United States District Court

for the
District of Arizona

SEALED

In the Matter of the Seizure of:
(Briefly describe the property to be seized)

Two Domain Names that Are Stored at Premises Controlled by Namecheap.

Case No. 24-9231 MB

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property be seized as being subject to forfeiture to the United States of America. The property is described as follows:

See Attachment A.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 7/11/2024
(not to exceed 14 days)

☐ in daytime - 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to any United States Judge on criminal duty in Arizona.

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be search or seized *(check the appropriate box)*

☒ for 30 days *(not to exceed 30)*. ☐ until the facts justifying, the later specific date of _____

Date and time issued: 6/27/2024@4:02pm

Eswillett
Judge's signature

City and State: Phoenix, AZ

Honorable Eileen S. Willett, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

With respect to the domain names "**MLRTR.COM**" and "**OTANMAIL.COM**" (collectively, the "**Subject Domain Names**"), Namecheap, Inc., (Namecheap), which has its headquarters at 4600 East Washington Street, Suite 305, Phoenix, Arizona, and is the domain registry for the **Subject Domain Names**, shall take the following actions to effectuate the seizure of **Subject Domain Names**:

1) On a date and time specified by the Federal Bureau of Investigation ("FBI") or as soon as practicable thereafter, Namecheap shall take all reasonable measures to redirect the **Subject Domain Names** to substitute servers designated by the FBI by associating the **Subject Domain Names** to the following authoritative name-server(s):
    (a) Hans.ns.cloudflare.com;
    (b) Surina.ns.cloudflare.com; and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Namecheap.
2) Prevent any further modification to, or transfer of, **Subject Domain Names** pending transfer of all right, title, and interest in the **Subject Domain Names** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Subject Domain Names** cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI or the U.S. Department of Justice.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) On a date and time specified by the FBI, the Government will display a notice on the website to which the **Subject Domain Names** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text). The notice may also contain an external hyperlink to a Government controlled site that provides further information on this bot farm.

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(a)(1)(A), 1956(a)(2)(A), and 1956(h) issued by the United States District Court for the District of Arizona as a part of a law enforcement operation and action by: the United States Department of Justice, National Security Division, National Security Cyber Section; the United States Attorney's Office for the District of Arizona; the United States Attorney's Office for the Northern District of Illinois; the Federal Bureau of Investigation; and the National Police of the Netherlands. For additional information, see https://www.justice.gov."

SEALED

United States District Court

for the

District of Arizona

In the Matter of the Seizure of: *(Briefly describe the property to be seized)* Two Domain Names that Are Stored at Premises Controlled by Namecheap.	)	Case No. 24-9231 MB

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe the following property is subject to forfeiture to the United States of America under 21 U.S.C. § 853 and 18 U.S.C. §§ 981 and 982:

See Attachment A.

The application is based on these facts:

See the Attached Affidavit of Federal Bureau of Investigation Special Agent [redacted]

☐ Continued on the attached sheet.

[redacted]
Applicant's signature

Approved by USA Gary M. Restaino

[redacted] Special Agent, FBI
Printed name and title

Sworn to before me and signed telephonically.

Date: 6/27/2024@4:02pm

EsWillett
Judge's signature

City and State: Phoenix, Arizona

Honorable Eileen S. Willett, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

With respect to the domain names "**MLRTR.COM**" and "**OTANMAIL.COM**" (collectively, the "**Subject Domain Names**"), Namecheap, Inc., (Namecheap), which has its headquarters at 4600 East Washington Street, Suite 305, Phoenix, Arizona, and is the domain registry for the **Subject Domain Names**, shall take the following actions to effectuate the seizure of **Subject Domain Names**:

1) On a date and time specified by the Federal Bureau of Investigation ("FBI") or as soon as practicable thereafter, Namecheap shall take all reasonable measures to redirect the **Subject Domain Names** to substitute servers designated by the FBI by associating the **Subject Domain Names** to the following authoritative name-server(s):

    (a) Hans.ns.cloudflare.com;

    (b) Surina.ns.cloudflare.com; and/or

    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Namecheap.

2) Prevent any further modification to, or transfer of, **Subject Domain Names** pending transfer of all right, title, and interest in the **Subject Domain Names** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Subject Domain Names** cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI or the U.S. Department of Justice.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) On a date and time specified by the FBI, the Government will display a notice on the website to which the **Subject Domain Names** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text). The notice may also contain an external hyperlink to a Government controlled site that provides further information on this bot farm.

> "This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(a)(1)(A), 1956(a)(2)(A), and 1956(h) issued by the United States District Court for the District of Arizona as a part of a law enforcement operation and action by: the United States Department of Justice, National Security Division, National Security Cyber Section; the United States Attorney's Office for the District of Arizona; the United States Attorney's Office for the Northern District of Illinois; the Federal Bureau of Investigation; and the National Police of the Netherlands. For additional information, see https://www.justice.gov."

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted], being duly sworn, hereby declare as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since 2022. I was previously employed as an intelligence analyst assigned to the Indianapolis Field Office of the FBI for approximately three years. As a Special Agent, I have conducted national security investigations related to foreign intelligence and cybersecurity. During these investigations, I have gained expertise in law enforcement techniques including the use of physical surveillance, financial examinations of cryptocurrency, witness interviews, and the execution of search warrants. Additionally, I have received training and possess experience relating to Federal criminal procedures, Federal statutes, and computer-related crimes. Presently, I am assigned to a national security cyber and counterintelligence squad within the Chicago Field Office of the FBI.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. As set forth below, there is probable cause to believe that the domain names **mlrtr.com** and **otanmail.com** (the "**Subject Domain Names**") are property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same). In particular, the

investigation to date has revealed that the **Subject Domain Names** have been purchased from an Arizona company and used by individuals abroad who are affiliated with the Russian Federal Security Service (the "FSB") to advance the interests of the FSB and the Russian government, thereby causing U.S. persons and entities to unwittingly provide goods and services to and for the benefit of the FSB, in violation of the International Emergency Economic Powers Act ("IEEPA"). Because the **Subject Domain Names** are property involved in a scheme to violate U.S. money laundering laws, they are subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1)(C).

4. As described below and in Attachment A, the **Subject Domain Names** are registered to an account associated with Namecheap, Inc. ("Namecheap"), a company headquartered in Phoenix, Arizona. The procedure by which the government will seize the **Subject Domain Names** is described below and in Attachment A.

BACKGROUND ON DOMAIN NAMES

5. Based on my training and experience and information learned from others, I am aware of the following:

6. Internet Protocol Address: An Internet protocol ("IP") address ("IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables computers connected to the Internet to

properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

7. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (*e.g.*, letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "google.com" are domain names.

8. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and "www" is the web server. An individual who controls a domain can create email accounts using the second-level domain. For example, an individual controlling the domain name www.example.com can create email accounts using @example.com (*e.g.*, EmailAddress@example.com).

9. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses.

10. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For

example, the company that controls the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which is headquartered in Reston, Virginia.

11. Registrar & Registrant: Domain names may be purchased through a registrar, such as Namecheap, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address to which a particular IP address resolves through an online interface. Registrants typically have to pay the registrar an annual fee to keep the domain name. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services, such as subscriber names, location, and payment methods.

12. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0 - 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

INTERNATIONAL MONEY LAUNDERING AND IEEPA

International Promotional Money Laundering

13. Title 18, United States Code, Section 1956(a)(2)(A) (international promotional money laundering) prohibits, in relevant part, the transportation, transmission, or transfer of funds or monetary instruments from or through a place *outside* the United States to a place *within* the United States, with the intent to promote the carrying on of specified unlawful activity. Pursuant to 18 U.S.C. § 1956(c)(7)(D), specified unlawful activity includes violations of IEEPA, which is codified at 50 U.S.C. § 1705 *et seq.* In addition, any person who "conspires to commit any offense defined in [§ 1956]" shall also be subject to criminal prosecution. *See* 18 U.S.C. § 1956(h).

IEEPA, Executive Orders, and Sanctions Regime

14. IEEPA authorizes the President of the United States to impose economic sanctions in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders with respect to that threat. Acting under IEEPA, the President and the Executive Branch have issued a variety of orders and regulations governing and prohibiting transactions with the government of the Russian Federation by U.S. persons and entities.

15. Pursuant to IEEPA, "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter." 50 U.S.C. § 1705(a). Moreover, anyone "who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an

unlawful act described in subsection (a) shall, upon conviction, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both. 50 U.S.C. § 1705(c).

16. On April 1, 2015, the President issued Executive Order 13694 ("E.O. 13694") finding "that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." E.O. 13694 further declared a national emergency to deal with this threat.

17. E.O. 13694 provides broad authority to the Secretary of the Treasury and the Secretary of State, in consultation with each other and, on occasion, the Attorney General, to designate as the target of blocking sanctions individuals or entities—thereafter, Specially Designated Nationals ("SDNs")—determined to be responsible for or complicit in, or to have engaged in, malicious cyber-enabled activities originating from outside the United States. Pursuant to E.O. 13694, property and interests in property of an SDN located in the United States are blocked and, under Section 3 of E.O. 13694, U.S. persons are prohibited from providing funds, goods, or services to or for the benefit of—or receiving the same from—the SDN, without first obtaining a license or other written authorization from the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC"). Additionally, E.O. 13694 further prohibits any transactions that evade or have the purpose of evading or cause a violation of the prohibitions set forth therein, as well as any conspiracy to violate such prohibitions.

18. On December 28, 2016, the President issued Executive Order 13757 ("E.O. 13757") "to deal with the national emergency with respect to significant malicious cyber-enabled activities declared in Executive Order 13694 . . . and in view of the increasing use of such activities to undermine democratic processes or institutions." In relevant part, E.O. 13757 amended E.O. 13694 to add an Annex to the earlier order and to make clear that all individuals and entities listed in the Annex would be subject to E.O. 13694's prohibitions. Significantly for purposes of this affidavit, the Annex lists the "Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a. FSB); Moscow, Russia." Thus, after December 28, 2016, U.S. persons were prohibited from providing funds, goods, or services to or for the benefit of—or receiving the same from—the FSB.

19. The prohibitions set forth in E.O. 13694 and E.O. 13757 are incorporated into OFAC's Cyber-Related Sanctions Regulations, which took effect on September 6, 2022. Specifically, subject to limited exceptions not otherwise applicable here, the Cyber-Related Sanctions Regulations likewise prohibit any U.S. persons from providing funds, goods, or services to—or receiving the same from—the FSB, without the requisite license or authorization. 31 C.F.R. § 578.201(b). Additionally, the Cyber-Related Sanctions Regulations also prohibit any transaction

that evades or has the purpose of evading or causes a violation of these prohibitions, as well as any conspiracy to violate the prohibitions. 31 C.F.R. § 578.205(a).[1]

20. According to OFAC records, at no time material to this warrant has the FSB—or any of the individuals or entities described below, including those who have worked at its direction—obtained a license or other written authorization to purchase, renew, transfer, use, or export the **Subject Domain Names**.

EVIDENCE ESTABLISHING PROBABLE CAUSE

21. The FBI is investigating an artificial intelligence-enhanced social media bot farm,[2] operated at the direction of the government of the Russian Federation ("Russia"), that creates and uses fictitious social media profiles—often purporting to belong to individuals in the United States—to promote messages in support of Russian government objectives. As described below,

[1] OFAC-issued General License 1, which authorizes U.S. persons to engage in certain limited transactions and activities with the FSB where such transactions are "ordinarily incident and necessary to" the "requesting, receiving, utilizing, paying for, or dealing in licenses, permits, certifications, or notifications issued or registered by the Federal Security Service" in connection with the import of IT products into Russia. *See generally* Cyber General License 1 (April 27, 2023), available at https://ofac.treasury.gov/media/931686/download?inline.

[2] A bot farm is an enhanced software package which allows for the creation of false personas on social media platforms. Bot farms are enhanced by integrating components which contain artificial intelligence, such as image production or text generation.

this social media bot farm was a tool developed ultimately for the benefit and use of the Russian government.[3]

22. As detailed below, individuals associated with the bot farm—who are believed to be based in Russia—have transferred funds internationally to purchase two domain names from a U.S.-based domain name registrar (Namecheap) in order to create private email servers, which have in turn been used to create email addresses that have then been used to register at least 968 fictious social media accounts for the benefit of the FSB and in furtherance of its goals. These cyber actors, however, did not obtain an OFAC license before purchasing or renewing the U.S.-based domain names for use by and for the benefit of the FSB. Because these actors have transferred funds from or through a place outside the United States to a place within the United States, with the intent to promote a specified unlawful activity (here, an IEEPA violation), there is probable cause to believe that they have violated U.S. money laundering laws.

---

[3] I am aware of open-source reporting that links the FSB to prior disinformation efforts on behalf of the Kremlin. The U.S. Department of State, for example, has explained that "disinformation outlets linked to Russia's Federal Security Service," among other Russian agencies, have created pretextual narratives to justify Russia's invasion of Ukraine. *See* "Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War," U.S. DEPARTMENT OF STATE, February 23, 2023, *available at* https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/.

In addition, the U.S. Department of State has sanctioned FSB officers for "repeated attempts to undermine the democratic processes in the United States and other countries." *See* "Targeting Russia's Global Malign Influence Operations and Election Interference Activities," U.S. DEPARTMENT OF STATE, June 23, 2023, *available at* https://www.state.gov/targeting-russias-global-malign-influence-operations-and-election-interference-activities-2/. In my judgment and based on the information set out in this affidavit, I believe the FSB's use of the social media bot farm is simply the continued effort by that agency to spread disinformation on behalf of the highest levels of the Russian government.

A Bot Farm is Created and Used by the Russian Government Influence Apparatuses

23. I have learned about the origins of the social media bot farm from another U.S. government agency ("U.S. agency"), and based on corroborative information developed over the course of my investigation, I find the information about the social media bot farm from this U.S. agency to be credible and reliable. According to information provided by the U.S. agency, development of the social media bot farm was organized by an individual identified in Russia ("Individual A"). In early 2022, Individual A worked as the deputy editor-in-chief at RT, a state-run Russian news organization based in Moscow.[4] Individual A has led the Directorate of Digital Journalism within RT from early 2022 until the present. Prior to 2022, RT leadership sought the development of alternative means for distributing information beyond RT's standard television news broadcasts. Individual A proposed to his leadership the development of software able to create and to operate a social media bot farm. In theory, the social media bot farm would create multiple social media accounts through which RT, or any operator of the bot farm, could distribute information on a wide-scale basis. RT leadership concurred with Individual A's proposal.

24. According to information from the U.S. agency, Individual A oversaw the development of the social media bot farm software through the Directorate of Digital Journalism.

---

[4] I know from open-source reporting that RT was formerly known as "Russia Today." In January 2017, the Office of the Director of National Intelligence released a U.S. Intelligence Community Assessment titled "Assessing Russian Activities and Intentions in Recent US Elections." The assessment described how the Russian government's influence campaign targeting the 2016 U.S. elections was "multifaceted," relying in large part on a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'" With regard to RT specifically, the assessment stated as follows:

At all times relevant to my investigation, another individual identified in Russia ("Individual B"), also worked for the Directorate of Digital Journalism. I learned from the U.S. agency that Individual B was a lead developer of the social media bot farm software.

25. According to information provided to me by the U.S. agency, the development was executed by Individual B, among others, who hid their identities and location (Russia) while beginning to purchase infrastructure for the social media bot farm in April 2022. The social media bot farm software was designed to give Individual A and other Russian government operators, described in more detail below, the ability to generate fictitious online personas on various social media platforms. The users would then be able to use these social media bots to post content and to amplify the messaging of their choosing on social media.

26. According to the U.S. agency, in early 2023, an individual identified in Russia who is an FSB officer ("FSB Officer 1") created the private intelligence organization ("P.I.O.").[5] The creation of the P.I.O. was approved by the Presidential Administration of Russia (a.k.a., "the Kremlin"), and the P.I.O. received financial support from that office. FSB Officer 1 has led the

---

> The rapid expansion of RT's operations and budget and recent candid statements by RT's leadership point to the channel's importance to the Kremlin as a messaging tool and indicate a Kremlin-directed campaign to undermine faith in the US Government and fuel political protest. The Kremlin has committed significant resources to expanding the channel's reach, particularly its social media footprint.

As borne out in my investigation, and based on my training and experience, I believe that the Russian government's use of state-funded media and its weaponization of social media was continuing.

[5] Based on my training and experiences, I understand that a private intelligence organization is a non-government or quasi-non-government organization devoted to the collection, analysis, and exploitation of information derived from various data sources.

P.I.O. from its inception to the present. FSB Officer 1 recruited Individual A, other FSB officers, and other individuals to join the P.I.O. the same month that the P.I.O. was created. At the time of the creation of the P.I.O., Individual A, through Individual B and the Directorate of Digital Journalism, had been developing the social media bot farm software for less than one year.

27. According to the U.S. agency, the true purpose of the P.I.O. was to advance the mission of the FSB and the Russian government. One manner in which the P.I.O. accomplished this mission was by attempting to sow discord in the United States by spreading misinformation through the social media accounts created by the bot farm.

28. According to the U.S. agency, in March 2023, Individual A, utilizing his position at RT, assisted FSB Officer 1 in arranging for the P.I.O. to provide investigative services to RT and to provide cover to the P.I.O.'s true mission. Such investigative services included acting as an analytical unit for RT and connected Russian news affiliates. Unofficially, and concurrent to their employment at RT, employees of the P.I.O. would continue their mission to conduct influence operations against foreign adversaries in coordination with the Kremlin. FSB Officer 1 often worked collaboratively with Individual A and other employees of the P.I.O., though, when necessary, FSB Officer 1 assigned duties to Individual A in order to further the influence operations which served the interests of the FSB and the government of Russia more broadly.

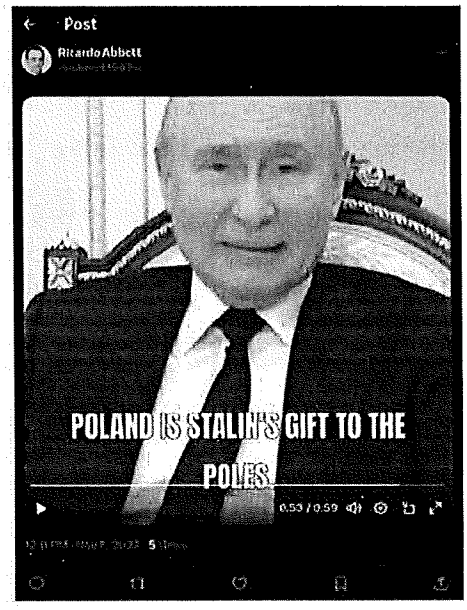
29. According to the U.S. agency, members of the P.I.O. planned to use the social media bot farm software for its intended purpose to covertly spread messages on behalf of the government of Russia. FSB Officer 1, Individual A, and a small number of other individuals within the P.I.O. were designated as authorized operators of the platform.

Bot Farm Targets Social Media Platform X Corp.

30. According to the U.S. agency several accounts hosted on the social media service X Corp. (formerly Twitter) were created by the P.I.O. through the bot farm to further its mission of serving the government of Russia.

31. As part of the investigation, I have reviewed several of the public-facing posts made by these bot accounts on the X Corp. platform. In one such post from October 2023, for example, the bot account replied to a post from the official account of a U.S. candidate for federal office. The bot account purported to be from the district the candidate was campaigning to represent. In response to the candidate's post—which addressed the conflicts in Ukraine and Israel—the bot account posted a video of President Putin justifying Russia's actions in Ukraine.

32. In another post, this time from November 2023, the bot account posted a video of President Putin discussing his belief that certain geographic areas in Poland, Ukraine, and Lithuania were liberated by the Soviet Union from Nazi control during World War II and were therefore "gifts" to those countries from Russia (screen shot depicted below). My review of these and other posts from the bot accounts identified by the U.S. agency, corroborates that the accounts have been used by the P.I.O. to advance the Russian government's narratives and interests.



33. In response to legal process, in April 2024, X Corp. provided subscriber records for the twenty-three identified accounts. These records indicate the accounts were created between June and December 2023, and as of April 2024, twenty of the twenty-three accounts remained active. Notably, nineteen of the twenty active accounts were registered using email addresses hosted by the **Subject Domain Names** (*i.e.*, @mlrtr.com or @otanmail.com), as summarized in the chart below:

Username	Email Address	Creation Date
khagenes198219	khagenes198219@mlrtr.com	2023-06-01
kschmeln88rmi	kschmeln88rmi@mlrtr.com	2023-06-01
rkulas1991vi	rkulas1991vi@mlrtr.com	2023-06-03
gboyer1985yz	gboyer1985yz@mlrtr.com	2023-06-08
nkling19966a	nkling19966a@mlrtr.com	2023-06-08
pmorar19990w	pmorar19990w@mlrtr.com	2023-06-08

Username	Email Address	Creation Date
tblock1999xe	vegodar220@anwarb.com[6]	2023-06-22
rabbott1987ru	rabbott1987ru@mlrtr.com	2023-06-26
kherman1987u4	kherman1987u4@mlrtr.com	2023-06-27
ehagenes1981eu	ehagenes1981eu@mlrtr.com	2023-06-27
cheller19869f	cheller19869f@mlrtr.com	2023-10-16
sgleason1971pi	sgleason1971pi@mlrtr.com	2023-10-17
nmoen1975gb	nmoen1975gb@mlrtr.com	2023-11-02
acruickjgzpvn	acruickjgzpvn@mlrtr.com	2023-11-02
mbraun1984zf	mbraun1984zf@otanmail.com	2023-11-22
jmurphy1989q9	jmurphy1989q9@otanmail.com	2023-11-30
tbraun19681s	tbraun19681s@otanmail.com	2023-11-30
jmckenzrvgj2t	jmckenzrvgj2t@otanmail.com	2023-12-01
knicolas1986k6	knicolas1986k6@otanmail.com	2023-12-01
jstamm1988gr	jstamm1988gr@otanmail.com	2023-12-01

FBI Identifies Subject Domain Names

34. In response to legal process, Namecheap provided records related to the **Subject Domain Names** used to register the nineteen social media accounts described above, **mlrtr.com** and **otanmail.com**.[7] According to these records, the same Namecheap account purchased the **mlrtr.com** domain name on April 21, 2022, and the **otanmail.com** domain name on June 23, 2023.

[6] This email address was the only active social media account not associated with the **Subject Domain Names**. An open-source search showed the account is associated with a disposable email service. Disposable email services enable a person browsing the internet to use a randomly selected email inbox for a very brief period of time (*e.g.*, approximately ten minutes). Disposable email services are attractive to users because they often do not need to create an account or provide other identifying information to the email service provider. After the account expires, the user no longer has access to the account and the information within the account is destroyed.

[7] If an internet user attempts to navigate to **mlrtr.com** from his or her web browser, the server refuses the connection. If an internet user attempts to navigate to **otanmail.com** from his or her web browser, they are presented with a generic gray-colored page that reads, "No Sponsors."

The Namecheap account was registered using the name Milan Blokhin[8] and the email address [Email Address 1]@gmail.com.[9] The user provided a registration phone number with a country code of +370 (associated with Lithuania), and a street address in Druskininkai, Lithuania. Based on a Whois search, the account registration IP address was associated with a Virtual Private Network ("VPN") connection that resolves to Lithuania.

35. Based on my training and experience, I know that a VPN service provider can route internet traffic through servers controlled by the service provider to make it appear that the traffic (specifically, the IP address) is originating from the service provider's server. Users of VPN services can select a VPN "exit node" associated with a location of his or her choosing. By selecting a Lithuanian exit node, for example, I believe the individual who registered the Namecheap account wanted to make it appear that he was connecting to the internet from a Lithuanian IP address to conceal the true location of his originating IP address.[10]

---

[8] Based on my research, the name Milan Blokhin appears to be a fictitious name. I know from training and experience that criminal actors often use aliases and fake personal information to obfuscate their connections to criminal activity. Searches in open-source and FBI databases for "Milan Blokhin" have yielded no relevant results. At this point in the investigation (and as described further below), I believe the name Milan Blokhin is not the true name of the actor who registered the Namecheap account and the **Subject Domain Names**.

[9] This email address, along with the recovery email addresses discussed below, are known to me but have been redacted because the investigation remains ongoing.

[10] In addition to general operational security concerns, I believe the Namecheap account registrant sought to conceal his true location—which, as explained below, I believe is in Russia—because in March 2022, Namecheap publicly announced that the company would no longer sell domains to residents of Russia due to Russia's invasion of Ukraine. *See* "FAQ – Transfer of Russian customers services from Namecheap," https://Namecheap.com/support/knowledgebase/article.aspx/10519/5/faq-transfer-of-russian-customers-services-from-Namecheap/. Thus, I believe the account registrant sought to obfuscate his true location (Russia) because he would not have otherwise been permitted under Namecheap policy to obtain the **Subject Domain Names**.

FBI Links Namecheap Account Registrant to Individual B

36. Because the Namecheap account registrant appears to have used a fictitious name to register the account and **Subject Domain Names**, FBI has conducted additional investigative steps to identify "Milan Blokhin's" true identity.

37. First, FBI obtained records from Google regarding the email address used by the Namecheap account registrant when registering the account, [Email Address 1]@gmail.com. In response to legal process, Google provided records indicating that Email Address 1 was created on April 19, 2022, two days prior to the purchase of the **mlrtr.com** domain name. The user registered the email address using the name Milan Blokhin, the same alias used to register the Namecheap account.[11] Analysis of Google IP records is also noteworthy. That analysis revealed that although two of the same VPN IP addresses accessed both Email Address 1 and the Namecheap account, the user created Email Address 1 from a non-VPN IP address that resolves to a telecommunications provider located in Moscow.[12] In other words, the user's IP address activity suggests that the actor was located in Russia when he registered Email Address 1 with Google, and that he used the same VPN IP address to obfuscate his location when subsequently accessing Email Address 1 and the Namecheap account described above.

---

[11] When registering Email Address 1 with Google, the registrant used the Cyrillic spelling of the name "Milan Blokhin," which has been machine translated for purposes of this warrant. The registrant used Latin characters for "Milan Blokhin" when registering the Namecheap account mentioned above.

[12] FBI has used an open-source research tool, IP Quality Score, to assess whether a given IP address is associated with a VPN server. According to IP Quality Score, the IP address used to register Email Address 1 is not associated with a VPN. Subsequent references in this affidavit to VPN or non-VPN IP addresses are based on FBI's analysis and use of the IP Quality Score research tool.

38. Records from Google further show that when registering Email Address 1, the user listed [Email Address 2]@gmail.com as the sole recovery email address. In response to legal process, Google provided subscriber records for Email Address 2. These records show the account was created on April 13, 2022, under the registration name Cassandra Rivas.[13] Based on my analysis of the IP records provided by Google, the same IP address used to register Email Address 2 (which resolves to a Lithuanian VPN) also registered the Namecheap account discussed above. Based on my training and experience, the use of a common registration IP address suggests that the same actor was behind the keyboard when registering Email Address 2 and the Namecheap account.

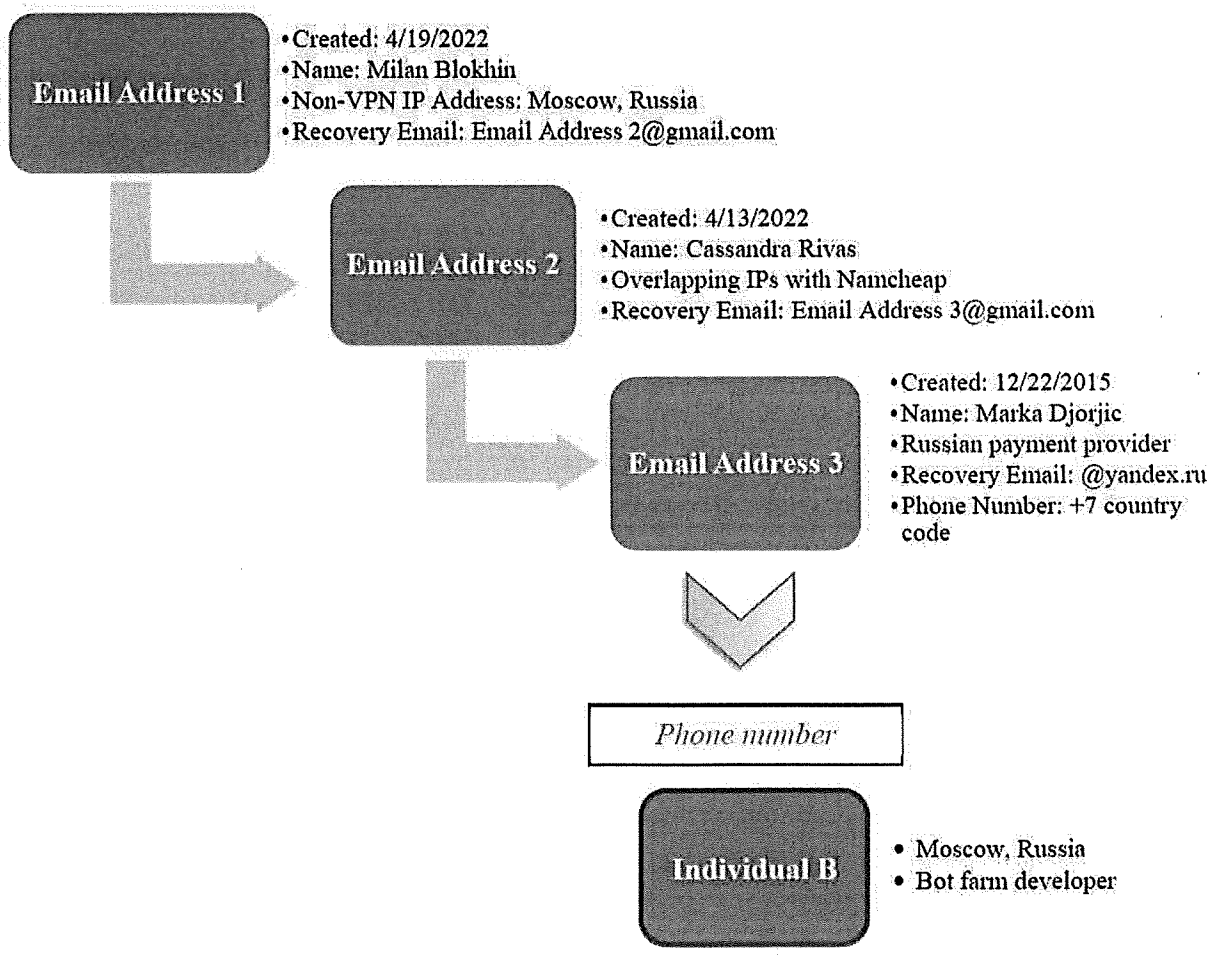
39. Records from Google further show that when registering Email Address 2, the user listed [Email Address 3]@gmail.com as the sole recovery email address. In response to legal process, Google provided subscriber records for Email Address 3. These records show the account was created in December 2015, nearly a decade prior to the creation of the Namecheap account and Email Address 1 and Email Address 2. The actor registered Email Address 3 using the Cyrillic spelling of the name Marka Djorjic (which has been machine translated)[14], and provided a recovery email address ending in @yandex.ru. The user also listed payment information associated with a Qiwi account and listed a Russian tax region. Based on my training and experience, I know Yandex is a Russian email provider and Qiwi is a Russian company that provides payment and

[13] Based on my research, the name Cassandra Rivas also appears to be a fictitious name. Searches in open-source and FBI databases for "Cassandra Rivas" have yielded no relevant results.

[14] Based on my research, the name Marka Djorjic also appears to be a fictitious name. Searches in open-source and FBI databases for "Marka Djorjic" have yielded no relevant results.

financial services. The use of a Yandex email address and a Qiwi payment account when registering Email Address 3 therefore further suggests that the user is located in Russia.

40. Records from Google further show that when registering Email Address 3, the user provided a telephone number with a country code +7, which is the international country code for Russia. After reviewing information obtained via open-source research regarding Russian tax data and mobile subscriber information, I found that this phone number is registered to Individual B mentioned above, a resident of Moscow, who served as a lead developer of the social media bot farm software.



41. Based on my training and experience, I know it is common practice among malicious actors to conceal their true identities online by creating email and other provider accounts using fictious names. Such actors, however, often provide recovery email addresses when registering fictitious accounts to ensure that they can access these fictious accounts in the event they forget the invented details used to set up the account. Some sophisticated actors go a step further, using fictitious recovery email addresses to add a further layer of obfuscation. In this case, for example, the actor linked several fictitious accounts as shown in the graphic above. However, the actor's third linked recovery email address—created nearly a decade prior to the events described in this warrant—contained identifying information (*e.g.*, a Russian telephone number) that linked to the actor's true identity. This series of efforts to obfuscate Individual B's identity evidences an intentional, willful desire to conceal his identity and whereabouts in furtherance of the bot farm scheme.

FBI Identifies International Payments to Namecheap for Subject Domain Names

42. As noted above, records from Namecheap show that the **mlrtr.com** domain name was purchased on April 21, 2022, and the **otanmail.com** domain name was purchased on June 23, 2023. In response to legal process, Namecheap provided payment records indicating that these purchases—and subsequent domain renewals—were made using a U.S.-based payment provider

called BitPay,[15] which allows users to make payments via bitcoin.[16] In response to legal process, BitPay provided investigators with information related to the BitPay user who made purchases to Namecheap in connection with the **Subject Domain Names**.

43. Based on BitPay records, between April 21, 2022, and May 14, 2024, an actor sent five separate bitcoin payments to Namecheap for the benefit of the Namecheap account discussed above. Based on my analysis of these five transactions, I believe these payments originated from outside the United States and were caused by Individual B or those associated with him, as further described below:

a. *April 21, 2022 (Purchase of **mlrtr.com**):* Records from BitPay show that on April 21, 2022, an individual sent 0.000224 BTC from a bitcoin address ending in -uq73 to Namecheap in connection with the purchase of the domain name **mlrtr.com**. Namecheap credited the account with $10 on the same day. The sender used a Lithuanian VPN IP address to view the payment invoice and send

[15] BitPay is a third-party payment service that allows online merchants to accept Bitcoin as payment at the checkout stage. Customers using BitPay do not necessarily have to create their own accounts, so some information, like the customer's name and email address, may be self-reported or not verified, while other information, like IP addresses, are captured by BitPay in the regular course of business.

[16] Bitcoin is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, bitcoin is not managed or distributed by a centralized bank or entity. Because of that, bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running bitcoin's software, called network nodes. These nodes record bitcoin transactions on the bitcoin blockchain.

Bitcoin are sent to and received from bitcoin "addresses," a 26 to 35-character string of letters and numbers that do not contain personally identifiable information about the payor or the payee. Because bitcoin transactions can therefore be used to move funds with a high-level of pseudonymity, cyber actors often use bitcoin or other cryptocurrency to obfuscate illicit financial transactions, conceal the source of funds, and/or launder criminal proceeds.

the bitcoin. The sender provided a Protonmail email address to complete the transaction.

b. *November 7, 2022 (Purchase of expired domain):* Records from BitPay show that on November 7, 2022, an individual sent 0.000715 BTC from bitcoin addresses ending in -5llf and -uqye to Namecheap in connection with the purchase of a now-expired domain name. Namecheap credited the account with $14 on the same day. The sender used a Swedish VPN IP address to view the payment invoice and send the bitcoin. The sender also provided Google Email Address 1 (described above) to complete the transaction, suggesting that the same individual(s) controlling Email Address 1 (and by extension, the other email accounts described above) also executed this payment.

c. *April 26, 2023 (Renewal of **mlrtr.com**)*[17]*:* Records from BitPay show that on April 26, 2023, an individual sent 0.000767 BTC from a bitcoin address ending in -6fu9 and the same bitcoin address used for the November 2022 transaction (ending in -uqye) to Namecheap in connection with the annual renewal of the domain name **mlrtr.com**. Namecheap credited the account with $20 on the same day. The sender used a Dutch VPN IP address to view the payment

[17] Based on my training and experience, I expect these renewals to continue on an annual basis. As explained throughout this affidavit, the cyber actors have developed a sophisticated tool that depends on the existence of the **Subject Domain Names** to operate. I therefore expect these actors to continue renewing the **Subject Domain Names**—and to continue committing acts of money laundering—as long as their tool is in existence.

invoice and send the bitcoin. A second non-VPN address—which resolves to a Moscow telephone network—also viewed the invoice. Notably, in October 2023, the same Dutch VPN IP address that made the payment also accessed Google Email Address 1 (described above), despite the fact that the sender provided a Protonmail email address to complete the transaction.[18]

d. *June 23, 2023 (Purchase of **otanmail.com**):* Records from BitPay show that on June 23, 2023, an individual sent 0.000388 BTC from a bitcoin address ending in -5u5x to Namecheap in connection with the purchase of the domain name **otanmail.com**. Namecheap credited the account with $10 on the same day. The sender used the same Dutch VPN IP address referenced above to view the BitPay invoice and send the bitcoin.[19] Two other non-VPN IP addresses—which resolve to Russia and Poland, respectively—also viewed the invoice. The sender provided the same Protonmail email address from the April 2022 purchase and April 2023 renewal to complete the transaction.

e. *May 14, 2024 (Renewal of **mlrtr.com**):* Records from BitPay show that on May 14, 2024, an individual sent 0.00018743 BTC from a bitcoin address ending in -a0cp to Namecheap in connection with the renewal of the domain name **mlrtr.com**. Namecheap credited the account with $10 on the same day. The

[18] The same Protonmail email address was provided to complete the April 2022, April 2023, and June 2023 purchases.

[19] This same Dutch VPN IP address accessed Google Email Address 1 in October 2023.

sender used another Dutch VPN IP address to view the BitPay invoice and send the bitcoin. The sender provided Google Email Address 1 (described above) to complete the transaction, suggesting that the same individual(s) controlling Email Address 1 (and by extension, the other email accounts described above) also executed this transaction.

44. Based on these BitPay records and my training and experience, I believe there is probable cause to believe the funds used to purchase the **Subject Domain Names** originated outside the United States. As detailed above, an analysis of IP records shows that the actors viewed the invoices and sent the payments from countries outside the United States. Furthermore, even if the actor used a VPN to conceal his true location when initiating the cryptocurrency payments, the bitcoin necessarily flowed into the United States through the VPN exit nodes located abroad (*i.e.*, Lithuania, Sweden, and the Netherlands). In addition, the actor accessed the payment invoices for the April and June 2023 transactions from non-VPN addresses in Russia and Poland, indicating the sender was likely outside the United States when the bitcoin was sent via BitPay to Namecheap. Given these facts, there is probable cause to believe the funds used to purchase the **Subject Domain Names** originated outside the United States.

FBI Identifies an Additional 949 Social Media Accounts Using Subject Domain Names

45. In response to legal process, on June 21, 2024, X Corp. provided records related to other X Corp. social media accounts registered with email addresses using the **Subject Domain Names**. Based on these records, it appears that at least 968 accounts have been registered between June 11, 2022, and March 1, 2024, with email addresses using the **Subject Domain Names**. This

includes the nineteen accounts that were previously identified in the investigation. Based on my training and experience, I know that the 968 email addresses are registered using infrastructure associated with the **Subject Domain Names**.

46. Of the 968 accounts identified through X Corp. records, 922 were registered using the domain **mlrtr.com** and 46 were registered using the domain **otanmail.com**. I have reviewed a sample of the public-facing posts shared by certain of these accounts. Based on my review, it appears that these accounts have similarly been used to advance Russian government narratives and interests. For example, in November 2023, a bot account posted a video in which the speaker claimed that the number of foreign fighters embedded with Ukrainian forces was significantly lower than public estimates. In another post nine days later, the same bot account posted a video of President Putin claiming that the war in Ukraine is not a territorial conflict or a matter of geopolitical balance, but rather the "principles on which the New World Order will be based."

47. Based on the information above, I believe the malicious actors have used the **Subject Domain Names** to create numerous email addresses on private email servers, which have in turn been used to register 968 fictitious social media accounts that have been used to promote messages in support of the Russian government. The actors caused Namecheap to provide the **Subject Domain Names** to and for the benefit of the FSB and paid for the **Subject Domain Names** using international cryptocurrency transactions, without first obtaining the required license from OFAC. Because doing so violated U.S. money laundering laws in furtherance of an IEEPA violation, the **Subject Domain Names** are subject to seizure and forfeiture.

48. Losing control over the **Subject Domain Names** would have a significant impact on the actor's malicious activities. As an initial matter, seizure and forfeiture of the **Subject Domain Names** would prevent the malicious actors from creating new X Corp. profiles using emails from these domain names. In addition, seizure and forfeiture of the **Subject Domain Names** would prevent the delivery of emails to these servers. Without access to the email accounts associated with the **Subject Domain Names**, the malicious actors would be unable to complete the multi-factor authentication that X Corp. employs to detect bot activity on its platform.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

49. Title 18, United States Code, Section 981(a)(1)(A) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same) is subject to forfeiture.

50. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause and "obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Forfeiture." Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and such warrant may be executed in any district in which the property is found.

51. Title 18 United States Code, Section 982(a)(1) provides, in relevant part, that when imposing sentence on a person convicted of an offense in violation of 18 U.S.C. §§ 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same), a court shall order that person's property that was involved in the offense forfeit to the United States.

52. Title 18, United States Code, Section 982(b)(1) incorporates by reference the procedures for seizure and forfeiture in Title 21, United States Code, Section 853. Title 21, United States Code, Section 853(f) provides in relevant part that a seizure warrant for property subject to forfeiture may be sought "in the same manner as provided for a search warrant. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture."

53. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **Subject Domain Names** for forfeiture. By seizing the **Subject Domain Names** and redirecting them to another website(s), the Government will prevent third parties from acquiring the names and using them to commit additional crimes. Furthermore, seizure of the

Subject Domain Names will prevent third parties from continuing to access the **mlrtr.com** and **otanmail.com** websites in their present form.

54. Title 18, United States Code, Section 981(h) provides that venue for civil forfeiture proceedings brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

55. Under 18 U.S.C. § 981(b)(3), a seizure warrant for property subject to civil forfeiture may be issued in any district in which a forfeiture action against the property may be filed, and may be executed in any district in which the property is found.

56. Title 21, United States Code, Section 881(j), incorporated by 21 U.S.C. § 853(j), provides that venue for criminal forfeiture proceedings brought under this section lies in the district where the defendant owning the property subject to criminal forfeiture is located or in the judicial district where the criminal prosecution is brought.

57. Title 21, United States Code, Section 853(l) provides that the district courts of the United States have jurisdiction to enter orders, including seizure warrants, without regard to the location of property which may be subject to criminal forfeiture under Section 853.

58. As set forth above, there is probable cause to believe that the **Subject Domain Names** are subject to civil forfeiture because they were used in the commission of violations of 18 U.S.C. §§ 1956(a)(2)(A) (international promotional money laundering) and 1956(h) (conspiracy to commit the same). Specifically, the **Subject Domain Names** are property involved in transactions or attempted transactions that violate 18 U.S.C. §§ 1956(a)(2)(A) (international

promotional money laundering) and 1956(h) (conspiracy to commit the same), done with intent to promote the carrying on of specified unlawful activity, specifically violations of IEEPA.

SEIZURE PROCEDURE

59. As detailed in Attachment A, the registrar for the **Subject Domain Names** is Namecheap, located at 4600 East Washington Street, Suite 305, Phoenix, AZ 85034. Upon execution of the seizure warrant, Namecheap shall be directed to restrain and lock the **Subject Domain Names** pending transfer of all right, title, and interest in the **Subject Domain Names** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Subject Domain Names** cannot be made absent court order or, if forfeited to the United states, without prior consultation with the FBI or Department of Justice.

60. In addition, upon seizure of the **Subject Domain Names** by FBI, Namecheap will be directed to associate the **Subject Domain Names** to new authoritative name servers to be designated by a law enforcement agent. The Government will display a notice on the website to which the **Subject Domain Names** will resolve indicating that the sites have been seized pursuant to a warrant issued by this Court.

CONCLUSION AND REQUEST FOR SEALING

61. For the foregoing reasons, there is probable cause to believe that the **Subject Domain Names** are therefore subject to seizure and forfeiture to the United States as explained in this affidavit, and I respectfully request that the Court issue a seizure warrant for the **Subject Domain Names**.

62. Because the warrant will be served on Namecheap and at a time convenient to it, Namecheap will transfer control of the **Subject Domain Names** to the Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

63. Finally, I request that the Court order that all papers in support of this application, including the affidavit and seizure warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Disclosure may alert the targets to the ongoing investigation, and/or give targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Subscribed to and sworn to before me telephonically on this 27th day of June 2024.

EsWillett

HONORABLE EILEEN S. WILLETT
United States Magistrate Judge