 and January 28, 2020, and again between April 10, 2020, and May 28, 2020, the same IP address was used to login to both of **KHODYREV's** Apple iCloud accounts (dducati@inbox.ru and dducati777@inbox.ru) as well as the *Makein* username/identity on both WWH Club. This IP address overlap further supports the inference that **KHODYREV** shares access to the *Makein* username to serve as a WWH Club administrator.

Other E-mails Used by KUBLITSKII to Moderate WWH Club

84. **KUBLITSKII** appears to have used two other e-mails to moderate WWH under the username "*AngelBatista*": tirrrion@gmail.com and 2013KPV@gmail.com.

85. The FBI's review of the backend data for WWH Club revealed that a user with profile name *AngelBatista* was one of the primary moderators on the site. The backend data contained more than 430 of *AngelBatista's* posts, which confirmed that he was assigned moderator privileges on the site. For example, he had authority

to lock topic threads for violating the rules, and he also instructed users when payment was required for certain topics. The registered e-mail address on WWH Club for *AngelBatista* was tirrrion@gmail.com.

86. Agents obtained records from Google pertaining to tirrrion@gmail.com, which revealed numerous emails from admin@wwh to tirrrion@gmail.com containing message threads between site administrators and moderators. There were also emails from noreply@skynetzone containing moderator messages from the WWH Club sister forum Skynetzone, where *AngelBatista* was assigned moderator privileges as well.

87. Google records revealed that tirrrion@gmail.com was connected by cookie to 2013KPV@gmail.com, and those two accounts, tirrrion@gmail.com and 2013KPV@gmail.com, were in frequent contact. The messages between the two accounts often contained stolen PII and credit card information. Some of the emails also contained scanned copies of fraudulent IDs, such as passports.

88. As described above, Google provided the FBI with records associated with 2013KPV@gmail.com pursuant to a federal search warrant, and those records contained the account user's personal photographs, travel and identification documents, and online purchases sent, which revealed that the 2013KPV@gmail.com account is owned by **KUBLITSKII**. Upon identification of **KUBLITSKII**, investigators also located personal photographs of **KUBLITSKII** and his girlfriend within the contents of tirrrion@gmail.com as well.

89. The Google records for 2013KPV@gmail.com contained numerous emails that confirmed the user of 2013KPV@gmail.com was associated with WWH Club username *AngelBatista*, the same moniker associated with tirrrion@gmail.com. For example, 2013KPV@gmail.com was used to register as *AngelBatista* on the sister forum Center-Club, which was owned by the same administrators as WWH Club. 2013KPV@gmail.com also sent a message stating that he could be contacted at angelbatista@jabbim.com. Thus, it appears that both accounts – tirrrion@gmail.com and 2013KPV@gmail.com – were used by **KUBLITSKII** in connection with the alias of *AngelBatista*.

90. Frequently, 2013KPV@gmail.com sent tirrrion@gmail.com messages that contained everything necessary to make purchases with stolen data, such as credit card numbers, the associated U.S. bank, and PII of the account holder. It also appeared the same password was created for each stolen credit account: "Krass1." Furthermore, based on emails from various merchants, it was apparent the stolen information was being used to make purchases online.

91. Further review of the Google records for 2013KPV@gmail.com revealed multiple messages from 2013KPV@gmail.com to Dducati@inbox.ru (*i.e.* **KHODYREV**) that contained stolen PII, bank account information, identification documents, and apparent fraudulent contract documents.

KUBLITSKII and KHODYREV Are Seeking Asylum in the U.S.

92. Based on Department of Homeland Security records, in December 2022, **KUBLITSKII**, a citizen of Russia, and **KHODYREV**, a citizen of Kazakhstan, arrived together in south Florida. To enter the U.S., they claimed asylum and provided DHS with the same residence address in Hollywood, Florida.

93. Upon arrival in Florida, **KUBLITSKII** opened an account at Bank of America with an opening deposit of $50,000 in cash.

94. A review of bank records and social media posts revealed **KUBLITSKII** rented a luxury condominium in Sunny Isles Beach, Florida, and he spends his time visiting the beach and various tourist attractions such as Sea World in Orlando, Florida. Despite an apparent expensive lifestyle, there is no evidence **KUBLITSKII** is or has been employed.

95. Furthermore, subsequent to his arrival in Florida, there is also no evidence that **KHODYREV** is or has been employed. Yet, in or around March 2023, **KHODYREV** purchased a 2023 Corvette at a South Florida dealership with approximately $110,000 cash.

96. Thus, while it does not appear either subject has employment in the U.S., both subjects are using a substantial amount of cash to fund an affluent lifestyle.

97. From my knowledge and experience, and from the evidence collected in this investigation, I believe that both **KUBLITSKII and KHODYREV** are jointly

using the profile of *Makein* to operate as administrators on the criminal forums WWH Club, Skynetzone, and Center-Club. I also believe that through their criminal activity, they are generating substantial profits in virtual currency.

CONCLUSION

98. Based on the foregoing, there is probable cause to believe that **KUBLITSKII** and **KHODYREV** have conspired, in violation of 18 U.S.C. § 371, to violate 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices). I therefore respectfully request that this Court authorize the requested criminal complaint charging **KUBLITSKII** and **KHODYREV** with those crimes and issue corresponding arrest warrants for **KUBLITSKII** and **KHODYREV**.

Respectfully submitted,

Gregory T. Christopher
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate via telephone, consistent with Federal Rules of Criminal Procedure 4.1 and ~~4(d)(3)~~ 4(d), this 22nd day of July 2024.

THE HONORABLE AMANDA A. SANSONE
United States Magistrate Judge