

UNITED STATES DISTRICT COURT
for the
District of Columbia

In the Matter of the Seizure of
(Briefly describe the property to be seized)
ONE DOMAIN NAME CONTROLLED BY
PUBLIC INTEREST REGISTRY, FOR
INVESTIGATION OF VIOLATIONS OF 18
U.S.C. § 1956
Case No. 20-sz-30

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 that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under U.S.C. § (describe the property): 18 U.S.C. § 981(a); 18 U.S.C. § 982(a); 18 U.S.C. § 1956; and 28 U.S.C. § 1651 (describe the property):

ONE DOMAIN NAME CONTROLLED BY PUBLIC INTEREST REGISTRY, further described in Attachment A, with seizure protocols described in Attachment B.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

Continued on the attached sheet.

Michael A. Johnson
Applicant's signature

Michael Johnson, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 04/24/2020

Judge's signature

City and state: District of Columbia

Deborah A. Robinson, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Seizure of
(Briefly describe the property to be seized)
ONE DOMAIN NAME CONTROLLED
BY PUBLIC INTEREST REGISTRY,
FOR INVESTIGATION OF
VIOLATIONS OF 18 U.S.C. § 1956
Case No. 20-sz-30

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 located in the jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows: ONE DOMAIN NAME CONTROLLED BY PUBLIC INTEREST REGISTRY, further described in Attachment A, with seizure protocols described in Attachment B.

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 05/07/2020 (not to exceed 14 days)

[ ] in the daytime - 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a 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 United States Magistrate Judge Deborah A. Robinson (name)

[ ] 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 searched or seized (check the appropriate box) [ ] for days (not to exceed 30). [ ] until, the facts justifying, the later specific date of

Date and time issued: 04/24/2020 Judge's signature

City and state: District of Columbia Deborah A. Robinson, U.S. Magistrate Judge Printed name and title

**Return**

Case No.: 20-sz-30

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_

*Executing officer's signature*

\_\_\_\_\_

*Printed name and title*

**ATTACHMENT A**

**Property to Be Seized**

This warrant applies to the domain name listed below:

**coronaprevention.org**

(the “SUBJECT DOMAIN NAME”), which is stored at premises owned, maintained, controlled, or operated by Public Interest Registry, which is headquartered at and/or which accepts service of process in Virginia.

## ATTACHMENT B

1. IT IS ORDERED that, with respect to the SUBJECT DOMAIN NAME, Public Interest Registry (“Subject Registry”), who is the domain registry, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAME:
  - a. Take all reasonable measures to redirect the SUBJECT DOMAIN NAME to substitute servers controlled by Homeland Security Investigations, by changing the authoritative name servers to any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registry. Specifically, upon seizure of the Subject Domain Names, the Subject Registry shall point the Subject Domain Names to the IPR Center’s Domain Names ns1.seizedservers.com (IP address 66.212.148.117) and ns2.seizedservers.com (IP address 66.212.148.118).
  - b. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
  - c. Prevent any further modification to, or transfer of, the SUBJECT DOMAIN NAME pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAME to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAME cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Homeland Security Investigations, or the Department of Justice.
  - d. Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

2. The Government will display a notice on the website to which the SUBJECT DOMAIN NAME will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized in accordance with a seizure warrant issued by the United States Court for the District of Columbia after a Magistrate Judge found by probable cause that the domain was forfeitable pursuant to 18 U.S.C. §§ 981 and 982, for violations of 18 U.S.C. § 1956. Notice of forfeiture proceedings for this domain will be issued as set forth by law.

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

**IN THE MATTER OF THE SEIZURE OF  
ONE DOMAIN NAME CONTROLLED  
BY PUBLIC INTEREST REGISTRY,  
FOR INVESTIGATION OF  
VIOLATIONS OF 18 U.S.C. § 1956**

**Case No. 20-sz-30**

**Under Seal**

**AFFIDAVIT IN SUPPORT OF A SEIZURE WARRANT**

I, Michael Johnson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a seizure warrant for domain name coronaprevention.org (the “Target Property”), which domain is controlled by the Public Interest Registry. The property to seize and seizure procedure is further detailed in Attachment A. There is probable cause to believe that the Target Property is subject to seizure and forfeiture as described herein.

2. I am a Special Agent with Homeland Security Investigations (“HSI”), and have been so employed since 2003. Since becoming a Special Agent, I have participated in numerous investigations into suspected fraud and money laundering. I am currently assigned to Special Agent in Charge, Philadelphia, Pennsylvania. As a special agent, I attended approximately 26 weeks of special agent training at the Federal Law Enforcement Training Center (“FLETC”), Glynco, Georgia, in various aspects of criminal investigations dealing specifically with criminal law, criminal tax law, money laundering, wire fraud, seizure, and various financial investigative techniques. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of arrest, search and seizure warrants.

3. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who

have been involved in this investigation, and through a review of reports from other officials and reliable cooperating individuals.

4. Because this affidavit is submitted for the limited purpose of securing authorization for seizure warrants, I have not included each fact known to me concerning this investigation. I have set forth only the facts that I believe are essential to establish probable cause.

5. The investigation has further revealed that there is probable cause to believe that the current owner of the site (“Subject A”) has laundered monetary instruments, caused the laundering of monetary instruments, and aided and abetted the laundering of monetary instruments in violation of 18 U.S.C §§ 1956(a)(3)(A), and (a)(3)(B). Thus, there is probable cause to believe that the Target properties are subject to criminal and civil seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1) as property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property.

### **TECHNICAL BACKGROUND**

6. Based on my training and experience and information learned from others, I am familiar with the following terms:

- a. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet.
- b. Domain Name: A domain name is a simple, easy-to-remember way for people 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” is a domain name.
- c. 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 “usdoj.gov.” 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.

- d. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. 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 registry for the .org top-level domains is Public Interest Registry, which is based in the United States.

7. Registrar & Registrant: Domain names may be purchased through a registrar, 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. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

### **STATUTORY BACKGROUND**

8. This application seeks a seizure warrant under both civil and criminal authority, because the Target Property could easily be placed beyond process if not seized by a warrant. The

Target Property is electronic data, which can easily and quickly be moved. The Target Property has currently been disabled, pending a seizure warrant which will permanently shut down the site.

9. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction, in violation of 18 U.S.C. § 1956, or any property traceable to such property is subject to civil forfeiture. Pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in a violation of 18 U.S.C. § 1956, or any property traceable to such property is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. Rather, these forfeitures encompass all property “involved in” the crime, which can include untainted or legitimate funds that are comingled with tainted funds derived from illicit sources.

10. Pursuant to 18 U.S.C. § 981(b), property subject to forfeiture under § 981 may be seized via a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding). 21 U.S.C. § 853(f) permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. Thus, seizure warrants may be obtained outside of the district where the property to be seized is located. As discussed more fully below, acts or omissions giving rise to forfeiture occurred within Washington, D.C.

11. The All Writs Act provides in relevant part that “all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a). The All Writs Act permits a court, in its “sound judgment,” to issue orders necessary “to achieve the rational ends of law” and

“the ends of justice entrusted to it.” *United States v. New York Telephone Co.*, 434 U.S. 159, 172-73 (1977). The Supreme Court has further held that the All Writs Act is a “residual source of authority to issue writs that are not otherwise covered by statute.” *Penn. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985). The courts have described this authority as both “broad” and “flexible.” *See, e.g., N.Y. Tel. Co.*, 434 at 173; *United States v. Catoggio*, 698 F.3d 64, 67 (2d Cir. 2012).

12. In *New York Tel. Co.*, the Supreme Court used the All Writs Act to compel a third party phone company to assist the government with the implementation of a pen register. 434 U.S. at 178. The government seeks not only to seize the Target Property by essentially turning off the site, but also to redirect persons going to those sites to a government-controlled site with a posted notification that the original site has been seized based on alleged violations of the above statutes and that such site is subject to forfeiture. Allowing this redirect to a government notice page is necessary to fully effect the seizure of the domain and provide notice to the owner of the Target Property and co-conspirators who might visit the Target Property. In order to redirect to such page, the government will provide the Public Interest Registry with the new government address to which the Target Property should point. Each internet registry/registrant has complied with such requests in the past, and it poses only a nominal burden on the registrant (*i.e.*, changing code in a computer program). This request is consistent, if not less intrusive, than the request to *New York Tel. Co.*<sup>1</sup> The seizure procedures are detailed below, and further so in Attachment B.

---

<sup>1</sup> The government does not concede that a seizure warrant based on forfeiture authorities alone is insufficient to cause a redirect of a seized website. However, in the abundance of caution, the government also cites to the All Writs Act as additional authority for the instant request.

## **FACTS ESTABLISHING PROBABLE CAUSE**

13. On March 13, 2020, the President of the United States declared a national emergency due to the COVID-19 pandemic.

14. On March 14, 2020, Subject A advertised the sale of the Target Property on a forum (“Forum A”).

15. I know from my training and experience (including published cybersecurity reports) that Forum A is known to focus on content related to, and populated by users interested in, hacking and hijacking online accounts.

16. The advertisement on Forum A specified that the Target Property would be an effective way to sell “high markup in demand products.”

17. The advertisement directed potential buyers to use an encrypted messaging application to communicate with Subject A about the purchase of the site.

18. On April 13, 2020, an HSI undercover agent (UCA) initiated a conversation with Subject A.

19. Subject A stated that the Target Property could be purchased for \$500.

20. I know from my training and experience that such the domains can typically be purchased for approximately \$20. Thus, Subject A was charging an exponential markup to sell the Target Property.

21. Subject A stated that payment should be made via bitcoin (BTC).<sup>2</sup>

---

<sup>2</sup> BTC is a pseudonymous virtual currency. Transactions are visible on a public ledger. Each transaction is referenced by a complex series of numbers and letters (as opposed to identifiable individuals) involved in the transaction. BTC is not issued by any government, bank, or company, but rather is controlled through computer software.

22. Subject A asked the UCA about the UCA's plan for the site. The UCA stated that he/she was going to "unload some merchandise" on it.

23. On April 16, 2020, the UCA informed Subject A that the UCA was having problems with a prior site he operated.

24. The UCA told Subject A that the UCA needed an additional few days to get the BTC ready to purchase the Target Property. Subject A responded that this was fine.

25. On April 17, 2020, the UCA, while in Washington, D.C., informed Subject A that the UCA's other site was officially offline and that the UCA still had "a ton of merchandise to sell." The UCA further explained that he/she was ready to buy the Target Property as it was "the next best thing out there."

26. Subject A responded that Subject A was ready to receive the BTC as payment, and that the UCA needed to create an account with the domain registrant in order to take control of the site once payment was completed. Subject A transmitted his/her BTC address to the UCA.

27. Subsequently on April 17, 2020, the UCA informed Subject A that the UCA was locked out of his/her BTC account at a virtual currency exchange. The UCA stated that his account may have been locked because the UCA was "selling all these fake covid testing kits." The UCA further explained that he/she had "a ton to sell and they were selling good so I need a good site like yours. I can't get stuck with all of these, who's going to want to buy them after the pandemic or when they find out they are fake?????"

28. Subject A stated that it was "genius" to sell "fake testing kits." Subject A further stated that he/she "wanted to do that but I couldn't get enough cash to bulk buy them from Alibaba [a Chinese e-commerce site]."

29. Subject A then asked the UCA if the UCA had a new site ready to be published at the Target Property. The UCA responded that he/she no longer had access to a site because the prior site was taken down.

30. Subject A recommended how to set up a new site and specifically directed the UCA to use a foreign-based service, so as to prevent U.S. authorities from shutting down the new site on the Target Property.

31. On April 20, 2020, the UCA sent a partial payment in BTC to Subject A.

### **SEIZURE PROCEDURE**

32. As detailed in Attachment B the registry shall be directed to restrain and lock the Target Property pending transfer of all right, title, and interest in the Target Property to the United States upon completion of forfeiture proceedings, to ensure that changes to that domain name cannot be made absent court order or, if forfeited to the United States, without prior consultation with law enforcement or the Department of Justice.

33. In addition, upon seizure of the domain name the registry will be directed to associate the domain name to a new authoritative name server(s) to be designated by a law enforcement agent.<sup>3</sup> The government will display a notice on the website to which the domain name will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

### **CONCLUSION**

34. Based upon the evidence gathered in this investigation and set out above, I submit that there is probable cause to believe that Target Property was used and/or intended to be used in

---

<sup>3</sup> According to the Internet Assigned Numbers Authority, an authoritative name server is a DNS server that has been designated to answer authoritatively for the designated zone, and is being requested to be listed in the delegation. It is recorded by its fully-qualified domain name, potentially along with its IP addresses.

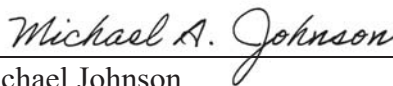
facilitating and/or committing the offenses described above. Accordingly, the Target Property is subject to seizure and forfeiture, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a).

35. Because the warrant will be served on the registrant, which respectively controls the Target Property, and the registrant at a time convenient to them thereafter, will transfer control of the Target Property to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

36. Further, I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Seizure Warrant. In support of this request, I inform the Court that I am currently in Pennsylvania, where I am working on the investigation of this and other matters. If I were required to appear before the Court in person, it would be a cost to the United States both in travel costs and time diverted from the substantive investigation. I submit that staff from the U.S. Attorney's Office are capable of identifying my voice and telephone number for the Court.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Respectfully submitted,

  
\_\_\_\_\_  
Michael Johnson  
Special Agent  
Homeland Security Investigations

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on April 24, 2020.

\_\_\_\_\_  
HON. DEBORAH A. ROBINSON  
UNITED STATES MAGISTRATE JUDGE