AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
VITALII CHYCHASOV a/k/a Vitaliy Chichasov a/k/a leaderok a/k/a ramashka a/k/a ldr.men a/k/a blackinfo

Defendant(s)

Case No. 8:21MJ2079TGW

CRIMINAL COMPLAINT

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

On or about the date(s) of set forth below in the county of Hillsborough in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy to commit access device fraud, from in or around January 2015 through the present (Count One);
18 U.S.C. § 1029(a)(2)	Trafficking in unauthorized access devices, for calendar years 2019, 2020, and 2021 (Counts Two through Four); and
18 U.S.C. § 1029(a)(3)	Possession of 15 or more unauthorized access devices, on or about May 25, 2020 (Count Five).

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Justin Allen, Special Agent IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date: Oct. 28, 2021

Judge's signature

City and state: Tampa, Florida

Thomas G. Wilson, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT

I, Justin Allen, being duly sworn, depose and state the following:

1. I am employed as a Special Agent with the Internal Revenue Service–Criminal Investigation (IRS–CI) and have been employed in this capacity since February of 2010. My responsibilities include the investigation of criminal violations of Titles 18, 26, and 31 of the United States Code, and related offenses. As part of my activities, I have been involved in the investigation of different frauds, to include, but not limited to, bank fraud, mail fraud, wire fraud, and tax fraud. I earned a Bachelor of Science degree in Accounting from Florida State University in 2004 and a Masters in Accounting from Florida State University in 2005. I received my Certified Public Accountant license from the State of Florida in 2006. I have attended over 500 hours of training in various aspects of criminal investigation as well as classes dealing specifically with tax evasion, money laundering, asset seizure and forfeiture, various financial investigative techniques, and related financial investigations. I received this training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the National Criminal Investigation Training Academy for Internal Revenue Service Special Agents, Glynco, Georgia. In my capacity as a special agent with IRS–CI, I have conducted a variety of financial, tax, narcotics, and money laundering investigations. I have assisted in the execution of numerous search warrants,

resulting in the seizure of paper, electronic, and other forms of evidence. I am currently a Task Force Officer with the Federal Bureau of Investigation assigned to the cybercrime task force in Tampa, Florida.

2. I have investigated many different federal crimes, including tax fraud, theft of government property, narcotics violations, wire and mail fraud, money laundering, and computer intrusions. Many crimes that I have previously investigated involved the use of computer hardware and software, including images of servers, to help perpetrate or further the crime. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute arrest warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a criminal complaint and arrest warrant for VITALII CHYCHASOV a/k/a Vitaliy Chichasov a/k/a leaderok a/k/a ramashka a/k/a ldr.men a/k/a blackinfo. This affidavit does not set forth every fact resulting from the investigation; rather, it sets forth facts sufficient to establish probable cause to believe that CHYCHASOV has violated the following criminal statutes:

a. Count One: 18 U.S.C. § 371 (conspiracy to commit access device fraud) from in or around January 2015 through the present;

b. Counts Two through Four: 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices) for calendar years 2019, 2020, and 2021; and

c. Count Five: 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices) on or about May 25, 2020.

DEFINITIONS

4. The following definitions apply to this affidavit:

a. An "Internet Protocol" or "IP" address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must have an assigned IP address so that Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most Internet Service Providers ("ISPs") control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the computer an IP address. Any and all computers using the same ISP account during that session will share an IP address. An IP address can only be assigned to one customer at a time and the customer's computer retains the IP address for the duration of the Internet session until the user disconnects. When an Internet user visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

b. "ISPs" are businesses that, among other things, enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines, provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers, remotely store electronic files on their customers' behalves, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with the ISPs. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.

c. A "server" is A computer that provided services for other computers connected to it via a computer network—i.e., a set of computers connected together locally for the purpose of sharing resources—or the internet. Servers could be physically located and accessed anywhere with a network or internet connection. A server could have been either a physical or virtual machine. A physical server was a piece of computer hardware configured as a server. Multiple virtual servers could be located on a single physical server, but each virtual server's data would be segregated from the data of the other virtual servers.

d. An "access device" was any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number (including social security number), or other telecommunications service, equipment, or instrument identifier, or other means of account access that could be used alone or in conjunction with another access device to obtain money, goods, services, or any other thing of value, or that could be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

e. An "unauthorized access device" was any access device that was lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

f. "Jabber" is an open-source instant messaging protocol widely used on the internet. It enables users to connect and message with each other over various operating system platforms.

g. "Bitcoin" is a type of cryptocurrency. Bitcoin are sent and received from Bitcoin "addresses." Every Bitcoin transaction is recorded on a publicly available ledger known as the "blockchain."

i. A Bitcoin address is somewhat analogous to a bank account number, and the address is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding "private key." This private key is the cryptographic

equivalent of a password, or pin, and the private key is necessary to access the Bitcoin address. Only the private key's holder can authorize bitcoin transfers from the holder's address to other Bitcoin addresses. The individual or entity who holds the private key for a Bitcoin address is therefore considered the "owner" of the address.

ii. Users can have multiple Bitcoin addresses at any given time and some users may even use a unique Bitcoin address for every transaction. Users often combine multiple Bitcoin addresses (and their corresponding private keys) in a single logical unit known as a Bitcoin "wallet."

iii. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is often used by individuals and organizations for criminal purposes, such as money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track proceeds of illicit activities. Although it is not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

iv. While a Bitcoin address itself does not generally reveal the address's owner (unless the owner opts to make information

about the owner's Bitcoin address publicly available), investigators can sometimes use the blockchain to identify the owner of a particular Bitcoin address or identify Bitcoin addresses that likely all belong to the same owner. For example, investigators can trace transactions to other Bitcoin addresses, including Bitcoin exchanges (companies that allow users to convert, for example, USD to Bitcoin and vice versa) and Bitcoin payment processors.

STATEMENT OF PROBABLE CAUSE

5. CHYCHASOV is a Ukrainian national and resident. CHYCHASOV and his coconspirators operated at least two websites, including SSNDOB.WS and SSNDOB.CLUB (collectively, "SSNDOBCLUB"), that sold personally identifiable information of U.S. citizens, including names, social security numbers, and addresses ("PII") to others. Investigators have determined that the SSNDOBCLUB websites have listed the PII for approximately 24,000,000 individuals and have generated more than 19,000,000 USD[1] in sales revenue since August 2017.

INVESTIGATION INITIATION

6. In September 2016, IRS-CI and the FBI began investigating an online marketplace that sold access to compromised RDP credentials (*i.e.*, IPs,

[1] Unless otherwise specified, currency references herein are in United States Dollars.

usernames and passwords) that allowed the purchasers to access without permission compromised computer servers located worldwide (the "Marketplace"). The Marketplace began operating in or around October 2014, and in around January 2017, the Marketplace began to offer for sale certain PII. The information could be purchased for approximately $5 per unit of PII. Based on my training and experience, and my investigation to date in this case, I know that stolen social security numbers are often used to commit a variety of crimes, including credit card fraud, unemployment insurance fraud, bank fraud, stolen identity refund fraud, and the like, which activities affect interstate and foreign commerce.

7. In coordination with several foreign governments and federal partners, IRS-CI and the FBI conducted a take-down operation against the Marketplace on or about January 24, 2019. The information obtained during the domain seizure and takedown included some of the raw data used to run the Marketplace. Upon reviewing this data, the investigators determined that the administrators of the Marketplace had partnered with the administrators of a second criminal website, known as SSNDOB.WS, which focused its efforts on in the sale of stolen PII.

8. After analyzing the seized Marketplace server, an FBI computer scientist determined that the Marketplace administrators were granted special access to the SSNDOB.WS website. This special access provided the Marketplace

with the ability to re-sell the SSNDOB.WS stolen PII to Marketplace customers on the Marketplace website, without the Marketplace's customers knowing the true origin of the information. For this service, both the Marketplace administrators and SSNDOB.WS administrators earned and shared in the profit on the sale of each unit of PII.

SSNDOBCLUB

9. Investigators obtained the login credentials for an existing SSNDOB.WS account from a source of information. On or about May 18, 2020, an FBI Online Covert Employee ("OCE") accessed the SSNDOB.WS website (using the source's credentials) and observed two jabber accounts listed as contacts for the website if, for example, a user needed support. One of the Jabber accounts was sdbclub@jabber.dk ("SUPPORT"). On or about May 25, 2020, the OCE, while within the Middle District of Florida, communicated with SUPPORT, and requested that SUPPORT register a new account with SSNDOB for the OCE. SUPPORT subsequently registered an account for the OCE on the domain SSNDOB.CLUB, rather than SSNDOB.WS.

10. I have reviewed both of the websites, SSNDOB.CLUB and SSNDOB.WS, and they appear to be identical. Both sites facilitate the sale of stolen PII of U.S. citizens, including citizens living in the Middle District of

Florida. Moreover, both sites accept Bitcoin[2] as a method of payment. SSNDOB.CLUB was registered on or about January 2, 2015, by an anonymous email account. SSNDOB.WS was registered on or about November 4, 2015, by **ramashka@india.com**.

11. Moreover, we have obtained copies of several key pieces of infrastructure for both the SSNDOB.CLUB and SSNDOB.WS sites and, as detailed below, an analysis of these servers leads me to conclude that these sites are substantially the same and are controlled by the same individuals.

SSNDOBCLUB INFRASTRUCTURE

12. The SSNDOBCLUB infrastructure used multiple servers located at various datacenters in Cyprus, Ukraine, Latvia, and Switzerland. The SSNDOBCLUB websites contained PII sourced from multiple servers, including servers maintained by the administrators and servers apparently maintained by third parties. Investigators have obtained copies of many of the SSNDOBCLUB servers through Mutual Legal Assistance Treaty ("MLAT") requests. Investigators were able to perform a forensic analysis on those servers.

Webservers

[2] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

13. The SSNDOB.CLUB and SSNDOB.WS front-end webservers[3] were maintained on two different servers, at an IP addresses ending in .217 in Cyprus and another ending in .106 in Latvia, respectively.[4] Users interacted with these servers via their web browsers. Investigators obtained a copy of both servers via MLAT. Both servers had substantially identical database structures, with the exception of one additional table on SSNDOB.WS. Each server had a database that contained entries with over 1,600,000 PII records. The records were located in a table with the same table name and column headers, and included duplicate PII records. Approximately 70,705 PII records from the databases on both servers were for individuals located in the Middle District of Florida, based on state and zip code.

14. The SSNDOB.CLUB server had a payments table that revealed a sum of $3,582,728 deposited, with the first payment made to the site on or about April 29, 2015. The SSNDOB.WS server had a payments table that revealed a sum of $690,090 deposited, with the first payment made on or about November 12, 2015. Based on my training and experience, and my investigation to date in this case, the volume of purchases made on the SSNDOBCLUB websites

[3] The front-end webservers were the servers that generated the graphical interface clients used to log into and view the sites.

[4] These servers contained the front-end webservers, but each of these servers also contained a "backend" customer database for each respective site.

indicates that there are numerous buyer-conspirators working with the administrators operating the SSNDOBCLUB sites.

15. Both webservers were configured to provide scheduled notifications to certain Jabber accounts. For example, Jabber account **ldr.men@xmpp.ru** would receive messages approximately every 30 minutes. Each message contained a list of client accounts that had received bitcoin deposits in the prior 30 minutes, and the corresponding amount of deposit in bitcoin and USD, the current conversion rate (to USD), as well as the domain to which the deposit was made (SSNDOB.WS or SSNDOB.CLUB). In my training and experience, and my investigation to date in this case, only an administrator of such a site would routinely receive this type of information.

Backend Database

16. The SSNDOB.CLUB and SSNDOB.WS webservers both communicated with a server in Cyprus at an IP address ending in .93. Investigators also obtained a copy of this server via MLAT. This backend server contained a database set up similar to the ones on SSNDOB.CLUB and SSNDOB.WS. However, this database had significantly more PII; one table alone contained approximately 22,392,299 PII records. Approximately 688,052 PII records from the table are for individuals located in Middle District of

Florida, based on state and zip code. Another table, believed to show sales, revealed a sum of $1,701,608 deposited since on or about November 5, 2020.

Admin Server

17. In addition to the webservers and backend, the administrators maintained other servers as part of their infrastructure, including an administrative server in Cyprus at an IP address ending in .119. The admin server connected and authenticated to the SSNDOB.CLUB, SSNDOB.WS, and the Backend Database servers. Based on my training and experience, and my investigation to date in this case, it is likely that the administrators logged into the admin server as a "work server" to further obfuscate their locations and identities. Investigators also obtained a copy of this server via MLAT.

18. The forensic analysis of the admin server revealed that a Jabber client was installed on it with multiple active Jabber accounts, including **ldr.men@xmpp.ru** and **ramashka@jabber.dk**. The first Jabber communication on this server is from **ldr.men@xmpp.ru** and is dated on or about March 27, 2015. Based on my training and experience, and my investigation to date in this case, only an administrator of the site would have had access to a server of this type.

19. Multiple compressed files that each contained exactly one million PII records were found on the server. A check against the PII found on the

backend and SSNDOB.CLUB and SSNDOB.WS servers revealed that the PII was likely also included on those servers.

IDENTIFICATION OF CHYCHASOV AS AN SSNDOBCLUB ADMINISTRATOR

20. On or about May 25, 2020, the OCE deposited Bitcoin into a SSNDOB.CLUB-controlled bitcoin address to facilitate the purchase of PII from the site. On or about May 25, 2020, the OCE, while present within the Middle District of Florida, purchased stolen PII, including social security numbers, unauthorized access devices, on SSNDOB.CLUB belonging to 15 individual victims who, based upon the PII record detail, appear to reside, or have resided, in the Middle District of Florida.

21. My investigation to date has revealed that the SSNDOBCLUB sites do not provide refunds to customers. My investigation has also revealed that the SSNDOBCLUB administrators appear to be the only "sellers" on the site. Based on my training and experience, therefore, the only individuals receiving monetary transfers from the site would be administrators of the site.

22. Investigators performed blockchain analysis[5] on the bitcoin address where the OCE sent bitcoin to fund the OCE's SSNDOB.CLUB account. The

[5] Blockchain analysis is the process of inspecting, identifying, clustering, modeling and visually representing data on transactions occurring within cryptocurrency blockchains using specialized software. The companies that create this software analyze the blockchain in an attempt to identify the individuals or groups involved with bitcoin transactions. Specifically, these companies create large databases that group bitcoin transactions into "clusters" through analysis of data underlying bitcoin

OCE's deposit went into a bitcoin address associated with SSNDOB.CLUB that I will refer to herein as ADDRESS A.

23. Using blockchain research software, investigators determined that ADDRESS A was associated with approximately 4,248 other addresses, that I will collectively refer to as "SSNDOBCLUB WALLET". According to blockchain research software, between on or about August 2, 2017, and on or about October 12, 2021, the SSNDOBCLUB WALLET had received more than 989 bitcoin (approximately $19.2M USD on the dates of transfer).

24. The blockchain analysis revealed that approximately 19 transactions originating from the SSNDOBCLUB cluster totaling approximately 45.99 bitcoin (approximately $1.38M) were sent directly to a single account at HitBTC, a virtual currency exchange based in Chile.

25. Know Your Customer[6] ("KYC") records obtained from HitBTC revealed that the account that had received over $1M in bitcoin from the

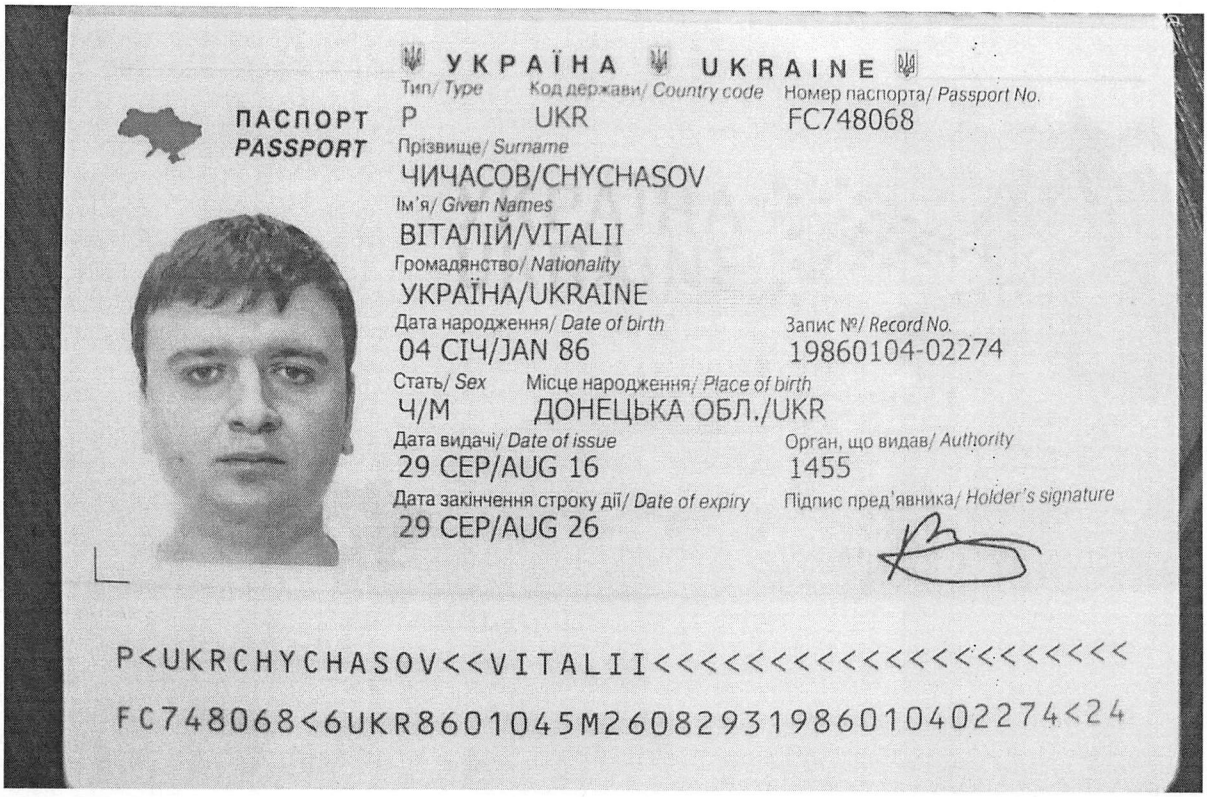
---

transactions. Through numerous unrelated investigations, law enforcement has found the intelligence provided by these companies to be reliable. This allows for law enforcement to utilize third-party blockchain analysis software to locate bitcoin addresses which transact at the same time (i.e., the blockchain logs transactions at same time by two different bitcoin addresses) and "cluster" these addresses together to represent the same owner. This third-party blockchain analysis software is an anti-money laundering software used by banks and law enforcement organizations worldwide. This third-party blockchain analysis software has supported many investigations, and has been the basis for numerous search and seizure warrants, and as such, has been found to be reliable.

[6] KYC guidelines in financial services require that professionals make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship. The procedures fit within the broader scope of a bank's anti-money laundering ("AML") policy. KYC processes are also employed by companies of all sizes for the purpose of ensuring their proposed customers, agents, consultants, or distributors are anti-bribery compliant, and are actually who they claim to be.

SSNDOBCLUB WALLET was registered to an individual named Vitalii CHYCHASOV using the email address petrporox@ukr.net. According to the HitBTC records alone, in calendar year 2019, CHYCHASOV earned approximately $33,462 from the sale of stolen social security numbers(which are unauthorized access devices), some of which belonged to Middle District of Florida victims; in 2020, he earned approximately $69,806 (from the sale of stolen social security numbers, some of which belonged to Middle District of Florida victims); and in 2021, he earned approximately $1,274,332 (from the sale of stolen social security numbers, some of which belonged to Middle District of Florida victims). From at least 2015, through the present, the SSNDOBCLUB sites were accessible from the Middle District of Florida.

26. CHYCHASOV provided a Ukrainian passport (FC748068) to authenticate the HitBTC account, which is displayed below.



27. HitBTC access logs revealed that an IP address ending in ..254 logged in or interacted with CHYCHASOV's HitBTC account on at least 20 occasions between on or about February 17, 2019, to on or about April 24, 2020. On at least 6 occasions, IP address .254 successfully authenticated via remote desktop to a SSNDOBCLUB infrastructure server with an IP address ending in .28 (located in Switzerland) between on or about January 4, 2020, and April 13, 2020. The IP address .254 geo-locates to Slavyansk, Donetsk Region, Ukraine, the same city in which CHYCHASOV resides. Investigators believe that CHYCHASOV logged into both his personal exchange account and

SSNDOBCLUB infrastructure from the same IP address located in the same city in which he resides.

28. Evidence collected supports the conclusion that CHYCHASOV also maintained an account at Bitfinex, a virtual currency exchange, with the username ramashka. KYC records from Bitfinex revealed the ramashka Bitfinex account had the email address ramashka@india.com and a Ukrainian phone number associated with it. The ramashka Bitfinex account received approximately 53.6 bitcoin (approximately $314,197 USD on the dates of transfer) directly from the SSNDOBCLUB WALLET from in or around August 2017, through in or around September 2018. The ramashka Bitfinex account received approximately $281,601 in 2017 and approximately $32,596 in 2018 from the SSNDOBCLUB WALLET.

29. Bitfinex provided access logs for the ramashka account. An IP address ending in .254 (the same IP also accessed CHYCHASOV's HitBTC account and a SSNDOBCLUB infrastructure server) accessed the ramashka Bitfinex account approximately 78 times between on or about August 29, 2017, through on or about September 5, 2018.

30. Ramashka@jabber.dk was an active account on the Jabber client software located on the SSNDOBCLUB Admin server. Investigators believe, based on the uniqueness of the moniker and receipt of funds directly from the

SSNDOBCLUB WALLET, that ramashka@jabber.dk is likely related to the individual controlling the ramashka Bitfinex account.

31. The SSNDOBCLUB Admin server also had a web browser installed on it. The web browser history included searches for one of the bitcoin addresses associated with the ramashka Bitfinex account as well as visits to a public blockchain software, blocktrail.com, to search for that bitcoin address and its transaction history.

32. **Ldr.men@xmpp.ru** was another one of the Jabber accounts active on the SSNDOBCLUB Admin server. As discussed above, the **ldr.men@xmpp.ru** Jabber account received automatic updates about buyer bitcoin deposits into SSNDOBCLUB at regular intervals. The SSNDOBCLUB Admin server also contained Jabber chat history for several other accounts including blackinfo@exploit.im and **ldr.men@xmpp.ru**. Furthermore, blackinfo@exploit.im was one of the Jabber handles listed as a support contact on the SSNDOB.CLUB website. The Jabber chat history of blackinfo@exploit.im revealed that on or about February 28, 2018, an unknown individual provided blackinfo@exploit.im with a new domain for UNICC, a widely known credit card shop, and asked for his login to the site. Blackinfo@exploit.im responded that the username "leaderok" was his login. Around the same time on or about February 28, 2018, **ldr.men@xmpp.ru** sent a message to an individual who the

investigation has determined is a coconspirator. The message appeared to contain the login and password credentials for the "leaderok" UNICC account. This supports the determination that blackinfo@exploit.im and **ldr.men@xmpp.ru** likely are controlled by the same person.

33. Additionally, investigators obtained customer records for an account named "leaderok" from a now-defunct virtual currency exchange known as Liberty Reserve. The "leaderok" Liberty Reserve account was registered using the name Vitaliy Chichasov. The account listed January 4, 1986 (Chychasov's true DOB) as the DOB and the email address vit-chichasov@yandex.ru.

34. I know, based on my training and experience, that individuals engaged in the type of criminal conduct described in this affidavit use their online monikers to gain notoriety in the cybercriminal space. These cybercriminals sometimes create monikers when they are younger and are less concerned about their operational security and the ability of law enforcement to link monikers to their true identities. That is one of the reasons why I believe ramashka, ramashka@jabber.dk, ldr.men@xmpp.ru, and leaderok are all likely controlled by CHYCHASOV. He may have created some of them a long time ago when he was likely less concerned about his criminal activities and the ability to link them to his true identity.

VICTIM INTERVIEWS

35. During the course of my investigation, I interviewed three victims, Victim D.B, Victim H.E, and Victim N.Y. Each victim is a resident of the Middle District of Florida and had their PII sold on the SSNDOBCLUB sites. Each victim confirmed that said victim did not provide his or her social security numbers to anyone to sell on the SSNDOBCLUB sites.

CONCLUSION

36. Based on the foregoing facts, probable cause exists to believe that Vitalii CHYCHASOV, in the Middle District of Florida and elsewhere, has violated the following statutes:

a. Count One: 18 U.S.C. § 371 (conspiracy to commit access device fraud) from in or around January 2015 through the present;

b. Counts Two through Four: 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices) for calendar years 2019, 2020, and 2021; and

c. Count Five: 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices) on or about May 25, 2020,

and therefore, I request this court issue a warrant for his arrest.

Justin R. Allen, Special Agent
IRS-CI

Subscribed to and sworn before me

This 28th day of October, 2021.

THOMAS G. WILSON
United States Magistrate Judge