DMP:AFM/SKW
F. #2021R01001

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– – – – – – – – – – – – – – – – – – – X

In re the Seizure of:

The Domain Name:

Try2services.vc

– – – – – – – – – – – – – – – – – – – X

TO BE FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR
SEIZURE WARRANTS**

Case No. 23-MJ-405

EASTERN DISTRICT OF NEW YORK, SS:

RICHARD PENA-ARIET, being first duly sworn, hereby deposes and states that he is a Special Agent with the U.S. Secret Service ("USSS"), duly appointed according to law and acting as such:

1. I am a Special Agent with the USSS and have been since 2014. I am responsible for conducting and assisting in investigations involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. This affidavit is made in support of an application for a seizure warrant for the following domain name: try2services.vc (the "Subject Domain").

3. The Subject Domain falls under the authority of the following top-level domain registry: Identity Digital (previously known as Donuts), located at 10500 NE 8th Street, Ste. 750, Bellevue, Washington, 98004 (the "Registry").

4. This affidavit is based upon my personal involvement in this investigation, my review of the investigative file, my training and experience, my consultation with experts in cybercrime and copyright infringement, and reports made to me by witnesses and other law enforcement officers involved in the investigation. Because this affidavit is being submitted for the limited purpose of establishing probable cause for obtaining seizure warrants, I have not included each and every fact known to me concerning this investigation. Where the contents of documents and the actions and statements of others are reported herein, such statements are set forth in substance and in part, unless otherwise indicated.

5. As set forth below, there is probable cause to believe that the Subject Domain is involved in access device fraud, in violation of Title 18, United States Code, Section 1029 and computer intrusion, in violation of Title 18, United States Code, Section 1030 (together, the "Subject Offenses").

6. On April 18, 2023, a grand jury sitting in the Eastern District of New York returned an indictment charging the defendant Denis Gennadievich Kulkov with, among other conduct, using the Domain Name (try2services.vc) to commit the Subject Offenses. See 23-CR-171 (FB), attached as Exhibit A. The indictment remains sealed at this time.

7. Accordingly, and as set forth in more detail below, there is probable cause to believe that the Subject Domain is subject to forfeiture pursuant to 18 U.S.C. §§ 1029(c)(1)(C) and 1030(i)(1)(A) as property that was used, or intended to be used, to commit the Subject Offenses.

STATUTORY FRAMEWORK

8. Pursuant to 18 U.S.C. § 1029, whoever "knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices" is subject to criminal punishment.

9. Pursuant to 18 U.S.C. § 1030, whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period" is subject to criminal punishment.

10. Pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used, or intended to be used, to commit a violation of 18 U.S.C. § 1029 is subject to forfeiture to the United States.

11. Pursuant to 18 U.S.C. § 1030(i)(1)(A), any personal property used, or intended to be used, to commit or facilitate the commission of a violation of 18 U.S.C. § 1030 is subject to forfeiture to the United States.

12. Pursuant to 21 U.S.C. § 853(f), this Court is empowered to issue a seizure warrant for any property subject to forfeiture.

DEFINITIONS AND TECHNICAL BACKGROUND

13. Internet Protocol Address: An Internet Protocol 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").

14. 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 "cnn.com" are domain names.

15. 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 is the web server.

16. Domain Name Servers: DNS servers, or "name servers," are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

17. 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. Here, for example, the registry for the ".vc" top-level domain is Identity Digital

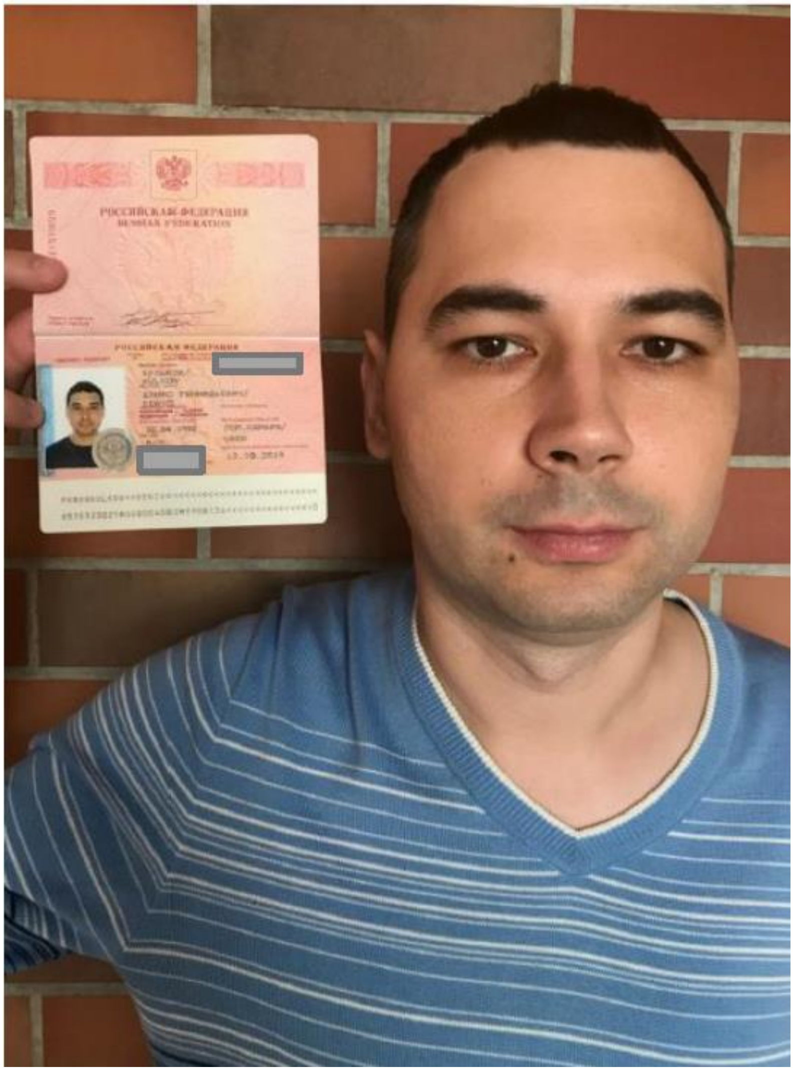
(previously known as Donuts), located at 10500 NE 8th Street, Ste. 750, Bellevue, Washington, 98004.

18. 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.

THE INVESTIGATION

A. Background

19. Since approximately 2013, law enforcement has been conducting an investigation into a platform called Try2Check and the defendant DENIS GENNADIEVICH KULKOV. A photograph of KULKOV holding his Russian passport found on his iCloud account is below, with the passport number redacted.



20. In approximately 2005, the defendant DENIS GENNADIEVICH KULKOV created the website Try2Check to engage in the scheme to assist cybercriminals in trafficking stolen credit cards. Between 2005 and the present, KULKOV operated Try2Check to further his criminal scheme. In total, between June 2014 and November 2022, KULKOV received the equivalent of at least $18 million USD in bitcoin for the scheme. Notably, blockchain tracing revealed that KULKOV transferred substantial funds he received from Try2Check to BTC-E, a cryptocurrency exchange that was seized by law enforcement in 2017 due to criminal action.

21. The defendant DENIS GENNADIEVICH KULKOV's scheme involved using Try2Check to authenticate U.S.-issued credit cards on behalf of cybercriminals by effecting unauthorized access to computers belonging to Victim-1, including on behalf of customers located in the Eastern District of New York.

22. Victim-1 functioned as an intermediary (or one of several intermediaries) between credit card issuers and businesses that accept payment via credit cards. When a consumer inserted a credit card into a point-of-sale machine at a business, the card information traveled to Victim-1's servers. Victim-1 then determined what issuer the credit card belonged to, communicated with the issuer on behalf of the business, and sent a signal back to the point-of-sale machine reflecting that the transaction had been authorized.

23. In addition to allowing businesses to charge consumers' credit cards, Victim-1 also offered a service whereby it merely confirmed a card's validity without actually charging the card, known as "preauthorization." For example, when a guest checks into a hotel, the hotel might request that Victim-1 preauthorize a charge on the guest's card to confirm that it is valid and has the necessary credit available, but the hotel typically will not charge the card until the guest checks out.

24. Try2Check took advantage of Victim-1's preauthorization service by submitting thousands of fraudulent preauthorization request to determine how many stolen credit cards in a batch remained active, and therefore were of value to cybercriminals.

25. Between approximately April 13, 2018 and December 31, 2018, Try2Check submitted at least 16 million fraudulent credit card preauthorization requests on behalf of cybercriminals. Similarly, between approximately September 24, 2021 and October 25, 2022, Try2Check submitted at least 17 million fraudulent credit card preauthorization

requests on behalf of cybercriminals. In turn, cybercriminals used this information to further traffic in stolen credit card data.

26. DENIS GENNADIEVICH KULKOV's receipts from operating Try2Check were significant. In total, between June 2014 and November 2022, KULKOV received at least the equivalent of $18 million in bitcoin in connection with the scheme, which amount includes only the revenue from the movement of funds visible on the Bitcoin blockchain, excluding alternative means of payment that Try2Check at times offered its users. KULKOV used his proceeds from the scheme to buy luxury goods, including a Ferrari sports car. A photograph of KULKOV driving the Ferrari sports car he purchased is below.

B. The Subject Domain

27. The Subject Domain, try2services.vc, serves as one of the main websites for Try2Check. Cybercriminals who wish to enlist the services of Try2Check typically register an account with Try2Check via the domain try2services.vc or one of the other domains operated by Try2Check. Try2Check, via the Subject Domain, accepts customer payments in exchange for the criminal service rendered by Try2Check. The Subject Domain also allows its customers to engage in illegal transactions by exploiting a vulnerability at a U.S. victim organization. In addition. Try2Check, via the Subject Domain, involves the laundering of monetary instruments, insofar as it accepts payment in cryptocurrency to obfuscate investigation of Try2Check's criminal proceeds. Therefore, the Subject Domain is involved in violations of the Subject Offenses.

28. A search of publicly available domain name registration records revealed that the Subject Domain was most recently registered on December 8, 2022. The registry operations for the .vc top-level domain are managed by Identity Digital, previously known as Donuts, which has its headquarters at 10500 NE 8th Street, Ste. 750, Bellevue, WA 98004.

SEIZURE PROCEDURE

29. The procedure by which the government will seize the Subject Domain is described in Attachment A. As detailed in Attachment A, upon execution of the seizure warrant, the Registry for the top-level domain, Identity Digital, shall be directed to restrain and lock the Subject Domain pending transfer of all right, title, and interest in the Subject Domain to the United States upon completion of forfeiture proceedings to ensure that changes to the Subject Domain cannot be made absent court order or, if forfeited to the United States, without prior consultation with the USSS or the United States Marshals Service.

30. With respect to the Subject Domain, the Registry, Identity Digital, will be directed to associate the Subject Domain to a new authoritative name server to be designated by a law enforcement agent. The Government will then display a notice on the website to which the Subject Domain will resolve indicating that the site has been seized pursuant to a warrant issued by this Court.

CONCLUSION

31. Based on the facts set forth above, there is probable cause to believe that the Subject Domain constitutes property used, or intended to be used, to commit violations of 18 U.S.C. §§ 1029 and 1030. The Subject Domain is therefore subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 1029(c)(1)(C) and 1030(i)(1)(A).

32. A restraining order, issued pursuant to 21 U.S.C. § 853(e), is not sufficient to guarantee the availability of the Subject Domain for forfeiture. Only seizing the Subject Domain and either blocking or redirecting traffic to another website will prevent third parties from continuing to access and use the Subject Domain, including due to the risk of registry error.

33. Accordingly, I respectfully request that the Court issue a seizure warrant, pursuant to 21 U.S.C. § 853(f), authorizing the seizure of the Subject Domain.

34. Because the warrant will be served on the Registry which controls the Subject Domain, and the Registry thereafter, at a time convenient to it, will transfer control of the Subject Domain to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

35. I further 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, except that copies of the seizure warrant may be served at the time they are executed, and the government may provide copies of the seizure warrant and this affidavit to any law enforcement or regulatory authorities for use in connection with the restraint, seizure and/or forfeiture of the Subject Domain, and as required by its discovery obligations, including Rule 16 of the Federal Rules of Criminal Procedure. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Dated: Brooklyn, New York
April 27, 2023

[redacted]

RICHARD PENA-ARIET
Special Agent
U.S. Secret Service

Sworn and subscribed to before me by telephone
this 27th day of April 2023

[redacted]

HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK