UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America
v.
ARDIT FERIZI

Case No.3:21-mj-70014 MAG

Defendant(s)

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 October 2017 - February 2018 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1028A	Aggravated identity theft

This criminal complaint is based on these facts:

See attached affidavit of FBI Special Agent Dustin Reid

☑ Continued on the attached sheet.

Approved as to form /s/
AUSA William Frentzen

/s/ Dustin Reid via telephone
Complainant's signature

Dustin Reid, Special Agent, FBI
Printed name and title

Sworn to before me by telephone.

Date: 01/07/2021

Judge's signature

City and state: San Francisco, CA

Hon. Alex G. Tse, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Dustin Reid, hereby swear and affirm as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (hereinafter "FBI") and have been so employed since July 2009. I received law enforcement training from the FBI Academy at Quantico, Virginia. I am currently assigned to the Cyber Task Force in the FBI's Jacksonville Field Office. In the performance of my duties with the FBI, I have participated in federal criminal investigations involving terrorism, public corruption, violent crime, and cyber matters. I have received additional computer-related training and participated in cyber terrorism working groups. I have interviewed and debriefed numerous witnesses, confidential sources, and cooperating defendants. I have participated in the execution of numerous search warrants, including search warrants in cyber investigations.

2. Because this affidavit is provided for the limited purpose of a criminal complaint, I have not included all aspects of the investigation. Rather, this affidavit is intended to show merely that there is probable cause for criminal complaint. I am familiar with the following facts based upon my investigative activities as well as information I have obtained from other law enforcement officials in the United States (hereinafter "U.S.").

3. Ardit FERIZI, a Kosovar citizen, was first brought to the Eastern District of Virginia (hereinafter "EDVA"), from Malaysia, on January 22, 2016, on a criminal complaint charging him with violations of Title 18, U.S. Code (hereinafter "U.S.C.") Section (hereinafter "§") 2339B "Providing material support to a designated foreign terrorist group", Title 18 U.S.C. § 1030(a)(2)(C) "Unauthorized access to a computer" and Title 18 U.S.C. § 1028A "Aggravated identity theft". FERIZI was subsequently indicted on four counts which included conspiracy to provide material support to a designated terrorist group, in addition to the above-mentioned three offenses, on February 16, 2016.

4. On June 15, 2016, FERIZI pleaded guilty to two of the four offenses, which were providing material support to a designated foreign terrorist group and unauthorized access to a computer. FERIZI admitted that he unlawfully accessed a database belonging to a U.S. e-commerce company and culled the personally identifiable information (hereinafter "PII") which belonged to approximately 1,300 U.S. military and other government employees, who were identified through their use of "*.mil" and "*.gov" e-mail addresses. FERIZI then knowingly provided that PII to a Syria-based member of the Islamic State of Iraq and al-Sham (hereinafter "ISIS") named Junaid Hussain. At the time, Hussain served as a hacker, recruiter, and attack

facilitator for ISIS. Hussain published the PII in August of 2015 as part of a directive that ISIS supporters kill the named U.S. military members and other government employees. Hussain was subsequently killed in an airstrike.

5. On September 23, 2016, FERIZI was sentenced to 20 years of incarceration.

6. On October 6, 2020, a motion for compassionate release for FERIZI was denied.

7. On December 3, 2020, a second motion for compassionate release was granted and FERIZI's 20-year sentence was modified to time served with 10 years of supervised release in Kosovo. The motion was granted in part due to FERIZI's 2018 diagnosis of asthma and alleged obesity, as well as a COVID outbreak at one of the facilities where FERIZI was housed in 2020. As of January 7, 2021, FERIZI was 25 years old.

8. In the order granting FERIZI's release, it was noted that there is no doubt FERIZI committed a serious offense. The order also noted that even defendants who have committed very serious offenses can be appropriately released from custody or supervision where "[t]here is no indication that defendant poses a risk to the public and reducing the defendant's sentence to time served will not diminish the seriousness of his offense or the respect for the law." The order granting FERIZI's release further provided the U.S.

Probation Office found no evidence of any prior convictions, but conceded that the government acquired records from Kosovo, which were "never translated into English" that reflected FERIZI had been arrested for criminal offenses on multiple occasions in Kosovo in the past.

9. The FBI translated the record of FERIZI's charges in Kosovo prior to 2020. I am aware that there were approximately ten charges that had been referred for prosecution or were under investigation in regard to FERIZI's hacking activity from 2011 through 2013. Additionally, on December 18, 2020, I learned that an arrest warrant was issued for FERIZI in Kosovo on March 11, 2016, which expired after one year. I am further aware that FERIZI has attempted to flee prosecution twice. In late 2014 or early 2015, FERIZI's passport had been seized by the Kosovo Police due to pending charges against him, however FERIZI was able to fraudulently obtain a second passport and flee Kosovo for Malaysia. Additionally, I believe FERIZI was fleeing law enforcement action against him when he was detained by the Royal Malaysian Police at the Kuala Lumpur International Airport on or about September 15, 2015. When FERIZI was detained on or about September 15, 2015, approximately one month had passed since Hussain had published the kill list that targeted approximately 1,300 U.S. military and Government employees, which Hussain received from FERIZI.

10. After completing a 14-day quarantine, which ended on December 21, 2020, it is expected that FERIZI will be deported to Kosovo by the Department of Homeland Security. As of January 6, 2021, FERIZI was in custody in Pennsylvania awaiting deportation.

11. From April 2, 2017 to September 25, 2019, FERIZI was in the custody of the Bureau of Prisons (hereinafter "BOP"), housed at the Federal Correctional Institute in Terre Haute (hereinafter "FCI Terre Haute"), Indiana. During part of this time, FERIZI was authorized to send and receive e-mail communications.

12. On or about January 16, 2018, the FBI received information that alleged FERIZI was involved in criminal activity while incarcerated at FCI Terre Haute which is in the Southern District of Indiana. The FBI reviewed information from a BOP monitored telephone call from an inmate, who was an associate of FERIZI at FCI Terre Haute, wherein the inmate warned a female associate that FERIZI was using his family members to liquidate the proceeds of his previous criminal hacking activity. The inmate warned his female associate not to touch any money from FERIZI or she would be involved in his criminal conspiracy.

13. The FBI interviewed the female associate of the inmate on December 10, 2020, who advised that she had been contacted to create bitcoin

accounts for FERIZI and his brother [redacted] The female associate of the inmate advised that she did not assist FERIZI and [redacted] because she believed it would be illegal.

14. The FBI also interviewed the inmate on December 17, 2020, and he describe that FERIZI had been involved in multiple fraudulent schemes from prison in coordination with his brother [redacted], who was operating FERIZI's bitcoin accounts while FERIZI was incarcerated.

15. An FBI review of BOP monitored e-mails sent from FERIZI to [redacted] identified that FERIZI sent the messages "keep my e-mail alive and not expiring" to [redacted] on October 3, 2017. In the same October 3, 2017 e-mail, FERIZI provided [redacted] the e-mail address arditferizi95@gmail.com and the password [redacted] as well as approximately five other e-mails and passwords.

16. An FBI review of BOP monitored phone calls identified a phone call between FERIZI and [redacted] on February 26, 2018, in which [redacted] stated he had accessed the e-mail accounts given to him by FERIZI.

17. On January 5, 2021, the FBI identified from search warrant returns that on February 25, 2018, files were prepared to be downloaded from the arditferizi95@gmail.com e-mail account that included large databases of stolen PII. The databases included extensive lists of stolen e-mail accounts,

partial credit card numbers, passwords, and other PII. The FBI assesses that based on the Internet protocol (hereinafter "IP") address which resolved to Kosovo, additional login activity to FERIZI's other e-mail accounts, and the telephone call between FERIZI and [redacted] on February 26, 2018, [redacted] downloaded the databases of stolen PII which were the fruits of FERIZI's previous criminal hacking activity. FBI IP address analysis identified that the email from Google which advised the files were ready to download passed through Mountain View, California, which is in the Northern District of California.

18. Given the above information, it is apparent that FERIZI knowingly transferred a means of identification of another person and caused writings to be transmitted by means of wire in support of the criminal scheme.

II. RELEVANT LAW

19. I am advised that Aggravated Identity Theft, as described in Title 18 U.S.C. § 1028A provides:

> Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

20. I am advised that an enumerated felony violation in U.S.C. § 1028A (c)(5) is provided as:

> Any provision contained in chapter 63 (relating to mail, bank, and wire fraud)].

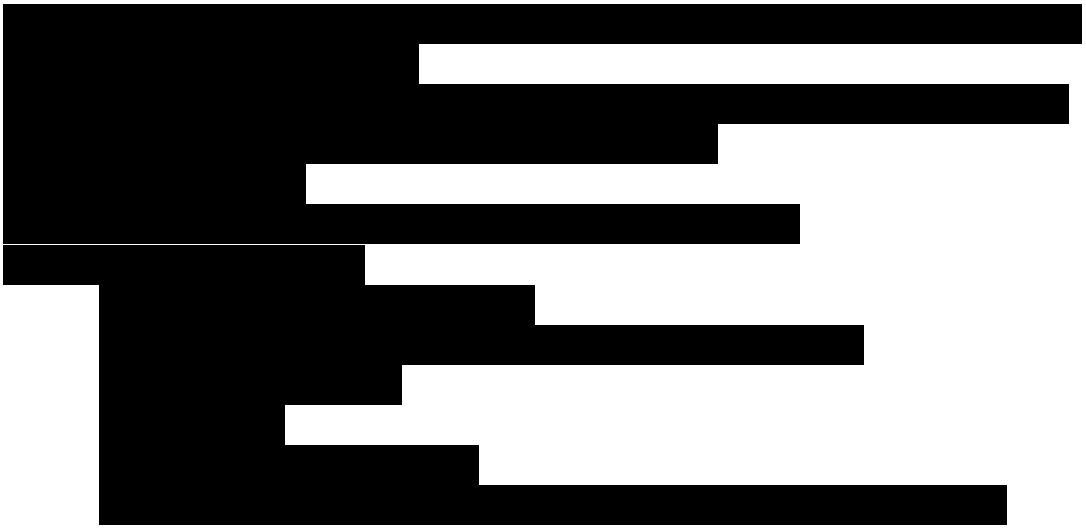
21. I am advised that Wire Fraud, as described in Title 18 U.S.C. § 1343 provides:

> Whoever, having devised 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 or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

III. STATEMENT OF PROBABLE CAUSE

A. 2017 CONSPIRACY FROM FCI TERRE HAUTE TO "CASH OUT" THE PROCEEDS OF FERIZI'S PAST CRIMINAL HACKING ACTIVITIES

22. On June 20, 2018, I reviewed the following information of monitored e-mail traffic, provided by BOP at FCI Terre Haute, which showed that FERIZI provided his brother [redacted] with e-mail and password information for FERIZI's accounts on or about October 3, 2017. In the e-mail to [redacted], who is believed to have been in Kosovo at the time, at [redacted]@gmail.com, FERIZI stated in substance "keep my e-mail alive and not expiring" and then FERIZI provided the following information to [redacted] regarding FERIZI's e-mail accounts and passwords:



23. In my training and experience, I am aware that e-mail service providers may close accounts due to extended periods of inactivity. I assess that FERIZI's message to [redacted] to keep the e-mail accounts "alive" indicated that he wanted [redacted] to sign into and access the accounts in order to preserve the data contained therein, which consisted of stolen databases of PII, further described below.

24. I reviewed documents from BOP at FCI Terre Haute that contained the translated transcripts of monitored phone calls involving FERIZI. In one phone call on or about February 26, 2018, FERIZI spoke with a male who FERIZI referred to as [redacted] or [redacted] which I believe to be FERIZI's brother [redacted]. During the conversation, [redacted] stated in substance "we have been able to open your e-mail".

25. On December 27, 2017, a BOP report identified that a phone call, which was monitored by BOP, was placed from an identified male inmate (hereinafter "MI") at FCI Terre Haute. During the phone call, MI spoke with an identified female individual (hereinafter "FI") who began the conversation by stating in substance that she had sent "those e-mails." MI responded in substance that MI and FI should not be involved in any business with FERIZI or use any money sourced from terrorism or child pornography. MI stated in substance that FERIZI told MI the information about where FERIZI's money came from on or about December 26, 2017. MI stated in substance that FERIZI confessed to him that FERIZI was "cashing out" from his crimes and using FERIZI's family members to do it. MI instructed FI in substance to gather any of the e-mails that she had access to regarding FERIZI's brother, who I assess to be a reference to [redacted] because FERIZI has only one brother. MI told FI in substance that if they were to touch any of the money from FERIZI, they would be involved in a criminal conspiracy with FERIZI. FI told MI in substance that she wished she had known this information before she sent the e-mail to FERIZI's brother. MI stated in substance that FERIZI's brother traveled to at least three or four countries liquidating everything as fast as he could. MI went on to tell FI in substance that FERIZI thinks he "pulled one over" on the U.S. Government. I note that

MI is serving a sentence of more than 20 years and was incarcerated at FCI Terre Haute as of December 17, 2020.

26. Based on my training and experience, the reference to FERIZI "cashing out" from his previous criminal activity likely refers to using thousands of sets of stolen PII, such as e-mails and passwords, to access victim PayPal accounts for criminal financial gain. This scheme is made viable due to the common practice of individuals using the same e-mail address and password to register accounts on multiple web sites, including PayPal.

27. PayPal is further described as a company in the U.S. that operates a worldwide online payment system that supports online money transfers and serves as an electronic alternative to traditional methods like checks and money orders. PayPal's corporate headquarters is located in the Northern District of California.

28. On December 10, 2020, I interviewed FI via telephone and FI provided the following statements in substance. FI recalled the phone conversation from December of 2017 in which MI warned her not to communicate with FERIZI because FERIZI was involved in terrorism and child pornography. FI recalled that, in the December 2017 phone call with MI, MI had warned FI that FERIZI was "cashing out" from criminal activity. FI conducted a search of her e-mails for the name of

FERIZI's brother, which was provided to her as [redacted] FI identified e-mails related to the incident beginning in or about October of 2017. FI described that she had been requested to open bitcoin accounts for FERIZI and [redacted]. FI believed FERIZI and [redacted] discussed FI opening Blockchain, Bitflyer, and Coinbase bitcoin accounts. FI advised that the e-mails occurred from approximately October 2017 through January of 2018. FI described that she believed the activity with FERIZI and his brother [redacted] was not legitimate, based in part on the use of bitcoin. FI stated that she did not continue assisting FERIZI and [redacted], as she did not want to risk her reputation by doing something illegal.

29. I understand that bitcoin is a type of digital currency, which operates independently of a central bank. Based on my training and experience, bitcoin is used by hackers because of its anonymity, as converting government-issued currency into bitcoin, sending, receiving, and converting bitcoin to government-issued currency does not require a verified identity. Coinbase and Bitflyer are cryptocurrency exchanges that act similar to banks for cryptocurrency. Coinbase is located in San Francisco and Bitflyer is located in Tokyo, Japan.

30. On December 11, 2020, FI voluntarily provided to the FBI an e-mail that she had sent to [redacted] at [redacted]@gmail.com on December

27, 2017 at approximately 11:07 AM. I assess that this is the same e-mail that FI had referenced on the BOP monitored telephone call with MI on December 27, 2017. The e-mail from FI to [redacted] contained the following message:

> I have been told to send you an email from the address to which you can send the user name and password for certain escrow accounts and then the escrow account information itself for the various accounts. Please send this information to the email from which this being sent.

31. Based on my training and experience, I know that escrow accounts are common in online criminal marketplace forums as they allow the sellers of stolen information to send the product to the escrow account while the buyer also sends the payment, such as a bitcoin payment, to the escrow account. Once the person operating the escrow account has confirmed the product and the payment have been received, the user of the escrow account will forward the product to the buyer and the payment to the seller.

32. On December 17, 2020, the FBI interviewed MI. In sum and substance, MI provided that FERIZI had a white iPhone 4 while incarcerated on which MI saw terroristic material and severed heads. MI provided the last name of the BOP officer that MI believed had brought in the iPhone for FERIZI to use. FERIZI wanted MI to pass information to FI regarding e-mail accounts that contained bitcoin so she could pass it to FERIZI's brother. MI believed that FERIZI had hundreds of millions of dollars in the form of

thousands of bitcoins in accounts that FERIZI's brother could access. MI stated FERIZI was a broker and claimed that FERIZI had a Dark web site to coordinate the sale of weapons, drugs, and children. I note that the Dark web, which is commonly used by hackers for online criminal marketplaces, is described as an area of the Internet that is intentionally hidden and may require specific software, configurations, or authorization to access. MI advised that FERIZI had a website that generated money from web traffic, but the primary purpose was to steal PII of people that clicked on the links. According to MI, after stealing information, FERIZI would set up money transfer accounts in the victim's name and hide money from deals he brokered. FERIZI had usernames and passwords to these fictitious accounts and wanted MI to pass information to FI in order for her to give it to FERIZI's brother. MI advised that FERIZI's brother was in charge of trading the bitcoin while FERIZI was incarcerated. MI further stated that in order to cash out the bitcoin, FERIZI's brother would go to overseas ATM machines, enter the encryption numbers, and convert bitcoin to cash. MI alleged that FERIZI's brother travelled to Germany, France, England, and Malaysia to liquidate the proceeds from their activities. MI saw one of FERIZI's accounts with $68,000 in it associated with the name [redacted]. MI advised that FERIZI would pass encryption codes to his brother through mailed letters

with codes in dots. MI advised that FERIZI traded Ethereum from prison and used Blockchain and Coinbase. I note that Ethereum is another type of virtual currency, similar to bitcoin. According to MI, FERIZI associated with former U.S. Secret Service Special Agent [redacted] (hereinafter [redacted]) while in prison and they both talked about how to hide their bitcoin. MI advised that FERIZI and [redacted] also talked about Ethereum transfers. MI further provided that FERIZI associated with convicted terrorists, including one with the nickname "Red".

B. CORROBORATION OF INFORMATION PROVIDED BY MI

33. On December 18, 2020, I identified former U.S. Secret Service Special Agent [redacted] was reported in a news article online (www.journals.sagepub.com) as having stolen $820,000 worth of bitcoin while investigating the Silk Road, which was a Dark web criminal marketplace, and that [redacted] funneled thousands of bitcoins from Silk Road to an account for himself. [redacted] later was convicted of stealing additional bitcoin from various seizures while working as a Secret Service agent. While forfeiture seizures against [redacted] known bitcoin were later carried out by the U.S. Government, I assess that this information partially corroborates the allegation from MI that FERIZI had access to thousands of bitcoins and was a broker on a website on the Dark web while incarcerated. On December 19,

2020, I was provided with BOP records showing that [redacted] was incarcerated at FCI Terre Haute from December 18, 2017 through February 20, 2019, which further corroborates the allegations made by MI as it shows [redacted] and FERIZI were at FCI Terre Haute at the same time.

34. I was advised on December 18, 2020, by BOP that FERIZI lost access to use of the FBI Terre Haute inmate e-mail system on or about December 13, 2017. This loss of the access for FERIZI to use e-mail on December 13, 2017 corroborates that he would attempt to find other ways to communicate for criminal purposes, such as using MI's e-mail access and FI's ability to communicate with FERIZI's brother without fear that BOP would monitor the communications. I note that the call from MI to FI warning her not to associate with FERIZI or his brother occurred on December 27, 2017. Additionally, the information that FERIZI lost access to inmate e-mail services on or about December 13, 2017, appears to corroborate an allegation from MI that FERIZI may have used "dot" codes in written mail to communicate with his brother in furtherance of a criminal conspiracy, as FERIZI no longer had access to e-mail [redacted]. FERIZI's extensive knowledge of computers, his proven hacking skills, and his offense involving his knowledge of computers, led to the BOP recommendation to have his computer access rescinded. The BOP document restricting FERIZI's access to

e-mail has standard language stating in sum and substance that inmates whose offense, conduct, or other personal history indicates a propensity to re-offend through the use of e-mail or jeopardize the safety, security, orderly operation of the correctional facility, or the public or staff, should be seriously considered for restriction.

35. According to the allegation by MI, a BOP staff member brought into the prison a white Apple iPhone 4 for FERIZI to use in furtherance of his criminal conspiracy. On December 18, 2020, BOP provided information regarding the first name and last name of an individual who had been an employee at FCI Terre Haute until 2020 whose last name matched the information provided by MI. The FBI interviewed the BOP staff member (hereinafter "BP1") on December 28, 2020. BP1 advised that he had regularly interacted with FERIZI at the Communications Management Unit (hereinafter "CMU") at FCI Terre Haute. BP1 advised that FERIZI associated with [redacted] and MI while at the CMU. BP1 stated in substance that he had not seen FERIZI involved in any criminal activity. BP1 stated in substance that he did not see FERIZI with a cell phone and had no knowledge of FERIZI ever having a cell phone while at the CMU. BP1 then provided that he had heard rumors that there was a cell phone in the CMU but BP1 never saw one. BP1 advised that MI told prison investigators that BP1 was

bringing in a cell phone to FERIZI. BP1 stated that he was investigated by the Special Investigative Service and they did not find any evidence that BP1 was bringing in a cell phone.

36. On December 17, 2020, I observed an FBI Special Agent (SA1), who specialized in investigations that involve violent crimes against children, access FERIZI's atubex.com website. In a Mirandized interview with the FBI on January 22, 2016, FERIZI admitted in sum and substance that he owned a pornography known as atubex.com. On December 17, 2020, the atubex.com website was found to contain pornography of an "age-difficult" nature and described itself in part as a "barely legal" pornography web site. SA1 attempted to access multiple videos which did not play when SA1 clicked on the hyperlinks to the videos. Instead of the videos playing, SA1 was redirected to other pornography websites. I assess that this information corroborates in part the allegation from MI that FERIZI was not interested in revenue from web traffic, but that FERIZI was interested in stealing PII from the victims that clicked on the links on his website as a part of a criminal conspiracy.

37. Additionally, FERIZI stated in sum and on substance during an FBI Mirandized interview on January 21, 2016 that FERIZI visited Malaysian prostitution houses every two or three days with a group of his friends. I assess that this information corroborates the allegation from MI that FERIZI

was involved as a broker for children or child prostitution in Malaysia. Further, I identified that Malaysia is known as a safe haven for child prostitution according to the Child Rights International Network (hereinafter "CRIN") which reported that Malaysia has seen an increase in child prostitution with an approximated average of 150 children being forced into the illegal industry every year. CRIN further described that child rights activists estimate that while some child victims in Malaysia are Malaysian, others come from Indonesia, Thailand, and India. CRIN also described that child rights workers advised these child sex victims do not work in brothels but are housed in dilapidated low-cost apartments and can cost as much as $100 U.S. dollars per child. I assess that FERIZI's description of visiting prostitution "houses" to the FBI further corroborates allegations by MI that FERIZI had the knowledge and ability to broker sales involving children and prostitution in Malaysia.

38. On December 18, 2020, BOP provided information that the person that MI identified as "Red" is [redacted] (hereinafter [redacted]). I identified that [redacted] is a convicted perpetrator of the 1993 World Trade Center Bombing who received a sentence of 240 years in prison without parole. BOP records show [redacted] was incarcerated at FCI Terre Haute from September 14, 2015 through December 2, 2019, which

shows that [redacted] was at FCI Terre Haute while FERIZI was also there. I assess the above information corroborates, in part, allegations made by MI regarding FERIZI.

39. Additionally, in the Mirandized interview with the FBI on January 22, FERIZI told the FBI he had a bitcoin wallet but never used it. FERIZI also advised he may have given the bitcoin wallet to some people, but he never received any money in the bitcoin wallet. I note that a bitcoin wallet is a private key or code that is known only to the person(s) in control of the bitcoin funds and essentially holds money in virtual way as if it were a physical wallet. I assess that FERIZI was minimizing his criminal activity and access to funds via bitcoin. I believe that FERIZI's admission to the FBI that he had a bitcoin wallet further corroborates in part the allegations from MI.

C. SEARCH WARRANT RETURNS FOR FERIZI'S E-MAIL ACCOUNTS FROM MICROSOFT AND GOOGLE

40. On January 4, 2021, I reviewed the results of a search warrant served to Microsoft for five of FERIZI's e-mail accounts, which was issued by the Northern District of California. In regard to the r00t3r-tgh@hotmail.com e-mail accounts belonging to FERIZI, I note that "r00t3r" is a hacking reference for gaining unauthorized "root" or administrative access and "tgh" likely refers to a criminal hacking group that FERIZI belonged to known as Team Grey Hat or TGH. From the search warrant, I identified that the e-mail

account r00t3r-tgh@hotmail.com received an e-mail on February 23, 2018 regarding a password reset that had been conducted with the IP address 185.67.177.15, which resolved to Pristina, Kosovo. I also identified that the password had been changed on the same date for the r00t3r-tgh@hotmail.com account. On February 25, 2018, I identified that the r00t3r-tgh@hotmail.com received an e-mail notification that a recovery e-mail address had been added as arditi-accounts@protonmail.com. Additionally, I identified that [redacted] was using the r00t3r-tgh@hotmail.com e-mail account due to an e-mail from "Riot Games" dated December 6, 2019, in which the username "Landerthebeast" appeared. I believe this information identified that [redacted], who used the nickname Lander, was the person who had accessed the r00t3r0tgh@hotmail.com account using IP address 185.67.177.15 on February 23, 2018, changed the password, and added the Protonmail encrypted e-mail address as a recovery e-mail option.

41. FBI investigation on December 29, 2020, identified that four of FERIZI's e-mail accounts had a new backup or recovery e-mail address which was partially obscured as ar*****@protonmail.com, which is consistent with the identification of arditi-accounts@protonmail.com identified in the Microsoft search warrant returns. I am aware that Protonmail is an encrypted e-mail system often used by hackers. The four accounts belonging to FERIZI

that had the Protonmail e-mail account listed as a recovery e-mail address were lajmetal@hotmail.com, r00t3r-tgh@hotmail.com, thedirectory@info.al, and ardit_kulleri_@hotmail.com. I asses that [redacted] created that Protonmail account and established it as a backup of recovery account for FERIZI's e-mail accounts in an effort to ensure [redacted] and FERIZI would be able to access the data contained in the accounts in the future.

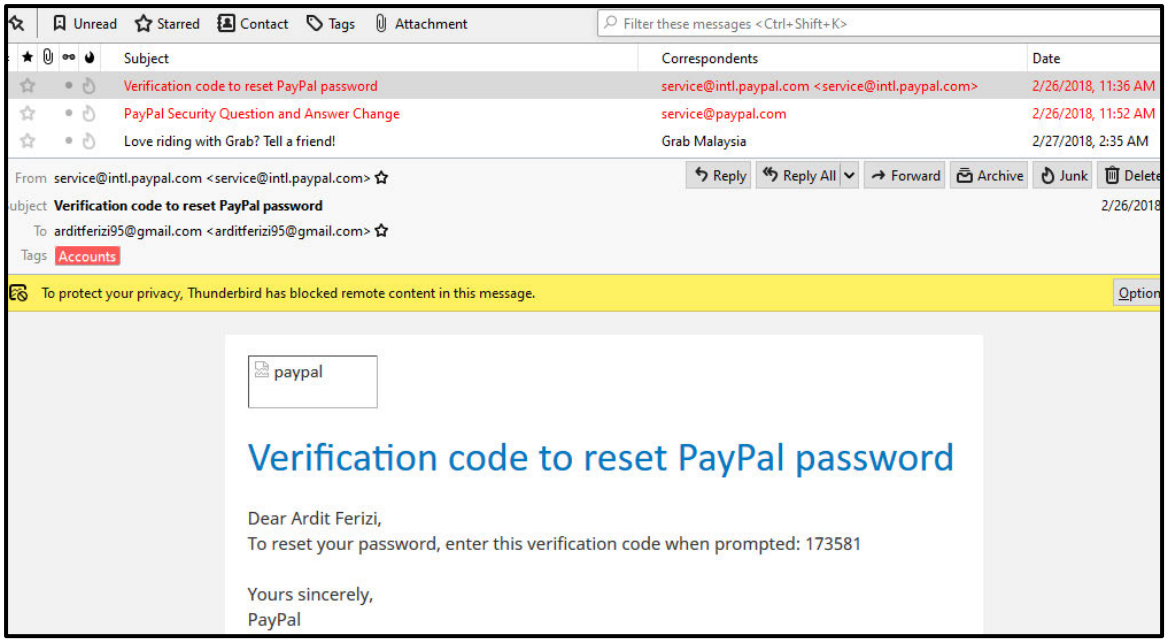
42. On January 5, 2021, I reviewed the results of a search warrant served to Google for FERIZI's e-mail account arditferizi95@gmail.com. I identified that beginning on February 23, 2018 and continuing through February 26, 2018, the following actions occurred. The e-mail account's password was changed, a spoofed e-mail was sent, a Google data archive was created, a PayPal account was reset, and PayPal security questions were changed. Displayed below are several emails that were found in the search warrant from Google for the arditferizi95@gmail.com account.

Subject	Correspondents	Date
Your password changed	Google	2/23/2018,
Security alert	Google	2/23/2018,
Verification code to reset PayPal password	service@intl.paypal.com <service@intl.paypal.com>	2/23/2018,
Review blocked sign-in attempt	Google	2/25/2018,
Security alert	Google	2/25/2018,
Access for less secure apps has been turned on	Google	2/25/2018,
Microsoft Outlook Test Message	Microsoft Outlook	2/25/2018,
Your Google data archive is ready	Google Download Your Data	2/25/2018,
Verification code to reset PayPal password	service@intl.paypal.com <service@intl.paypal.com>	2/26/2018,
PayPal Security Question and Answer Change	service@paypal.com	2/26/2018,

43. I note that hackers use e-mail "spoofing" to fraudulently impersonate another entity by appearing to be another entity in the "From" section of an e-mail in furtherance of criminal schemes. The spoofed e-mail with the title "Microsoft Outlook Test Message" was sent from arditferizi95@gmail.com to arditferizi95@gmail.com, on February 25, 2018, but had been spoofed to appear as if it originated from Microsoft Outlook. The IP address of the sender was 185.67.177.15, which resolved to Pristina, Kosovo, which I attributed to [redacted] per the above information. I believe that [redacted] was the person who sent the spoofed e-mail test, which demonstrated his abilities as a hacker involved in criminal fraudulent schemes. Based on the content of the telephone call between FERIZI and [redacted] on February 26, 2018, in which [redacted] told FERIZI he had accessed FERIZI's e-mail, as well as the IP address information, I believe [redacted] conducted all of the activity on the arditferizi95@gmail.com e-mail account between February 23, 2018 and February 26, 2018, including preparing all of the data with large databases of stolen PII to be downloaded.

44. Additionally, [redacted] appears to have taken steps to recover a PayPal account linked to the arditferizi95@gmail.com e-mail account, which I believe to have been for criminal "cash out" purposes, as described above in

allegations from MI. A screen capture of the e-mail from PayPal dated February 26, 2018 is displayed below.



45. I identified that multiple large databases of stolen PII, which were the fruits of FERIZI's previous criminal hacking activity, were prepared to be downloaded via Google Takeout tool by [redacted], FERIZI's brother. On February 25, 2018, an e-mail was received on the arditferizi95@gmail.com e-mail account which provided in sum and substance that the Google data archive was ready for download. I am aware that Google allows users to download all of their emails as well as the content of their Google Drive, which is a file storage area provided by Google, via the Google Takeout tool. I identified that the Google Takeout files, which included large databases of stolen PII, were available for download or about February 25, 2018 at 5:59pm.

I note that the Google Takeout tool must be initiated by a user and it does not occur on its own, which indicates that [redacted] used the Google Takeout tool in order to take the large databases of stolen PII.

46. On January 7, 2021, I identified that the e-mail dated February 25, 2018, from Google to arditferizi95@gmail.com titled "Your Google data archive is ready", passed through the IP address 209.85.220.69, which resolved to Mountain View, California in the Northern District of California.

47. One such database in the Google Takeout archive data was titled "Untitled Spreadsheet", located in the "hehe" folder, and contained 51 rows of what appeared to be stolen PII from Macy's customers. The stolen Macy's database included the e-mails, passwords, and partial credit card numbers of the victims. An image of the contents of the database is displayed below, with the e-mails and passwords of the victims redacted by the FBI.

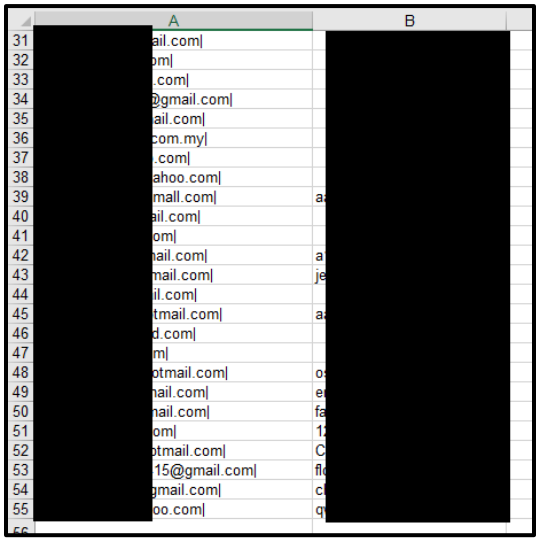
[Macy's American Express ® Card ********4161] |	http://www.macys.com/	[redacted]	
[Macy's Credit Card ********7670] |	http://www.macys.com/		
[Macy's Credit Card ********5160] |	http://www.macys.com/		
[Macy's Credit Card ********7500] |	http://www.macys.com/		
[Macy's American Express ® Card **********5136] |	http://www.macys.com/		
[Macy's Credit Card *******1810] |	http://www.macys.com/		
[Macy's Credit Card ********1871] [Macy's American Express ® Card **********4866] |	http://www.macys.com/		
[Macy's American Express ® Card **********1433] |	http://www.macys.com/		
[Macy's Credit Card ********4870] |	http://www.macys.com/		
[Macy's American Express ® Card **********6358] |	http://www.macys.com/		
[Macy's Credit Card *******9120] |	http://www.macys.com/		
[Macy's American Express ® Card **********5267] |	http://www.macys.com/		
[Macy's Credit Card **********0213] |	http://www.macys.com/		
[Macy's Credit Card ********4091] |	http://www.macys.com/		
[Macy's Credit Card ********1381] |	http://www.macys.com/		
[Macy's Credit Card ********9151] |	http://www.macys.com/		
[Macy's American Express ® Card ********9271] [Macy's American Express ® Card **********4102] |	http://www.macys.com/		
[Macy's American Express ® Card **********8617] |	http://www.macys.com/		
[Macy's Credit Card ********1191] |	http://www.macys.com/		
[Macy's Credit Card ********4861] |	http://www.macys.com/		
[Macy's American Express ® Card **********9728] |	http://www.macys.com/		
[Macy's Credit Card ********5790] |	http://www.macys.com/		
[Macy's American Express ® Card **********0047] [Macy's American Express ® Card ********3390] |	http://www.macys.com/		
[Macy's Credit Card ********6820] |	http://www.macys.com/		
[Macy's American Express ® Card **********8380] |	http://www.macys.com/		
[Macy's Credit Card ********4480] |	http://www.macys.com/		
[Macy's Credit Card ********4220] |	http://www.macys.com/		
[Macy's Credit Card **********4463] |	http://www.macys.com/		

48. On December 15, 2020, the FBI identified and interviewed three victims whose e-mail accounts, passwords, and partial credit card numbers, were contained in the e-mail account arditferizi95@gmail.com in the file that contained stolen PII for 51 Macy's customers. All three victims provided that the e-mail addresses and passwords in the stolen Macy's database were in fact used by them. All three victims confirmed that they had an account with Macy's. All three victims also provided that they had been further victimized by other instances of identity theft. One of the three victim interviews is further described below.

49. On December 15, 2020, the FBI interviewed a Macy's customer victim (hereinafter "MV1") who confirmed that the e-mail and password identified by the FBI belonged to her, which she used for an American Express Macy's credit card. MV1 advised that she no longer uses that e-mail account as she believes it was hacked about three years ago. MV1 believed her account had been hacked due to a large number of deleted emails, a large number of phishing e-mails asking her to reset her password, and e-mails requesting her to download software. MV1 advised that she experienced high levels of credit card fraud over the past four to five years and that she normally has to change her credit card numbers three to four times a year due to fraud.

50. The FBI also identified other databases that appeared to contain stolen PII that had been made privately available online by FERIZI to [redacted] via the Google Drive account associated with arditferizi95@gmail.com. Databases were identified with the label "#opisrael" that contained first name, last name, e-mail address, phone number, ID number, and address data for what appeared to be more than 17,000 victims. I subsequently learned that "Op Israel" is a reference to an annual coordinated cyber-attack where hacktivists target Israeli government websites and Israeli citizens. The "OpIsrael" cyberattacks include attempts to expose the PII of Israeli victims through the Internet. FERIZI admitted to the FBI in a Mirandized interview on January 22, 2016 that the purpose of the FERIZI's hacking group Pentagon Security Crew was to hack and conduct joint operations with Anonymous, such as "Op Israel."

51. The FBI also identified another database that appeared to contain stolen PII that had been made privately available online by FERIZI to [redacted] via the Google Drive account for arditferizi95@gmail.com. A database was identified with the label "Untitled spreadsheet" that contained what appeared to be 55 stolen e-mails and their corresponding passwords. An image of the data from the "Untitled spreadsheet" database is displayed below with the e-mail and password for the victims redacted by the FBI.



	A	B
31	[redacted]ail.com|	[redacted]
32	[redacted]om|	
33	[redacted].com|	
34	[redacted]@gmail.com|	
35	[redacted]ail.com|	
36	[redacted]com.my|	
37	[redacted].com|	
38	[redacted]ahoo.com|	
39	[redacted]mall.com|	a
40	[redacted]il.com|	
41	[redacted]om|	
42	[redacted]ail.com|	a
43	[redacted]mail.com|	je
44	[redacted]il.com|	
45	[redacted]tmail.com|	a
46	[redacted]d.com|	
47	[redacted]m|	
48	[redacted]otmail.com|	o
49	[redacted]ail.com|	e
50	[redacted]ail.com|	fa
51	[redacted]om|	1
52	[redacted]otmail.com|	C
53	[redacted]15@gmail.com|	fl
54	[redacted]gmail.com|	c
55	[redacted]oo.com|	q

52. The FBI also identified a database with the label "USA-Emails-Clean" that appeared to contain 438,334 rows of e-mail addresses that had been made privately available online by FERIZI to [redacted] via the Google Drive account for arditferizi95@gmail.com. In this database, I identified e-mail addresses that appeared to belong to U.S. Government employees which ended in the extensions "*usdoj.gov", "*hq.doe.gov", "*sanantonio.gov", "*flsenate.gov", "*sec.gov", "*gsa.gov", and "*noaa.gov".

D. [redacted] INVOLVEMENT IN FERIZI'S PAST HACKING ACTIVITIES

53. A search warrant was obtained, in EDVA, on or about September 13, 2015, for Facebook account 10003223062873, which was associated with FERIZI. A review of the search warrant return from Facebook of FERIZI's account (100003223062873) identified a private message conversation with [redacted], who used the Facebook account

with identification number 1599880614. The below messages, which were translated from Albanian to English by the FBI, were exchanged between FERIZI and [redacted] on September 7, 2015, wherein [redacted] proposes that FERIZI take 100,000 e-mail accounts that were exposed in a hacking operation in 2015.

From	Translated Message
[redacted]	Do you know how I thought of getting 100K emails?
[redacted]	There is a web Ashley Madison....Some people go to it to find bitches lol
FERIZI	Yes
[redacted]	Some hackers have made it public, 100K emails and they have said that they will make public another 40million if it doesn't get closed.
FERIZI	hahaha
FERIZI	I understand
FERIZI	Don't worry, we will look into it :)
FERIZI	(Y)
[redacted]	Because 1. No morals 2. You have lied to your clients that have paid to speak with women, but they talked to men. Hahaha 95% of them in that page were men.
FERIZI	Yes, yes I know!
[redacted]	And the 100K emails are public.
FERIZI	I have 200.
FERIZI	Brother:)
FERIZI	fresh (Y) and active:) (Y)
[redacted]	You can take /download them with Linux
[redacted]	Ok, I was just saying.
[redacted]	(Y)
FERIZI	:)
[redacted]	They made public,
[redacted]	27 million emails.
[redacted]	https://torrentz.eu/5d13c1a88a2bf85f3af0ab2cbe859dec208dc7e7
[redacted]	You have to pay to register in there.
[redacted]	Almost everyone in there is from Europe and America (USA).

54. I note that as a result of FERIZI providing the password to the arditferizi95@gmail.com e-mail account to [redacted] on October 3, 2017, [redacted] appears to have downloaded 438,334 e-mail accounts in a file named "USA-Emails-Clean" on February 26, 2018, which was identified the search warrant return from Google on January 5, 2021.

55. Additional reviews of search warrant return for FERIZI's Facebook account (100003223062873) identified that FERIZI had sent a list of approximately 100,001 rows of stolen e-mails and their corresponding passwords in a private message to himself. This is a common practice for hackers who want to be able to traffic in stolen PII for financial gain. The FBI reviewed the 100,001 set of login credentials and found that they were stolen by FERIZI from the identified victim company in the U.S. in 2015, through which FERIZI obtained the "*.gov" and "*.mil" e-mail addresses that he provided to ISIS.

E. FERIZI'S EXTENSIVE CRIMINAL HACKING HISTORY: 2010-2015

56. On January 21, 2016, FERIZI signed a Miranda waiver form and provided a voluntary statement to the FBI. In sum and substance, FERIZI informed the FBI that he created a Kosovar hacking group, known as Kosovo Hackers Security (hereinafter "KHS"), in 2010. FERIZI said KHS was created to counter Serbian hackers who at the time were attacking

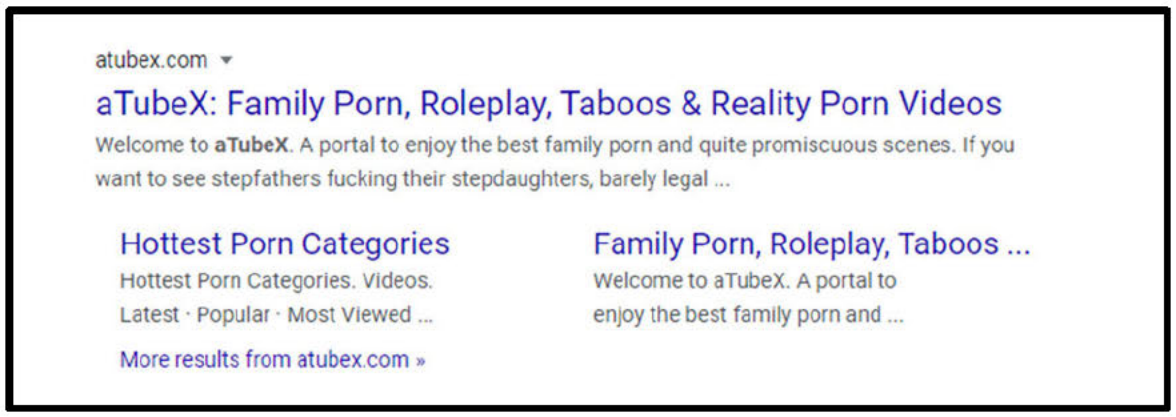
Kosovo-based websites. In 2010, FERIZI was still learning hacking skills and began conducting penetrations of Serbian Government and private websites. FERIZI said that he and another member of KHS conducted a cyberattack on the IBM research website.

57. FERIZI also told the FBI, on January 21, 2016, that he owned the website LeakedCure.com. FERIZI described LeakedCure.com as a healthcare website about diet and health that he used to make money off the Google advertisements. As described, FERIZI operated the website LeakedCure.com in order to generate revenue from Google advertisements. On December 13, 2020, I identified that LeakedCure.com was an operational website and that FERIZI's brother [redacted] has 62 posts on the website as an author. I note that it is common for hackers like FERIZI to use hacker tools, including their control of infected computers, to generate fake traffic to websites in order to fraudulently increase the revenue they can obtain from Google advertisements which are placed on the website. It is also common for hackers to place malicious code, such as cookie stealers to steal information from visitors to the website, as described above.

58. On January 22, 2016, FERIZI signed a second Miranda waiver form and provided a voluntary statement to the FBI. In sum and substance, FERIZI informed the FBI that FERIZI created several websites and attempted

to generate revenue from Google advertisements which included the websites atubex.com and l0cus.co.

59. FERIZI said that atubex.com was an adult pornography website he created, and he used a video stealer to post content. I identified that atubex.com is an active and functional web site as of December 16, 2020. I believe that the pornography website atubex.com may have been relevant to the aforementioned conspiracy identified by inmate MI regarding his statements that FERIZI was cashing out from hacking activity while FERIZI was in prison and that the source of his money was from terrorism and child pornography. A screen capture of the description of atubex.com is displayed below which included the definition that it hosts "barely legal" pornography. The screen capture was collected on December 16, 2020. A review by FBI personnel identified the website hosted age-difficult material, indicating that it was not immediately verifiable as child pornography.



60. In the FBI interview with FERIZI on January 22, 2016, FERIZI stated in substance the following information. FERIZI said that l0cus.co contained shared databases. I believe that FERIZI's use of the phrase "shared" databases is synonymous with "stolen" databases of PII that FERIZI made available online. FERIZI noted that another member of FERIZI's hacking group KHS named [redacted] (hereinafter "[redacted]") had administrative access to l0cus.co.

61. On September 10, 2015, the FBI identified the l0cus.co website was a hacking forum with forum topics on hacking, hacking tools, and stealing databases. A screen capture of l0cus.co dated September 10, 2015 is displayed below. I note that the "Last Post" in the "Accounts & Dumps" thread appears to be titled in substance "PayPal hacked by l0cus".

62. In the FBI interview with FERIZI on January 22, 2016, FERIZI advised that [redacted] utilized the hacker nickname "SkyNet". FERIZI said [redacted] was working on illegal activities, such as account checkers for stolen data for eBay, PayPal and financial web sites. FERIZI said the account checkers [redacted] used are made by Vietnamese programmers. After acquiring the checkers, [redacted] and others would then modify the account checkers for their own use. [redacted] had told FERIZI that he and others were hacking eBay accounts and using the access to purchase items. Also, FERIZI stated that [redacted] would use the account checkers to verify which stolen e-mail accounts were valid and then sell the valid accounts to other people on marketplace web sites.

63. A review of the search warrant for FERIZI's Facebook account (10003223062873) identified a private message exchange with [redacted] account (100008424857354) displaying their use of account checkers on stolen login credentials on August 5, 2015. The below image was redacted by the FBI to remove the victims' e-mail addresses, passwords, and address information. I note that the account checker appears to be named "Sykc0de" which may be a reference to [redacted] hacker nickname "SkyNet".

Facebook Business Record Page 9184

Body [sykc0de.org] Live =>[redacted]@yahoo.com | [redacted]1 | Mail: Die | Ebay: Live | Personal[US] | Verified | Fresh | $31.96 | PayPal New Look[+Joined in 2006+] | User Agent : iTunes/9.1 (Macintosh; U; PPC Mac OS X 10.2 | Checked on skyc0de.org at 7:48 am - August 5, 2015

Recipients [redacted](100008424857354)
Ardit Ferizi (100003223062873)
Author Ardit Ferizi (100003223062873)
Sent 2015-08-06 00:04:43 UTC
IP 110.159.108.196
Deleted false
Body 5

Recipients [redacted](100008424857354)
Ardit Ferizi (100003223062873)
Author Ardit Ferizi (100003223062873)
Sent 2015-08-06 00:04:44 UTC
IP 110.159.108.196
Deleted false
Body [sykc0de.org] Live =>[redacted]@aol.com | [redacted]1 | Mail: Uncheck | Ebay: Die | Personal[US] | Verified | $0.00 | No SMART | BMLT Credit : $1,500.00 | Have Bank | [DISCOVER - x6697 - Confirmed - 1/2019]-[VISA - x3222 - Confirmed - 8/2016]-[VISA - x9486 - Confirmed - 4/2018] | [redacted], [redacted]binghamton, NY 13903, United States | No Payment | PayPal New Look[+Joined in 2008+] | User Agent : Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html | Checked on skyc0de.org at 7:50 am - August 5, 2015

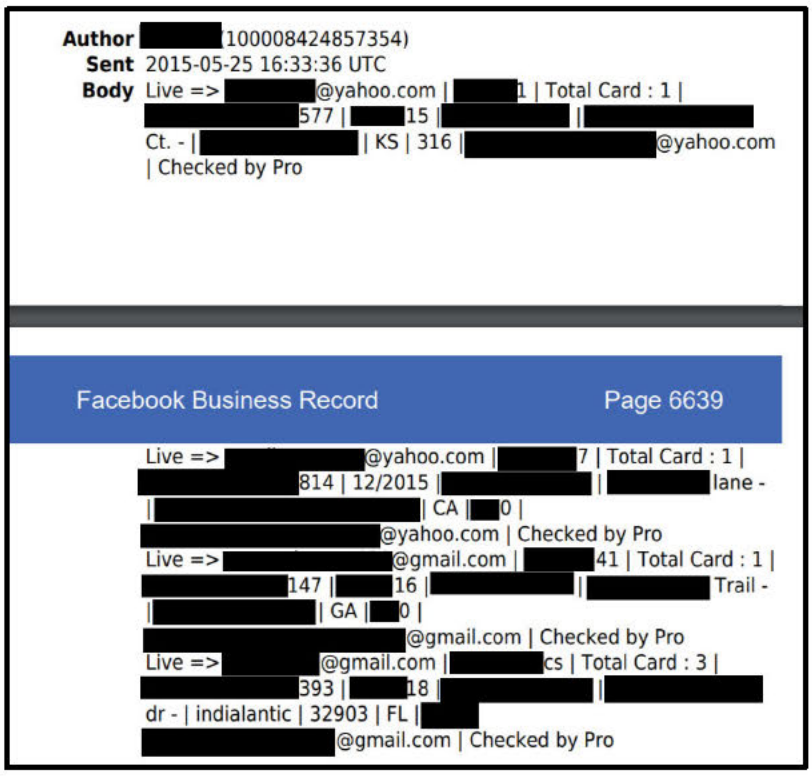
64. I understand, based on my training and experience, that an account checker allows a hacker, in a quick and automated way, to identify if a group of stolen login credentials from one website can be repurposed to unlawfully access the accounts of the same victims on other websites (i.e. PayPal, eBay, Amazon, and Facebook), based on the common practice of individuals using the same e-mail and password for multiple web sites.

65. On December 17, 2020, I identified 7 Facebook private messages exchanged between [redacted] and FERIZI in which they used a checker on a victim's stolen login credentials approximately 17 times between July 12, 2015

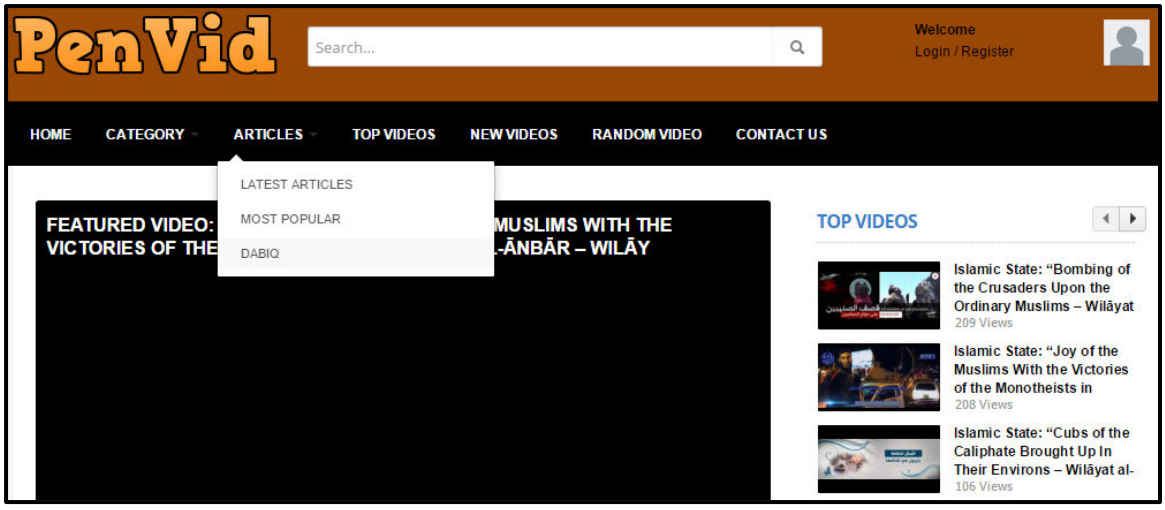
and August 23, 2015. I note that each of these instances is an attempt to gain unauthorized access to a victim's accounts.

66. On May 7, 2018, a search warrant for [redacted] Facebook account with identification number 100008424857354, was issued from the Middle District of Florida. On May 14, 2018, I identified 90 Facebook private messages in which [redacted] ran a checker on a victim's stolen credentials approximately 196 times. I note that each of these instances is an attempt to gain unauthorized access to a victim's online account, such as a PayPal account.

67. I identified one of the victims (hereinafter "V1") of the above account checker scheme and interviewed her on April 4, 2020. V1 stated in substance that she had experienced multiple instances of suspicious activity in regard to her financial accounts. V1 further described three events in which fraudulent purchases had been attempted against her Bank of America account. Displayed below is the account checker that [redacted] ran against V1's e-mail and password which identified 3 cards, which I believed to be credit cards, as well as a full credit card number. The below image was redacted by the FBI.



68. FBI investigation of FERIZI identified that he owned and operated the website Penvid.com, which hosted more than seventy official ISIS propaganda videos as well as Dabiq, the official online magazine of ISIS in 2015. FERIZI stated in substance on January 21, 2016 in a Mirandized interview with the FBI that his initial goal with Penvid.com was to make money from advertisements. In a Mirandized interview with the FBI on January 22, 2016, FERIZI admitted that he was aware that Dabiq magazine was hosted on his website. A screen capture of how the FERIZI's Penvid.com web site appeared in May of 2015 is displayed below.



IV. CONCLUSION

69. Based on the facts detailed above, I respectfully submit that there is probable cause to believe that from on or about October 3, 2017 and continuing through at least February 26, 2018, Ardit FERIZI:

a. Knowingly transferred, without lawful authority, a means of identification of another person as prohibited by Title 18 U.S.C. § 1028A; and

b. Knowingly devised a scheme to defraud, and for obtaining money and property by means of false and fraudulent pretenses that related to the material facts, and for the purpose of executing such scheme, transmitted or cause to be transmitted by means of wire communication in interstate and foreign commerce, writings as prohibited by Title 18 U.S.C. § 1343.

/s/ Dustin Reid via
telephone

Dustin Reid
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before
me this 7th day of January, 2021

HON. ALEX G. TSE
United States Magistrate Judge