United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)
THE USE OF A NETWORK INVESTIGATIVE TECHNIQUE FOR A COMPUTER ACCESSING EMAIL ACCOUNT: PSANCHEZ@INVERMAR.US

Case No. 17-MJ- 653

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: **THE USE OF A NETWORK INVESTIGATIVE TECHNIQUE FOR A COMPUTER ACCESSING EMAIL ACCOUNT: PSANCHEZ@INVERMAR.US, as more particularly described in Attachment A,**

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
***See* Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1343 all of which is more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of **Title 18, United States Code, Section 1343.**

The application is based on these facts:
- ☒ continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Barry W. Couch, Special Agent
Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.
Date: November 3, 2017

Judge's signature

City and state: Rochester, New York

HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

ATTACHMENT A

Location to be Searched

This warrant authorizes the use of a network investigative technique on the portion of any computer accessing TARGET EMAIL, psanchez@invermar.us, that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

ATTACHMENT B

Information to be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence, instrumentalities, contraband and fruits of violations of Title 18, United States Code, Section 1343 (Wire Fraud). This information may include environmental variables and/or certain registry-type information, such as:

1. The computer's IP address.
2. The computer's User Agent String.

This warrant does not authorize the physical seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of stored wire and electronic information as described above. See 18 U.S.C. § 3103a(b)(2).

ADDENDUM TO SEARCH WARRANT
SEARCH OF COMPUTERS

1. The computer or electronic media search authorized by this warrant shall be completed within 60 days from the date of the warrant unless, for good cause demonstrated, such date is extended by Order of this Court.

2. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents or other electronically stored information which are identified in the warrant itself.

3. Should the government not locate any of the items specified in the warrant (or other fruits, contraband, instrumentalities, or property subject to forfeiture) within the authorized search period (including any extensions granted), the government shall return the computer or electronic media to the owner.

4. In any circumstance not covered by paragraph three (3) above, upon completion of the search, the government, upon request of the owner of the computer, shall promptly return to the owner of the computer copies of all files and documents requested and specified by the owner, excluding any items or files seized pursuant to the warrant or other fruits, contraband, instrumentalities or property subject to forfeiture.

5. If electronically stored data or documents have been identified by the government pursuant to this warrant, or other fruits, contraband, instrumentalities or property subject to forfeiture, the government may retain the original hard drive or other data storage mechanism pending further order of this Court. The retention of the original hard drive or other data storage mechanism does not relieve the government of its obligation to return to the owner of the computer files, documents or other electronically stored information identified in paragraph four (4) above.

6. Nothing in this warrant shall limit or prevent the government from retaining the computer or electronic media as fruits, contraband, or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in the warrant shall limit or prevent the owner of the computer or electronic media from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data. Software or hardware.

7. Should there be a dispute or a question over ownership of any computer or any electronically stored data or documents stored therein, the government shall promptly notify this Court so that such dispute or question can be resolved.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF: THE USE OF A NETWORK INVESTIGATIVE TECHNIQUE FOR A COMPUTER USING EMAIL ACCOUNT PSANCHEZ@INVERMAR.US	Case No. 17-MJ-_____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Barry W. Couch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) for approximately nine years. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment,

mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I make this affidavit in support of an application under Rule 41(b)(6)(A) of the Federal Rules of Criminal Procedure in support of an application for a search warrant to use a network investigative technique ("NIT"). I request approval to send one or more communications to any computer accessing psanchez@invermar.us (TARGET EMAIL). Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Title 18, United States Code, Section 1343 (which makes it a crime to transmit communications by means of wire, in interstate or foreign commerce, for purposes of obtaining money by means of false or fraudulent pretenses) have occurred and that evidence, instrumentalities, contraband and fruits of those violations exist on the computer(s) that receives the NIT described above.

4. 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.

RELEVANT STATUTES

5. This investigation concerns alleged violations of: 18 U.S.C. § 1343 – Wire Fraud.

a. 18 U.S.C. § 1343 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

6. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

7. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can

be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

8. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

9. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

10. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

11. "Attachment" refers to a data file (examples include Microsoft Word, PDF, or picture file) that, when included with an email, transfers the file directly to the recipient(s) of the email.

12. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

14. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.

15. "Proxy Server" or "Proxy" is a computer that acts as a gateway between a local network (e.g. all of the computers at one company or building) and a larger-scale network such as the internet. A Proxy Server can be used to protect a users' privacy by routing a user's IP Address through an intermediary computer, thereby masking the user's actual IP address and location which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way proxy services route communications through other computers, traditional IP identification techniques are not viable. When a user using a proxy service accesses a website, for example, the IP address of the proxy service, rather than the user's actual IP address, shows up in the website's IP log.

16. "Virtual Private Network" or "VPN" is a digital network that connects to a private network over the internet. It allows remote computers to act as though they were on the same secure, local network, emulating the properties of a point-to-point private link. For

example, someone working from home on their home network can connect to their company's network though a VPN. When a user accesses a website or data though a VPN, it would show the IP Address of the VPN server the user connected to the website through, not their true IP Address. When connecting to the internet through a VPN service, a user has the ability to choose the country and city they would like to appear to be from, which can obfuscate their geographic location.

PROBABLE CAUSE

17. In August 2017, the Payment Services department of a local business (VICTIM) located in the Western District of New York, received an email request appearing to originate from one of their product suppliers, Invermar, to change their banking information for wire transfer payments. The TARGET EMAIL used by the TARGET USER to communicate the changes in Invermar's banking information was psanchez@invermar.us. It should be known that the VICTIM was familiar with a legitimate Invermar email address of psanchez@invermar.cl and the slight change in lettering at the end of the email address was not noticed by the VICTIM until after they completed wire transfers through the newly provided banking information. The VICTIM, who regularly communicated and conducted business with Invermar through email, understood the change in Invermar's banking information to be valid. The VICTIM attempted several times in August 2017 and September 2017, to pay their invoices due to Invermar, with the new banking information provided by the TARGET USER. However, those attempts were denied by the receiving banks. Finally, near the end of September 2017, and in October 2017, the VICTIM successfully completed

four wire transfers to the TARGET USER using new banking information provided by the TARGET USER, totaling approximately $1.2 million. As of today, the VICTIM has been able to recover approximately $300,000 of their loss from the bank the successful transfers occurred through. It is unknown at this time whether or not the VICTIM will be able to recover any more of their loss.

18. This Search Warrant attempts to obtain legal authority to identify the user (hereinafter TARGET USER) of TARGET EMAIL. Given the actions of the actor whom successfully executed a scheme to defraud the VICTIM, your Affiant believes that TARGET USER repeatedly stole the money of the VICTIM, a victim company within the District of Western New York, by committing wire fraud. As a sophisticated cybercriminal, the TARGET USER took steps to hide his/her true identity and the location from which he/she is connecting and communicating.

19. The deployment of the NIT will occur through email communications with the TARGET USER, with consent from the VICTIM. The FBI will provide an email attachment to the victim which will be used to pose as a form to be filled out by the TARGET USER for future payment from the VICTIM. The FBI anticipates the target user, and only the target user, will receive the email and attachment after logging in and checking emails. The subject will download the attachment which will deploy a technique designed to identify basic information of the TARGET USER's location. Your Affiant believes the TARGET USER will see the opportunity to complete documentation necessary to illegally acquire money and download the attachment. The attachment will only be included to the email(s) sent to the

TARGET EMAIL and will not be sent to any other email address. Based on past activities of other individuals participating in similar schemes, the FBI anticipates TARGET USER will potentially access the TARGET EMAIL only after accessing a proxy or VPN service. As such, the FBI will use a document with an embedded image requiring the computer to navigate outside the proxy service in order to access the embedded item.

20. The general public will be protected from any violation of privacy through careful and direct deployment of the NIT to the specific target email. Following the sending of the NIT to the target user, the FBI will ensure the tool is removed from the VICTIM's network. The FBI will maintain, at all times, ownership of the NIT.

THE REMOTE SEARCH TECHNIQUE

21. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help law enforcement locate the user of the TARGET EMAIL. Accordingly, I request authority to use the NIT, which will be deployed via email to investigate any user who logs into the TARGET EMAIL on any computer.

22. If a computer successfully activates the request to download the embedded image, the FBI computer hosting that image will show that download. Given the TARGET USER's potential anonymity techniques via proxy service as well as general curiosity, the deployment of this technique may result in the TARGET USER downloading the image

multiple times. In each case, the web server log of the FBI machine will only show the timestamp, originating IP Address, and User String.

23. The subject will open the attachment which will include an embedded image hosted on a server operated by the FBI. By opening the attachment, and exiting protected mode (requiring a second manual step), the user's computer will connect to the FBI server to access the image content and, in doing so, will pass IP address information to the destination web server. This operation will not include a search of the user's computer nor will it include the downloading of code to the machine; rather, this operation will pass the IP address and user agent string much like an IP address and user agent string are passed when any user accesses any web site. Given that no content is being searched nor is any computer code executed locally on that machine, the Government does not believe that a Search Warrant is required to execute the Embedded Image Option. In an abundance of caution, coupled with the fact that the user will need to exit protected mode within the Microsoft Word application, the Government is requesting authorization through a Search Warrant.

24. Specifically, this technique is designed to collect the items described below and in Attachment B, i.e., information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence, instrumentalities, contraband and fruits of violations of target offenses. This information may include the following:

a. The computer's IP address (Internet Protocol Address). An IP Address is a unique numeric address used to direct information over the Internet. IPv4 addresses are written as a series of four groups of numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178).

Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

b. The User Agent String. The User Agent String is a short string of information that web browsers and other applications send to identify themselves to the web servers. The User Agent String commonly identifies the browser version, software version, operating system version, and device type.

c. No screenshots of any kind will be taken of the computer of the when the TARGET USER opens the attachment sent to the TARGET EMAIL.

25. Each category of information sought by the NIT may constitute and/or contain evidence of the crimes under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer's true assigned IP address can be associated with an Internet Service Provider ("ISP") and a particular ISP customer. The user agent string can help identify a pattern of web browsing techniques used while conducting illegal activity.

26. Based on my training, experience, my consultation with forensic computer experts, and the investigation described herein, your Affiant knows that network level messages and information gathered directly from a sending computer can be effective in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. Getting an IP address and other information directly from the computer being used by the subject can defeat such techniques but only if the user or computer logic is outside of a proxy network session when executing the NIT exploit. The NIT will cause the above-described

information to be sent over the Internet to a computer controlled by the FBI who will analyze the resulting information.

TIME AND MANNER OF EXECUTION OF THE SEARCH

27. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) "to execute the warrant within a specified time no longer than 14 days" and (b) to "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time . . . ." The government seeks permission to deploy the NIT at any time of day or night within 14 days of the date the warrant is authorized. There is good *cause* to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. More specifically, the government has no control of the timing or when the subject(s) will access the target emails accounts. The government also seeks to read any the information that the NIT causes to be sent from the activating computer at any time of day or night during the 14 days from the date the warrant is authorized. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

JURISDICTION

28. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district.

AUTHORIZATION REQUEST; DELAYED NOTICE

29. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I request that this Court authorize the officers executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed.

30. This application seeks a warrant authorizing the use of computer software on the computer accessing the TARGET EMAIL that, after successful installation, will collect and send information from that computer and make it available to government personnel authorized by the requested warrant to receive and review such information. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B). However, as further specified in Attachment B, which is incorporated into the warrant, the applied-for warrant does not authorize the physical seizure of any tangible property.

31. It is intended that the collection and sending of such information will be performed without the knowledge of the TARGET USER.

32. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the owner or user of the target emails would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1).

33. To the extent that Attachment B describes stored wire or electronic information, such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the network investigative technique does not deny the users or administrators access to the account information, nor does the technique permanently alter any of the information stored in the accounts. See 18 U.S.C. § 3103a(b)(2).

SEARCH AUTHORIZATION REQUESTS

34. Accordingly, for each of the aforementioned reasons, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to the FBI network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

b. that the government may receive and read, at any time of day or night, within 14 days from the date the Court authorizes the use of the NIT, the information that the NIT causes to be sent to the computer controlled by the FBI;

c. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken until the time that a suspect has been identified and has been placed in custody from the sending of the NIT unless notification is further delayed by the court; and

d. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

REQUEST FOR SEALING

35. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the search warrant is relevant to an ongoing investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

36. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence,

instrumentalities, contraband and fruits of criminal activity related to wire fraud, in violation of Title 18, United States Code, Section 1343.

37. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence of these crimes.

38. Based on the information described above, there is probable cause to believe that deploying the NIT on the computer described in Attachment A, to collect information described in Attachment B, will result in the United States obtaining the evidence and instrumentalities of the target offenses described above.

BARRY W. COUCH, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 3 day of November, 2017

HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE