IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	Case No. 3:24-mj-113
v.	)	
	)	AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION
NICOLAE-ADRIAN MĂRGĂRIT	)	
	)	
	)	

AGENT AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION OF NICOLAE-ADRIAN MĂRGĂRIT

I, Steele Holland, being duly sworn, depose and state:

1. I am a task force officer of the Federal Bureau of Investigation (FBI) assigned to the Richmond Division and detailed from the Virginia Department of State Police. I became a task force officer with the FBI in March 2015. I am currently assigned to the Cyber Squad within the FBI Richmond Division where I am primarily responsible for the investigation of cyber matters, which include computer-enabled criminal violations relating to computer enabled fraud designed to induce victims to wire money to criminally controlled bank accounts.

2. Before becoming a task force officer, I was assigned as a special agent with the Virginia Department of State Police starting in January 2014. In that role, I received and distributed intelligence material to appropriate parties and provided field support by way of actionable intelligence. Prior to my role as a special agent, I was a uniformed state trooper with the Virginia Department of State Police, beginning in January 2003. Throughout my employment as a police officer, I conducted criminal investigations and I have received many classes in basic and advanced criminal investigation techniques. As a task force officer with the FBI, I have received training in the investigation of cases involving computer crimes and the use of computers to advance criminal schemes.

3. As a task force officer of the FBI, I am authorized to conduct investigations, carry firearms, execute warrants, make arrests for offenses against the United States and perform other such duties as are authorized by the FBI. Through the course of these investigations, I have conducted interviews and secured other relevant information using a variety of investigative techniques.

4. This affidavit is submitted in support of a request by the United States for extradition of NICOLAE-ADRIAN MĂRGĂRIT (MĂRGĂRIT). In the course of my duties, I have become familiar with the evidence and the charges against MĂRGĂRIT. During the course of the investigation, I have, among other things, reviewed: law enforcement reports; computer, Internet, telephone, business, and bank records; and computer forensics evidence, which provided information concerning the criminal conduct of MĂRGĂRIT and his co-conspirators.

5. Below, I have set forth the evidence establishing each of the four counts in the criminal complaint pending against MĂRGĂRIT. I have not attempted to describe all of the evidence in the government's possession.

FACTS OF THE CASE

6. MĂRGĂRIT is a member of an international criminal conspiracy with other individuals located in the country of Romania, which has engaged in a variety of criminal activities, to include drug trafficking and cybercrime. MĂRGĂRIT has conducted cybercriminal operations for the group. The particular scheme under investigation here involved the targeting of online sellers with Amazon. Phishing emails were sent to Amazon sellers. In a sophisticated man-in-the-middle cyber scheme, the login credentials for victims' Amazon Seller Central accounts were compromised. MĂRGĂRIT then accessed these accounts, changed the financial account information for disbursements from Amazon to the sellers, and transferred the money

directly to offshore bank accounts in Romania, Greece, and Hungary. Information provided by Amazon revealed that over 600 seller accounts appear to have been accessed by the same perpetrators. The investigation is ongoing, and the loss amounts continue to grow as new victims are identified. To date, MĂRGĂRIT's scheme has resulted in more than $1.6 million in actual losses, and more than $3.6 million in attempted losses.

7. All internet traffic for accessing Amazon Seller Central accounts for U.S.-based sellers is routed through an Amazon server located in the Eastern District of Virginia.

8. In or around November 2020, the FBI began investigating a series of Amazon marketplace account compromises. The Amazon seller victims received phishing emails purportedly from Amazon Seller Notification, informing them that Amazon was unable to verify some of the information provided in their seller account. The email address for these phishing emails (e.g., seller-performance@8cnzvfen-amazon.com) was obscured by the use of alias email addresses. These emails instructed victims to log into their Amazon Seller Central account, locate the emergency notification section, and to enter a valid phone number. Once this was completed, they were to reply within 24 hours with a confirmation email and they would be sent a verification email to confirm the update as the principal account owner. Victims then received a second email that appeared to be from Amazon with a "Complete Review" button to confirm the update of their phone number. The "Complete Review" button contained a malicious hyperlink to a web page hosted on servers that MĂRGĂRIT and/or his conspirators leased with Newfold Digital, which is a U.S.-based internet hosting company.

9. The initial incident involved an internet merchant located in the Eastern District of Virginia, identified herein as "Seller No. 1," which sells toys on Amazon.com. Seller No. 1's owner and Chief Executive Officer determined that the company's Amazon marketplace seller

account was compromised and that a bi-weekly disbursement from Amazon.com for sales was redirected to an unknown bank account ending in -629. However, Amazon was later able to stop the disbursement and return the funds to Seller No. 1. The attempted losses due to the fraud were $176,469.62.

10. Seller No. 1 received two emails on or about November 17, 2020, sent to their business Gmail address. In the first message, allegedly sent by Seller Notification, seller-notification@www-amazon.com, they were informed that Amazon was unable to verify some of the information provided in their seller account. These emails instructed Seller No. 1 to log into their Amazon Seller Central account, locate the emergency notification section, and to enter a valid phone number. Once this was completed, they were to reply within 24 hours with a confirmation email and they would be sent a verification email to confirm the update as the principal account owner. The Reply-To address for this message appeared to be directed to Seller Notification. However, the actual email address was the phishing address seller-performance@8cnzvfen-amazon.com.

11. A few minutes later, Seller No. 1 received a message that appeared to be from the alias email address seller-performance@amazon.com, which obscured the actual address of seller-performance@8cnzvfen-amazon.com. A WHOIS[1] query at Centralops.net[2] for the "8cnzvfen-amazon.com" domain revealed that it resolved to IP address 66.96.147.105, which is an IP address that was used several times in the fraud scheme as discussed below. The mail

[1] WHOIS (pronounced "who is"), which stands for "who is responsible for this domain name," is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems, but it is also used for a wider range of other information.

[2] Centralops.net is a website that provides access to several free utilities, including WHOIS, for conducting internet research regarding internet domain names, IP addresses, and email addresses, among other things.

exchanger records indicating that email associated with this address should be directed to Google's email servers[3]. This message thanked Seller No. 1 for their confirmation email and instructed them to click on a "Complete Review" button in the email to confirm the update of their phone number as principal account owner. This button contained an embedded hyperlink that connected to a URL[4] that directed a user to a web page hosted on phishing servers controlled by the conspiracy. These messages were received, and the "Complete Review" button was clicked on, by a Seller No. 1 employee, which ultimately led to Seller No. 1's username and password for their Amazon Seller Central account being stolen. **This November 17, 2020 email to Seller No. 1 provides the basis for the wire fraud charge alleged in Count One of the Criminal Complaint.**

Expansion of the Investigation

12. Based upon information provided to investigators by Amazon, the owner of a business located in the Eastern District of Virginia – identified herein as "Seller No. 2" – was interviewed regarding the loss of $8,491.33. Seller No. 2 was also an Amazon seller targeted in the subject phishing scheme. On or about October 29, 2020, the owner received an email to his Gmail address from Seller Notification, seller-performance@2bv5bden-amazon.com. This email was similar in content to the first email received by Seller No. 1, requesting the input of a valid phone number and a confirmation reply message. The owner of Seller No. 2 responded to this email.

[3] Google permits users to register an email address having a domain name other than "gmail.com" or "google.com" and have Google provide email handling services for that address.

[4] URL is an acronym for "uniform resource locator," colloquially known as a Web address, and is a reference to a resource that specifies its location on a computer network and a mechanism for retrieving it. URLs most commonly reference specific web pages.

13. After responding, the owner received a second email on or about October 29, 2020, which appeared to come from Seller Notification. The actual email address, which was obscured by an alias email address, was seller-notification@2bv5bded-amazon.com. This email requested that Seller No. 2 verify his recent account changes by clicking on a "Begin Verification" button. The owner clicked on this link. The 2bv5bded-amazon.com domain resolved to IP address 66.96.147.105, the same IP address associated with the scheme that targeted Seller No. 1. The mail exchanger records for this address were also associated with Google.com. The "Begin Verification" button contained a similar malicious hyperlink designed to phish Seller No. 2's Amazon account credentials. **Seller No. 2's Amazon Seller Central account was unlawfully accessed on October 30, 2020, which provides the basis for the computer fraud charge alleged in Count Two of the Criminal Complaint.**

14. On or about December 10, 2020, December 17, 2020, and December 22, 2020, the Seller No. 2 owner received three additional emails from the subject(s). Each of these messages indicated that an issue had been found with Seller No. 2's Amazon Seller Central account and requested a reply to start the verification process. The contents of these messages were similar to the first emails received by both Seller No. 2 and Seller No. 1 and did not include buttons with hyperlinks. The December 10, 2020, and December 17, 2020 messages were allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To addresses for each was actually seller-performance@1cr4x7en-amazon.com. A WHOIS query at centralops.net revealed that this domain again resolved to 66.96.147.105 with Google.com providing email services. The December 22, 2020 email was also allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To address was actually

seller-performance@8cnzvfen-amazon.com, the same email address used for messages received by Seller No. 1.

15. Using the information connected to the Seller No. 1 and Seller No. 2 account takeovers, Amazon conducted an internal investigation to identify any other seller accounts targeted by the same actors. On January 28, 2021, Amazon provided an initial referral report to the FBI with identifiers for 622 additional seller accounts that appear to have been accessed by the same perpetrators. Of these accounts, 267 had their financial payment information changed at the time of the report, resulting in approximately $500,000 in additional fraudulent disbursements and over $2.2 million in attempted fraudulent disbursements.

16. Using the data obtained by the Seller No. 1 account, Amazon also provided investigators with certain attributes by which it could identify potentially related incidents. Those attributes included: (1) seller account access from IP address ranges 104.128.112.0–104.128.127.255 and 154.13.53.0—154.13.63.255; (2) target URLs that would allow the perpetrators to change email settings and view upcoming disbursements; and (3) account access from a new device not previously used by the legitimate account holder. The perpetrators first accessed the seller's account from one of the IP address ranges identified above. The perpetrators then visited the seller's accounts notification section and changed the email address used for account update notifications, often providing a new address that added an "l" to the beginning of the existing address on the account. The perpetrators also accessed the disbursement page, which details the amount and timing of any upcoming disbursements. Ultimately, the perpetrators changed the designated financial account for disbursements so that any future disbursements were paid to the financial account(s) of the subject(s).

17. On May 19, 2023, Amazon investigators reported that using the attributes described above, as well as data points exchanged between investigators and Amazon throughout the course of the ongoing investigation, the total losses to Amazon seller victims attributable to this scheme was $1,669,429.82, with an additional total recalled disbursements of $274,753.64 and total cancelled disbursements of $3,424,876.52. The aggregate amount of actual and attempted losses was thus $5,369,059.98.

18. In reviewing the account activity described above, the investigation revealed that the perpetrators often accessed and made changes to the seller accounts from Amazon Web Service or "AWS"-hosted Amazon Elastic Compute Cloud virtual machines (commonly referred to as EC2). As shown below, the use of EC2 is connected to MĂRGĂRIT. Each EC2 "instance" [5] is associated with an AWS account. In many of those cases, subjects would change information in the seller accounts, including updating financial account information, from the vantage point of the AWS services to avoid suspicious activity detection.

19. The investigation further revealed that the owner of Amazon Seller No. 3 received an email from seller-performance@1cr4x7en-amazon.com on February 11, 2021, stating that he was required to update his contact settings on his Amazon marketplace account or risk losing access to the platform. The email address seller-performance@1cr4x7en-amazon.com was the same address used to send a similar message to Seller No. 2. On February 11, 2021, the Seller No. 3 owner responded to the email stating that he updated his account. Records from Amazon

[5] One of Amazon Web Service's (AWS) most well-known products is called Amazon Elastic Compute Cloud (EC2) , and offers businesses the ability to run applications on the public cloud. A software "**instance**" is a separate copy of a software application or service that runs on the same infrastructure, typically servers, as other copies. Instances are created by duplicating the application's data and configurations, which allows multiple users to interact with the software independently.

indicate that on February 12, 2021, Seller No. 3's profile was accessed by IP address 154.13.55.109 three times over the course of two minutes. This IP address was part of the same suspect IP address range used in the Seller No. 2 compromise. Records from Amazon further indicate that the attacking IP address accessed the profile's payment account section. On February 18, 2021, Amazon sent a disbursement to a Hyperwallet account[6] with account number ending in 5617 in the amount of $29,126.53.

20. Further information provided by Amazon revealed that the owner of Amazon Seller No. 4 also had her account's payment section accessed by attacking IP address 154.13.53.12 over the course of two minutes on September 23, 2020. Records from Amazon further indicate that on November 6, 2020, November 20, 2020, and December 4, 2020, Amazon disbursed $17,833.81, $23,494.55, and $49,118.43 respectively to a Hyperwallet account with account number ending in 1848. This IP address was part of the same attacking IP address range in the Seller No. 2 and Seller No. 3 compromises.

21. Based on conversations with officials at Amazon.com with whom the FBI has consulted about this case, it appears that MĂRGĂRIT and/or his co-conspirators took steps to reduce attention from Amazon's security systems when accessing the Amazon seller victim accounts. MĂRGĂRIT and/or his co-conspirators leased eight accounts with AWS to run applications on the public cloud through the EC2 product. MĂRGĂRIT launched EC2 "instances" with Microsoft Windows operating systems (i.e., virtual Windows machines)

[6] Hyperwallet is a financial payment service owned by PayPal. Hyperwallet provides payment processing for a diverse collection of global industries. Hyperwallet enables its merchants (clients) to send payments to their customer base (payees) via virtual accounts and direct transfers. In virtual accounts, payees can choose how they want to withdraw money from Hyperwallet. These options include prepaid cards, Venmo transfers, PayPal transfers, checks, cash pickup, or donations. Hyperwallet is designed to facilitate the quick movement of money internationally.

and used those instances to access the Amazon seller accounts at issue. According to Amazon.com officials, accessing the victim accounts from within Amazon's infrastructure lowered the security profile of the conspirators' actions and helped avoid suspicious activity detection on Amazon's infrastructure.

22. The investigation has revealed that four of the AWS accounts used to launch EC2 instances were leased using email addresses that can be linked to or controlled by MĂRGĂRIT. For example:

a. One email address, mata82465@gmail.com, was used to register two AWS accounts. Records from Google show that mata82465@gmail.com was the recovery email address for another account, adypno@gmail.com. The adypno@gmail.com address was registered under the name "Adrian Nicolae" with a date of birth of December 4, 1984, which is MĂRGĂRIT's correct birthday.

b. Another AWS account was registered with adypv1@gmail.com. Google records for this account provide a recovery address of bocap@protonmail.com, which was the destination account to which the phished logon credentials were sent after being harvested by the conspiracy's CGIProxy servers.

c. Yet another AWS account was registered with detreaba112@gmail.com, which is linked to a laptop computer seized from MĂRGĂRIT and is discussed in paragraph 33 below. An email search warrant conducted on the detreaba112@gmail.com account, which is discussed in paragraphs 25 and 26 below, revealed that the email account contained a copy of the CGIProxy

software that was virtually identical to the version found on the Newfold Digital phishing servers and MĂRGĂRIT's laptop computer.

23. MĂRGĂRIT's servers with Newfold Digital ran a modified version of CGIProxy. Those servers are linked to MĂRGĂRIT's as discussed in paragraphs 33 and 34 below. CGIProxy is a publicly available software that can be used to create a web proxy server that allows users to access websites anonymously. After clicking the "Complete Review" button, the victim's web browser was routed to MĂRGĂRIT's CGIProxy server, which in turn would reach out to the legitimate Amazon Seller Central webpage to obtain and display that webpage to the victim's browser. After obtaining the Amazon Seller Central webpage, MĂRGĂRIT's script altered the HTML language[7] before displaying the page to the victim. Every link within the HTML language for the legitimate Amazon Seller Central webpage was altered so that they all pointed back through MĂRGĂRIT's phishing server to ensure the loop continued. When victims entered their username and passwords for their seller accounts, the phishing server would capture and harvest them. The phishing server would forward these credentials to the legitimate Amazon Seller Central server, which would return to the victim through the phishing server session cookies[8] for the connection. The phishing server

[7] Hypertext Markup Language (HTML) is the standard markup language for documents designed to be displayed in a web browser. It defines the content and structure of web content. In simple terms, it is the computer code used to build websites and webpages, and it tells a web browser how the webpage should be displayed on the computer user's web browser.

[8] A **cookie** is a small data file that a web server sends to a user's device while they are browsing a website. The user's web browser stores the cookie and sends it back to the server each time the user requests a new page from that website. Many cookies are persistent; they will remain on a user's computer even after the web browser is closed. **Session cookies**, also known as transient cookies, are temporary cookies that are deleted when a user closes their browser. Session cookies are used to store user-specific information during a single visit to a website, such as login credentials or items in a shopping cart.

also harvested the session cookies. MĂRGĂRIT's phishing script then wrote the victims' logon credentials, session cookies and IP address to a text file, which was emailed to bocap@protonmail.com. (This email is linked to MĂRGĂRIT through other evidence.)

24. Rather than changing the victims' payment information to traditional bank accounts located in the United States, for many victims' accounts MĂRGĂRIT used Hyperwallet account numbers. With other victims' accounts MĂRGĂRIT used banks located outside the United States. This obviated the need to recruit money mules to open U.S.-based bank accounts to initially receive the stolen money before attempting to move the funds overseas.

25. On April 19, 2021, a search warrant was executed for multiple Google email addresses associated with the AWS accounts used by the subject(s) to access the compromised Amazon seller accounts as well as the three email addresses used in the phishing emails (which were hidden by the alias email):

- seller-performance@2bv5bden-amazon.com
- seller-performance@1cr4x7en-amazon.com
- edelmira.salina.ruiz@gmail.com
- mata82465@gmail.com
- detreaba112@gmail.com
- adypv1@gmail.com

Subscriber information obtained from Google for email account adypno@gmail.com listed the subscriber for the account as "Adrian Nicolae," with a date of birth of December 4, 1984.

26. Results from this search warrant were received on or about April 22, 2021. A review of the account information provided by Google revealed that multiple Romanian IP addresses were used to login to these email accounts. Cyber criminals will employ aliases to trick their targets into believing they are sending an email to one address but are actually sending

it to another. One feature of Google's Gmail allows users to use alternate email addresses, which serves as a forwarding email address that a user adds to a user's primary email address. By using an alias email address, received emails will appear to be from the alias email address rather than the primary sending address. As previously mentioned, the seller-notification@1cr4x7en-amazon.com email address was used in the phishing attacks against Seller No. 2, Seller No. 3 and Seller No. 4.

27. Analysis of login IP addresses for phishing email addresses along with the other fraud-related accounts showed substantial IP address overlap, indicating that MĂRGĂRIT likely controlled all accounts. I know from my training and experience investigating cybercrime cases that IP addresses typically are not reassigned to different users within the span of a few minutes. It is common for static IP addresses such as these to remain assigned to the same online user for hours at least, and usually they remain assigned for periods of days. Thus, when multiple accounts are accessed from the same IP address within a matter of minutes, there is a strong inference that it was the same person accessing all of the accounts. Occasions when multiple accounts were accessed within a short timeframe from the same IP address, and from which we can infer that it was the same person doing so, are described as follows:

a. November 28, 2020, five email addresses were accessed from the same IP address during a 40-minute span.

b. January 15, 2021, six email addresses were accessed from the same IP address during a 27-minute span.

c. February 22, 2021, six email addresses were accessed from the same IP address during a 26-minute span.

d. March 7, 2021, six email addresses were accessed from the same IP address during a 9-minute span.

e. April 13, 2021, six email addresses were accessed from the same IP address during a 32-minute span.

Money Laundering and Conspiracy

28. Once Seller No. 2's Amazon seller central account was compromised and its deposit account changed to the Hyperwallet account ending in 2790, the funds were then transferred through Hyperwallet on or about November 12, 2020, to a Romanian-based ING bank account ending in 5979 in the amount of $8,491.33.

29. In addition to fraudulent funds being transferred to overseas bank accounts, the investigation also revealed multiple people acting in concert to avoid fraud detection and facilitate the seamless transfer of funds from the scheme. Search warrant production for the detreaba112@gmail.com account revealed the following email conversation with an account identified as georgenicoloiu16@gmail.com:

> *On Wed, Sep 16, 2020 at 2:17 PM george nicoloiu <georgenicoloiu16@gmail.com> wrote:*
>
> *I will send you something else from the NBG National Bank, around 8 this evening. It is a company registered to a [private] individual and it is very-very old and established. Up to 200 can be done easily.*
>
> *On Wed, Sep 16, 2020 at 2:05 PM Andy Passmore <detreaba112@gmail.com> wrote:*
>
> *Anyway, you are spot-on... because it has not really been working, almost not at all until now. Have a little patience, because it is going to be good.*
>
> *On Wed, Sep 16, 2020 at 3:57 AM george nicoloiu <georgenicoloiu16@gmail.com> wrote:*

Okay, poppy.

On Wed, Sep 16, 2020 at 1:46 PM Andy Passmore <detreaba112@gmail.com> wrote:

I am taking care [of it], but I am not rushing like last time... I was looking back, and we sent 700k in a rush and it did not work, because I rushed it. I am doing them nice and slow...
This time I want to stress you out, because you will have no place to get as many accounts as I want to. :))))))

On Tue, Sep 15, 2020 at 12:26 PM george nicoloiu <georgenicoloiu16@gmail.com> wrote:

Maybe you can do something faster, even if it is less, just like that, for starters, do you know what I am saying? We will see what happens, how it is... because as far as I know, those large ones are difficult. 🥺🥺🤦

On Tue, Sep 15, 2020 at 5:30 PM Andy Passmore <detreaba112@gmail.com> wrote:

Okay 😉

On Tue, Sep 15, 2020 at 7:25 AM george nicoloiu <georgenicoloiu16@gmail.com> wrote:

PIREUS BANK

SWIFT CODE
PIRBGRAA
IBAN:
GR32 0172 1870 0051 8709 9484 820

ION MARIN KAI YIOS EE (the name of the company)
DOMIKA YLIKA (what the company does)

Up to 300

30. According to records obtained by Hyperwallet and Amazon, the Greece-based Pireus account ending in 4820 shown above received an approximate total of $171,885.27 from six different amazon seller accounts between November 12, 2020, and November 30, 2020.

31. Records obtained from Hyperwallet showed that Hyperwallet accounts were used to transfer funds intended for Amazon sellers to accounts controlled by MĂRGĂRIT's conspiracy from at least September 30, 2020, through September 12, 2022. **This provides the date range for the money laundering conspiracy charge alleged in Count Three of the Criminal Complaint.**

The Romanian Investigation of MĂRGĂRIT

32. On May 28, 2020, officials from the Valcea regional office in Romania for the Directorate for Investigating Organized Crime and Terrorism (DIICOT) executed a search and arrest warrant on a residence where MĂRGĂRIT was residing that was associated with the organized criminal organization described in paragraph 6 above. The Romanian investigation revealed that MĂRGĂRIT obtained credentials of Amazon users through phishing activities. Subsequently, he gained unauthorized access to their user accounts and modified payment details, replacing the holder's account with a financial account facilitated by MĂRGĂRIT. As a result, when a good or service offered through Amazon was purchased, the money was sent to the accounts operated by MĂRGĂRIT's group members instead of the legitimate account of the Amazon seller. MĂRGĂRIT absconded before his trial started in that case.

33. U.S. law enforcement agents obtained copies of a laptop and two phones seized during MĂRGĂRIT's arrest from Romanian officials pursuant to a request for legal assistance. Analysis of the laptop showed the following:

a. A copy of CGIProxy that was remarkably similar (with only minor variations) to the version operating on the phishing servers hosted by Newfold Digital was present on the laptop. MĂRGĂRIT's version had clearly been customized to run the same phishing scheme and included script instructions directing that stolen victim account credentials be forwarded to bocap@protonmail.com, which was the same email address used by the CGIProxy phishing servers to forward stolen logon credentials.

b. Three Word document files were found on MĂRGĂRIT's computer that contained victim information and email addresses. Amazon confirmed that at least 27 of the emails belonged to victims of the phishing scheme.

c. Analysis of the laptop's memory ("RAM") identified 245 unique email addresses, 35 of which were also present in the search warrant returns for detreaba112@yahoo.com, detreaba112@gmail.com, seller-notification@8cnzvfen-amazon.com, and seller-notification@2bv5bden-amazon.com.

d. Analysis of the internet browser history from MĂRGĂRIT's laptop, which was reviewed in conjunction with business records obtained from Amazon.com, revealed that on May 6, 2020, he directly accessed the Amazon Seller Central account of a victim in this phishing scheme.

The 2023 Romanian Arrest of MĂRGĂRIT

34. In September 2023, DIICOT investigators again arrested MĂRGĂRIT. At the time of MĂRGĂRIT's arrest, DIICOT seized a laptop computer, thumb drive, and three smart phones, including a Samsung Galaxy. U.S. law enforcement authorities obtained copies of the

devices from Romanian authorities pursuant to a request for legal assistance. Analysis of devices revealed the following:

a. Laptop: The laptop computer's Microsoft Edge browser history revealed that it had been used to navigate to and access the Newfold Digital CGIProxy phishing servers. The laptop also contained an encrypted volume that was 900 GB. It has not yet been decrypted but is presumed to contain incriminating evidence.

b. Samsung Galaxy: The phone contained five session cookies associated with the domain amazon.com. Three of these cookies were created on February 3, 2023, and two of the cookies were created on January 2, 2023. The phone also contained nine emails associated with Amazon Seller Central accounts bearing substantial similarities to the fraudulent emails received by victims in the phishing scheme. A review of the web browser history from the Samsung Galaxy cell phone also revealed four connections to the CGIProxy phishing servers on January 2, 2023, and three connections to the CGIProxy phishing servers on February 1, 2023.

Wire Fraud and Conspiracy

35. The facts discussed in the paragraphs above show that MĂRGĂRIT's participated in the ongoing phishing scheme to defraud Amazon sellers from at least November 17, 2020, which was the date that Seller No. 1 received a phishing email, through February 3, 2023, which was the last date of session cookies from Amazon.com that were found on the Samsung Galaxy phone seized from MĂRGĂRIT by DIICOT investigators. **This provides the date range for the wire fraud conspiracy charge alleged in Count Four of the Criminal Complaint.**

IDENTIFICATION AND LOCATION

36. MĂRGĂRIT is a male with hazel eyes and brown hair. He was born on December 4, 1984. Photographs of MĂRGĂRIT are attached as Exhibit E to the affidavit of Assistant United States Attorney Brian R. Hood. MĂRGĂRIT is the holder of a Romanian passport, issued on May 4, 2018, with passport number 055776912. I have reviewed photographs of MĂRGĂRIT's Romanian passport and Romanian identification card. These photographs were discovered as saved files on the laptop seized from MĂRGĂRIT by DIICOT investigators in 2020. I have also reviewed a photograph of MĂRGĂRIT's taken from his Romanian arrest documentation, which is also attached as Exhibit E, and determined that this photograph matches the same person depicted in images of the passport and identification card found on MĂRGĂRIT's laptop computer.

CONCLUSION

37. This affidavit is sworn to before a Magistrate Judge of the United States District Court for the Eastern District of Virginia, who is a person duly empowered to administer an oath for this purpose.

Steele D. Holland

Steele Holland
Task Force Officer
Federal Bureau of Investigation

I certify that this is the original affidavit, sworn to and subscribed to before me on this 15th day of January, 2025 in Richmond, Virginia.

/s/

Hon. Summer L. Speight
United States Magistrate Judge
Eastern District of Virginia