

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 21-20084-CR-SCOLA/GOODMAN

UNITED STATES OF AMERICA

vs.

**SERGIO GIULIANI NITA,**  
a/k/a "juliensweiss,"  
a/k/a "giulonline,"

**Defendant.**

---

**AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION OF**  
**SERGIO GIULIANI NITA**

I, Jason P. Failing, being duly sworn, depose and state:

1. I am a Special Agent with the Internal Revenue Service Criminal Investigation ("IRS-CI"). The Internal Revenue Service ("IRS") administers and enforces the United States federal tax laws. As an IRS-CI Special Agent, I am responsible for investigating violations of U.S. federal criminal law, including violations relating to wire fraud, money laundering, and conspiracy. Currently, I am assigned to the IRS-CI Cyber Crimes Unit based in Washington, D.C. I have received training and gained experience in interviewing techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures.

2. I make this affidavit in support of the request of the United States of America to the Hellenic Republic for the extradition of **SERGIO GIULIANI NITA**, also known as "juliensweiss," also known as "giulonline" (hereinafter, **GIULIANI NITA**).

3. In the course of my duties, I have become familiar with the evidence and the charges against **GIULIANI NITA**. During the course of the investigation, I have, among other things, conducted interviews, reviewed law enforcement reports, and analyzed computer, Internet, telephone, business, and bank records, which provided information concerning the criminal conduct of **GIULIANI NITA** and his co-conspirators.

4. Below, I have summarized the evidence establishing each of the three counts in the Indictment charging **GIULIANI NITA**.

### **FACTS OF THE CASE**

#### **Overview**

5. Since 2015, U.S. law enforcement agencies, led by IRS-CI, have been investigating a sophisticated, large-scale stolen identity tax refund fraud scheme. This scheme, which involved a coordinated attack on an IRS computer system, utilized various money laundering networks that were previously established and operating before this particular scheme occurred.

6. The investigation revealed that between approximately August 2013 and February 2016, **GIULIANI NITA** partnered with other cybercriminals to: steal U.S. taxpayers' identities; file tax returns in U.S. taxpayers' names using their stolen personal identification information ("PII"); and launder the fraudulently obtained tax refunds. To that end, **GIULIANI NITA** and his associates, including Co-Conspirator 1—a previously convicted cybercriminal—created a number of shell companies and financial accounts in the names of identity-theft victims, then used those companies and accounts to receive and transfer stolen tax refund monies.

#### **IRS Data Breach**

7. The IRS provides an online service called "Get Transcript," which enables taxpayers to access their own tax data over the Internet. A taxpayer who wishes to obtain online

access to their tax data must create an account on IRS's website. To create the account, the taxpayer must first provide certain personal information, including the taxpayer's name and email address. The IRS then sends a confirmation code to the email address provided. The taxpayer must retrieve that code, enter the code on the IRS website, and successfully complete additional identity authentication steps in order to complete the account setup process. The additional identity verification steps include providing additional PII, such as date of birth and Social Security number, and correctly answering certain questions which are based on the taxpayer's credit history. Once the account is created, the taxpayer can access his or her tax data for the preceding four years.

8. On or about May 14, 2015, IRS personnel noticed that certain IRS mail servers had "queued" approximately 27,000 emails. Emails normally become queued when there are too many scheduled to be sent simultaneously or if the domain server for which the emails are destined is not active or does not exist. The long queue triggered a system alert requiring review by the IRS's Computer Security Incident Response Center ("CSIRC"), which is responsible for investigating unusual activity on the IRS's computer network. CSIRC personnel found that the approximately 27,000 emails all originated from `irs.online.services@irs.gov`, which is the IRS email account that sends automatically generated confirmation codes to taxpayers who are attempting to create user accounts for the Get Transcript service described above.

9. Investigators discovered that between on or about January 1, 2015, and on or about May 14, 2015, there were more than 224,000 suspicious attempts to obtain a confirmation code from the IRS in order to ultimately obtain access to the Get Transcript service. Investigators discovered that these 224,000 attempts to create IRS accounts originated from a relatively small number of obscure email domains such as "flurred.com"—a highly unusual pattern that ultimately revealed a fraudulent scheme to steal taxpayer records. Of the approximately 224,000 attempts,

approximately 113,000 were successful; that is, approximately 113,000 Get Transcript accounts were created, which enabled the account creators to steal U.S. taxpayer information.

10. Since discovering these account takeovers, the IRS has identified approximately 17,000 suspicious tax returns for tax year 2014. All of these returns are believed to be fraudulent because they were filed (a) in the names of taxpayers for whom Get Transcript accounts were created from one of the small number of obscure email domains discussed above and (b) after the suspicious Get Transcript accounts were created. In total, the perpetrators of the above-described scheme fraudulently claimed IRS tax refunds totaling over \$50 million USD.

**Tracing of Fraudulently Obtained Tax Refunds**

11. Of the approximately 17,000 suspicious tax returns, approximately 7,700 filers provided directions to the IRS to send tax refunds, totaling approximately \$25 million USD, to Green Dot, a company that provides financial services, including pre-paid debit cards and corresponding online financial accounts. Of that approximately \$25 million USD, approximately \$4 million USD was successfully deposited into Green Dot accounts. Subsequently, as described in the table below, that money was sent to the following eight shell companies via Green Dot’s “Bill Pay” function, which allows Green Dot account holders to generate and mail paper checks to vendors in any amount up to \$1,500 USD:

Company Name	Bill Pay Checks Received/Issued
FLV Mobile Solutions LLC	\$1,887,675.00 USD
Supra Auto Services LLC	\$1,380,617.00 USD
JT Digital Doctors LLC	\$881,485.00 USD
TJ Electronic Supplies LLC	\$218,589.00 USD
DJ Digital Experts LLC	\$115,357.00 USD
Fresco Web Design LLC	\$98,905.00 USD
Joslin Home Improvement LLC	\$98,192.00 USD
SCT Mechanics LLC	\$81,854.00 USD
Total:	\$4,762,674.00 USD

12. The paper Bill Pay checks mailed to the above-listed eight shell companies were sent to various mailbox addresses located throughout the country, including in the Southern District of Florida, within the State of Florida. Specifically, the checks were mailed to mailbox addresses controlled by a company called Mailbox Forwarding, an entity which provides customers with mailing addresses and various mailbox-related services. One of the services Mailbox Forwarding offers is to receive and scan pieces of mail on behalf of its customers. The scanned images are then uploaded to an online platform and made available to customers. Customers can also request that Mailbox Forwarding deposit any checks received by mail directly into a bank account of their choosing. Based on records provided by Green Dot and Fiserv—the company that partners with Green Dot to provide the “Bill Pay” service—the checks used to further transfer the fraudulently obtained tax refunds were delivered to Mailbox Forwarding and subsequently deposited into shell company bank accounts controlled by **GIULIANI NITA** and his co-conspirators. A description of the eight shell companies and their corresponding bank accounts follows:

- a. FLV Mobile Solutions LLC was registered with the Florida Department of State on or about August 12, 2013 at address 2000 Ponce De Leon Blvd., Suite 600-37, Coral Gables, Florida 33134 with D.J. listed as the managing member. Bank of America account x2115 in the name of FLV Mobile Solutions LLC and account holder D.J. was opened on or about September 11, 2013. According to Bank of America records, this account received approximately 1,882 Bill Pay checks totaling approximately \$1,887,675 USD during the time period on or about January 22, 2015, through on or about May 19, 2015.
- b. Supra Auto Services LLC was registered with the Florida Department of State on

July 23, 2013 at address 75 North Woodward Ave. #82871, Tallahassee, Florida 32313 with F.J. listed as the managing member. Bank of America account x7555 in the name of Supra Auto Services LLC and account holder F.J. was opened on or about July 31, 2013. According to Bank of America records, this account received approximately 1,380 Bill Pay checks totaling approximately \$1,380,617 USD during the time period on or about January 15, 2015, through on or about May 15, 2015.

- c. Bank of America account x0164 in the name of JT Digital Doctors LLC and account holder T.J. was opened on or about July 22, 2014. According to Green Dot and Fiserv records this company was issued approximately 752 Bill Pay checks totaling approximately \$881,485 USD during the time period on or about February 23, 2015, through on or about May 15, 2015.
- d. TJ Electronic Supplies LLC was registered with the New York Department of State on November 25, 2013 at address 187 Wolf Road, Suite 101, Albany, New York 12205 by Business Filings Incorporated. Bank of America account x7125 in the name of TJ Electronics Supplies LLC and account holder T.J. was opened on or about May 12, 2014. According to Green Dot and Fiserv records this company was issued approximately 186 Bill Pay checks totaling approximately \$218,589 USD during the time period on or about March 12, 2015, through on or about May 12, 2015.
- e. Bank of America account x7337 in the name of DJ Digital Experts LLC and account holder D.J. was opened on or about December 15, 2014. According to Green Dot and Fiserv data this company was issued approximately 96 Bill Pay

checks totaling approximately \$115,357 USD during the time period on or about March 24, 2015, through on or about May 12, 2015.

- f. Fresco Web Design LLC was registered with the Florida Department of State on or about July 31, 2013, at address 123 Southeast 3rd Ave., Suite 400, Miami, Florida 33131 with F.J. listed as the managing member. Bank of America account x2063 in the name of Fresco Web Design LLC and account holder F.J. were opened on or about February 23, 2015. According to Green Dot and Fiserv records this company was issued approximately 84 Bill Pay checks totaling approximately \$98,905 USD during the time period on or about March 20, 2015, through on or about May 12, 2015.
- g. Joslin Home Improvement LLC was registered with the Florida Department of State on or about July 24, 2013 at address 2637 East Atlantic Blvd. #26245, Pompano Beach, Florida 33062 and listed R.J. as the managing member. Bank of America account x4472 in the name of Joslin Home Improvement LLC and account holder R.J. was opened on or about February 17, 2015. According to Green Dot and Fiserv records this company was issued approximately 84 Bill Pay checks totaling approximately \$98,192 USD during the time period on or about March 25, 2015, through on or about May 12, 2015.
- h. SCT Mechanics LLC was registered with the Florida Department of State on or about September 3, 2013 at address 23150 Fashion Dr., Suite 232, Estero, Florida 33928 and listed S.K. as the managing member. Bank of America account x0812 in the name of SCT Mechanics LLC and account holder D.S.K. was opened on or about September 11, 2013. According to Bank of America data this account

received approximately 50 Bill Pay checks totaling approximately \$81,854 USD during the time period on or about March 4, 2015, through on or about March 13, 2015.

13. From the population of approximately 17,000 suspicious tax filings referenced above, U.S. law enforcement officers interviewed approximately 100 taxpayers. These interviewees confirmed that they were victims of identity theft and that they had not filed the suspicious tax returns received by the IRS and which resulted in refund monies being sent to Green Dot accounts opened in the victims' names.

14. Additionally, interviews with the purported incorporators, officers, and bank account holders of and for the eight shell companies identified above, including D.J., F.J., and S.K., revealed that those persons were not involved in the creation of the shell companies or the corresponding bank accounts. U.S. law enforcement officers later confirmed, based on their discovery of stolen identification documents on Co-Conspirator 1's electronic devices, that these purported incorporators were themselves victims of identity theft.

15. According to Bank of America records, at least two of the eight previously listed shell companies, FLV Mobile Solutions LLC and Supra Auto Services LLC, transferred large sums of money to Latvian bank accounts tied to Co-Conspirator 1, who is described further below, and a member of his family. For example,

- a. FLV Mobile Solutions LLC sent approximately twenty-two wire transfers totaling approximately \$1,684,040 USD from Bank of America account x2115 to Regional Investment Bank account x8500 in Latvia in the name of Norvale Universal LLP during the time period on or about February 18, 2015, through on or about May 18, 2015.



- b. Supra Auto Services LLC sent approximately ten wire transfers totaling approximately \$621,357 USD from Bank of America account x7555 to Regional Investment Bank account x4460 in Latvia in the name of Delbrand Merchants Corp during the time period from on or about February 25, 2015, through on or about May 1, 2015.
  
- c. According to Bank of America records, account x5153 in the name of name V Auto Group LLC was opened in the names of Co-Conspirator 1 and Co-Conspirator 2 (a member of Co-Conspirator 1's immediate family). Bank of America account x5153 was opened on or about August 20, 2008. This account received numerous international wire transfers from Norvale Universal LLP and Delbrand Merchants Corp, which maintained the Latvian bank accounts described in the preceding two paragraphs. Account x5153 in the name of V Auto Group LLC received approximately seven wire transfers totaling approximately \$1,248,085 USD from Regional Investment Bank account x8500 in the name of Norvale Universal LLP during the time period on or about March 20, 2015, through on or about May 14, 2015.
  
- d. According to Bank of America records, account x5153 in the name of V Auto Group LLC received approximately six wire transfers totaling approximately \$286,880 USD from Regional Investment Bank account x4460 in the name of Delbrand Merchants Corp during the time period on or about February 23, 2015 through on or about March 17, 2015.
  
- e. According to Bank of America records, account x5153 in the name of V Auto Group LLC sent approximately \$2,005,970 USD to several accounts held by Co-

Conspirator 2 in the United States and Russia during the time period on or about March 9, 2015, through on or about August 7, 2015.

- f. According to additional bank records, Co-Conspirator 2 sent approximately \$993,036 USD to two Russian bank accounts opened by Co-Conspirator 1, during the time period on or about March 17, 2015, through on or about May 15, 2015.

#### Co-Conspirator 1

16. Co-Conspirator 1 is a previously convicted cybercriminal who was charged in or around 2008 in the Eastern District of New York with access device fraud for laundering proceeds of a cyber-attack against a United States financial institution. Co-Conspirator 1 pleaded guilty to the charges.

17. On or about May 22, 2014, Co-Conspirator 1 was arrested by the New York Police Department while transporting an accomplice to various Automated Teller Machines (ATMs) for the purpose of withdrawing tax refund fraud proceeds.

18. During a voluntary interview conducted by U.S. law enforcement on or about May 22, 2014, Co-Conspirator 1 admitted that he was an active participant on various Russian-language cybercrime forums, including Verified and Mazafaka, where professional cybercriminals interact and offer to provide services to one another for pay.

19. Co-Conspirator 1 also admitted his participation in tax refund fraud and provided law enforcement with the online aliases or "monikers" of individuals he was working with to conduct this activity. During the interview, Co-Conspirator 1 admitted he transferred tax refund fraud proceeds to Bank of America accounts he created using fake documents. Co-Conspirator 1 also admitted having numerous pre-paid cards in his residence that bore the names of other individuals.

20. On or about May 23, 2014, Co-Conspirator 1 provided law enforcement with written consent to search his residence, located in Brooklyn, New York City, within the State of New York. During the search, law enforcement obtained numerous electronic devices, including laptop computers, hard drives, thumb drives, pre-paid debit cards, and various Magnetic Swipe Readers (“MSR[s]”). Based on my knowledge, training, and experience, MSRs are often utilized by cybercriminals who are involved with access-device and other fraud schemes.

21. On or about May 23, 2014, Co-Conspirator 1 was released from police custody. On or about May 26, 2014, he fled the United States to Russia under an assumed name. His current whereabouts are unknown; however, he is believed to be residing in Russia.

22. A review of Co-Conspirator 1’s electronic devices obtained during the consent search of his residence identified documents of incorporation, bank records, identification documents associated with the incorporators, and IRS documents for FLV Mobile Solutions LLC, Supra Auto Services LLC, TJ Electronic Supplies LLC, Fresco Web Design, Joslin Home Improvement LLC, and SCT Mechanics LLC.

23. Co-Conspirator 1’s electronic devices also contained numerous electronic lists of PII, logs of wire transfers associated with the eight shell companies identified above, and links to pre-paid card services. For example, two .txt files created and/or modified on or about April 6, 2013, and on or about April 20, 2012, contained the PII of approximately 364 and approximately 3,900 individuals, respectively. In addition, a Word document created and/or modified on or about July 11, 2013, included approximately seventeen hyperlinks to pre-paid debit card service registration pages as well as comments stating whether or not pre-paid cards had been successfully ordered, in what names, and how often accounts could be established.

24. Text message or “chat” logs recovered from Co-Conspirator 1’s electronic devices

included various conversations between Co-Conspirator 1 and other cyber-criminals, including communications regarding the false and fraudulent documents Co-Conspirator 1 used to establish the shell corporations detailed above. In other conversations, Co-Conspirator 1 stated that he worked with partners to create credit card accounts using stolen identities and processed minimum payments on the credit card accounts in order to avoid detection.

**GIULIANI NITA's Text Message Communications with Co-Conspirator 1**

25. Chat logs recovered from Co-Conspirator 1's electronic devices during the search of his residence in May 2014, included a lengthy conversation between Co-Conspirator 1 and **GIULIANI NITA**, who used an encrypted chat program account under the alias "juliensweiss." This chat covers the time period from in or around March 2012, through in or around May 2014. This chat shows that both individuals were heavily involved and familiar with tax refund fraud, pre-paid debit cards, PayPal accounts, and money laundering.

26. In these chats, **GIULIANI NITA** and Co-Conspirator 1 discussed techniques to transfer tax refund money from pre-paid debit cards by using PayPal accounts and then further transferring those funds to traditional bank accounts.

27. For example, on or about May 19, 2014, **GIULIANI NITA** shared with Co-Conspirator 1 a custom computer script that he created to process pre-paid card payments through PayPal. This script indicates that a payment of \$387 USD was submitted using PayPal's Website Payments Pro API Solution and the script includes a line that states "Payment sent to: contact@khmultiservice.com". As discussed in further detail below, KH Multi Services LLC was a shell company utilized by **GIULIANI NITA** to receive and transfer fraudulently obtained tax refund monies throughout the course of the scheme. Notably, during the chats with Co-Conspirator 1, **GIULIANI NITA** stated that he was able to process millions of dollars of tax

refund money in this manner.

28. During the chats with Co-Conspirator 1, **GIULIANI NITA** stated that he only works with a close team of people, only two to three people, and that he pays most of them in cash. **GIULIANI NITA** also said that he received a lot of tax refunds through Green Dot and that his partners would file the tax returns. **GIULIANI NITA** described how his partners would open Green Dot accounts in the same names as the individuals that purportedly filed the tax returns so that the names would match.

29. On or about April 2, 2015, Co-Conspirator 1 messaged **GIULIANI NITA** and stated that he needed more credit card numbers. **GIULIANI NITA** told Co-Conspirator 1 to “talk to my friend selltoanyone”—an online moniker.

30. According to the chat logs recovered from Co-Conspirator 1’s devices, on or about April 2, 2012, Co-Conspirator 1 contacted selltoanyone@secure.net.im and stated that “julien” (**GIULIANI NITA**) told Co-Conspirator 1 that selltoanyone@secure.net.im may have credit cards for sale. Selltoanyone@secure.net.im stated that he did have them for sale and offered 370 unique credit cards. Selltoanyone@secure.net.im then provided Co-Conspirator 1 with the address of a “carding” website. Based on my knowledge, training, and experience, carding websites are online “stores” or depositories where cybercriminals store, purchase, and sell stolen account information, often credit card account information of the type sought by Co-Conspirator 1 in this instance.

31. Thereafter, selltoanyone directed Co-Conspirator 1 to register on the website and provide selltoanyone with his username; selltoanyone promised to credit Co-Conspirator 1’s account balance. Per selltoanyone’s instructions, Co-Conspirator 1 could then purchase the credit card information he needed from the carding website. Selltoanyone told Co-Conspirator 1 that the carding site was selltoanyone’s own shop that that Co-Conspirator 1 could obtain credit card

numbers for free. Co-Conspirator 1 registered for the website and provided selltoanyone with his username, user44. Co-Conspirator 1 asked about the "600 US card" listed in the shop and selltoanyone responded by saying "600 cvv2".

32. Selltoanyone then directed Co-Conspirator 1 to click "buy cvv2, buy fullz, buy paypal" and Co-Conspirator 1 responded "ok." Selltoanyone also offered to sell SpyEye logs to Co-Conspirator 1. Based on my knowledge, training, and experience, SpyEye is a malware program that attacks particular internet browsers on Windows operating systems and uses keylogging and form grabbing in order to steal user credentials such as usernames and passwords. SpyEye allows cyber-criminals to steal money from online bank accounts and initiate transactions even while the legitimate users are logged into their online bank accounts.

33. According to earlier chat logs recovered from Co-Conspirator 1's devices, on or about April 2, 2012, Co-Conspirator 1 and GIULIANI NITA were discussing how GIULIANI NITA could pay Co-Conspirator 1. In this chat GIULIANI NITA stated that he obtained \$3,984 USD from the cards that Co-Conspirator 1 provided to him and that Co-Conspirator 1's share was \$1,947 USD. Co-Conspirator 1 asked for payment by Liberty Reserve and GIULIANI NITA stated that his friend only had about \$1,200 in Liberty Reserve.

34. Liberty Reserve was a centralized digital currency or "cryptocurrency" that was eventually shut down by U.S. authorities in or around May of 2013. Liberty Reserve was indicted by the Southern District of New York for allegedly laundering \$6 billion USD of criminal proceeds, including proceeds of credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. On or about April 2, 2012, at approximately 3:30 p.m., Co-Conspirator 1 provided GIULIANI NITA with "U9686878," which is a unique Liberty Reserve account number. On the same day, GIULIANI NITA responded by saying

“done” and Co-Conspirator 1 said “got it thanx”.

35. As part of U.S. law enforcement’s action against Liberty Reserve, a copy of the service’s internal database was obtained. This database provides law enforcement with, among other data, the subscriber records, transactions records, and Internet Protocol address logs for Liberty Reserve accountholders. An Internet Protocol (“IP”) address is a unique, numeric address assigned to computers connected to the Internet.

36. A review of this database shows that on or about April 2, 2012, at 7:35 p.m., account U3865653 in the name of “SellToAnyone [sic]” sent approximately \$1,200 to account U9686878 in the name of “Vladimir Brovkin” of Ukraine. According to Liberty Reserve records, account U3865653 also sent approximately \$750 to account U9686878 on or about April 5, 2012, just after receiving approximately \$1,100 from account U6883894. According to Co-Conspirator 1’s chats with GIULIANI NITA, on or about April 5, 2012, the same date, GIULIANI NITA told Co-Conspirator 1 to check his Liberty Reserve account as GIULIANI NITA sent the rest of the money.

37. According to chat logs recovered from Co-Conspirator 1’s devices, on or about April 5, 2012, selltoanyone@secure.net.im provided Co-Conspirator 1 with a Liberty Reserve payment confirmation, which provided proof of payment of \$750 from account U3865653 to U9686878. Co-Conspirator 1 responded by saying “got it thank u”.

38. A review of Liberty Reserve account U3865653 shows that this account transferred a significant amount of funds to Liberty Reserve account U8322949. These transfers often occurred soon after the U3865653 received or accumulated a significant amount of money and these transfers often brought the U3865653 account balance to or close to zero.

39. A review of the U8322949 account reveals that it was opened in the name of GIULIANI NITA, located in Liège, Belgium, and listed e-mail account giulonline@live.com as the subscriber contact e-mail address.

40. During his chats with Co-Conspirator 1, GIULIANI NITA mentioned Liège, Belgium twice; noted that it was like the Caribbean of Europe; stated he controlled a Belgian personal bank account; said he had a Polish-Belgian girlfriend; and stated that he had a Belgian passport. During these chats, GIULIANI NITA also mentioned that he had a business bank account in Hong Kong and a personal bank account in Belgium. GIULIANI NITA also discussed Romania and how he still knows some people there.

41. A review of the U8322949 Liberty Reserve account shows that on or about January 1, 2012, this account sent approximately \$2,700 USD to HSBC Hong Kong to an account in the name of Dawis Multi Service Limited—a shell company utilized by GIULIANI NITA to receive and transfer tax fraud proceeds, as discussed further below.

42. According to HSBC records, the Dawis Multi Service Limited account ending in x7838 wired approximately \$2,000 on or about May 19, 2014 to the United Overseas Bank in Singapore for the benefit of Sergio Nita [sic].

43. A review of the U8322949 Liberty Reserve account also shows that between 2011 and 2013, that account sent \$10,567 USD, in the form of Western Union wires, to GIULIANI NITA in various locations, including the Netherlands, Belgium, and Romania.

44. A review of the U8322949 Liberty Reserve account further shows multiple IP address logins from Romania and from Belgium. For example, IP 85.26.64.113 logged in approximately 107 times from on or about November 29, 2012, through on or about August 13,



2012. This IP address geo-locates to Belgium, where GIULIANI NITA stated he resided during his communications with Co-Conspirator 1.

**Additional Shell Companies Utilized by GIULIANI NITA**

45. In or around August of 2015, Green Dot identified approximately 136 Green Dot pre-paid debit card accounts that issued multiple Bill Pay checks to FLV Mobile Solutions, one of the shell companies controlled by Co-Conspirator 1, totaling approximately \$369,994 USD. All of these particular Bill Pay checks were cancelled by Green Dot and the funds were returned to the respective pre-paid card accounts. Approximately thirteen of the approximately 136 cards then redirected the returned fraud proceeds to “KHMultiservice,” one of the shell companies controlled by GIULIANI NITA, totaling approximately \$36,556 USD.

46. Green Dot employees reviewed their records and noted that, from in or around March 2014, through in or around March 2016, there were a total of approximately 949 IRS tax refund deposits totaling approximately \$2,235,420 USD that were deposited into approximately 943 Green Dot pre-paid card accounts. Tax refunds were the main source of funds deposited into these accounts.

47. These accounts subsequently transferred the funds almost exclusively to “KHMultiservice” and had very few transactions with any other entities. Green Dot noted that approximately \$2,007,910 USD was transferred from these accounts to “KHMultiservice.”

48. Records provided by PayPal, an online payment processor, show that the KHMultiservice account was registered in the name of “KH Multi Services LLC” and opened by an individual with the initials K.H. This PayPal account was created on or about October 26, 2011, and the listed contact e-mail address is [contact@khmultiservice.com](mailto:contact@khmultiservice.com): the same address used in the automated computer script sent by GIULIANI NITA to Co-Conspirator 1 on or about May

19, 2014.

49. From in or around October 2011, through in or around June 2018, the PayPal account registered in the name of KH Multi Services LLC received approximately \$6,358,349 USD. From in or around November 2011, through in or around December 2018, this PayPal account sent approximately \$5,982,159 USD to a Bank of America account ending in x2753 in the name of KH Multi Services LLC, which, like the associated PayPal account, was also opened in the name of K.H.

50. K.H. was interviewed by law enforcement and stated that he does not have any affiliation with KH Multi Services LLC and that he has never heard of Green Dot pre-paid debit cards.

51. According to Bank of America records, on or about October 27, 2011, bank accounts ending in x2753 and x3806 were opened in the name of KH Multi Services LLC using the PII of K.H. The account ending in x2753 received approximately \$7,597,387 USD in deposits from on or about October 27, 2011, through on or about May 4, 2018. A significant majority of these deposits are from payment processors such as PayPal, Stripe and ProPay. The account ending in x3806 received approximately \$1,043,877 USD in deposits from on or about April 12, 2012, through on or about March 30, 2017. A significant majority of these deposits are from online payment processors such as PayPal, WePay, Square, Stripe and ProPay.

52. A majority of the funds deposited into the KH Multi Services LLC Bank of America account ending in x2753 were then wired internationally to an HSBC Hong Kong bank account ending in x7838 in the name of Dawis Multi Service Limited. From on or about March 27, 2012, through on or about August 2, 2017, approximately \$5,997,674 USD was wired from account x2753 to account x7838.

53. According to Bank of America records, the HSBC Hong Kong bank account ending in x7838 in the name of Dawis Multi Service sent approximately \$583,567 USD to V Auto Group LLC's Bank of America account ending in x5153. This account, as previously noted, was opened and controlled by Co-Conspirator 1 and Co-Conspirator 2 (Co-Conspirator 1's family member).

54. According to Bank of America records, Dawis Multi Service also sent a \$500 USD wire transfer to TJ Electronics Supplies LLC's Bank of America account ending in x7125 on or about July 7, 2014. This account, as previously noted, was associated with one of the shell companies controlled by Co-Conspirator 1.

#### **Selected Identity-Theft Victims**

55. As noted, during the course of the investigation, law enforcement identified a number of identity-theft victims, in whose names GIULIANI NITA and his co-conspirators (a) submitted tax returns and (b) created Green Dot online financial accounts to launder the fraudulently obtained tax refund monies.

56. Of the fraudulent tax returns and financial accounts identified in the preceding paragraph, a number were submitted and opened from IP Addresses located within the Southern District of Florida.

#### **GIULIANI NITA's Personal E-Mail Account**

57. A review of the e-mails seized from GIULIANI NITA's personal e-mail account, giulonline@live.com, which were obtained via search warrant, shows that this account was controlled by GIULIANI NITA. This evidence further confirms GIULIANI NITA's control of the Dawis Multi Service shell company bank account.

58. For example, on or about December 8, 2011, giulonline@live.com sent an e-mail to a third party using the domain "@onlinecompanyregister.com," stating, "Hi , my name is Sergio,

and I have your website and details from mr. Mircescu ( selltoanyone@secure.net.im ) . I am interested in the offer you made ( that was actually for me ).” Attached to this e-mail are (1) the Belgian driver’s license in the name of **GIULIANI NITA**, date of birth October 23, 1981, of Bucharest, Romania, with the individual’s picture; (2) the Belgian identity card in the name of **GIULIANI NITA**, date of birth October 23, 1981, of Bucharest, Romania, with the individual’s picture; and (3) an invoice in the name of Mr. Nija Sergio [sic] listing an address in Liège, Belgium. A comparison of the driver’s license picture to the identity card picture shows that it is the same person. This e-mail was for the purpose of registering “Phone Network IM Limited” as a United Kingdom company. On or about December 9, 2011 **GIULIANI NITA** sent another e-mail stating that he sent payment of \$1,925.01 USD via Western Union in the name of **GIULIANI NITA** of Liège, Belgium.

59. On or about June 20, 2019, **GIULIANI NITA** e-mailed a third party using the domain “@yandex.ru” a signed 11-month rental contract for Mar Baltico, Numero 44, Planta 2, Puerta 1, 03183, Alicante, Spain. This rental contract lists **GIULIANI NITA**, date of birth October 23, 1981, of Romanian nationality as the tenant.

60. On or about February 15, 2019, **GIULIANI NITA** e-mailed the same third party using the domain “@yandex.ru” an image of Romanian passport 056863494 in the name of **GIULIANI NITA**, date of birth October 23, 1981.

61. On or about February 15, 2019, **GIULIANI NITA** also e-mailed the same third party using the domain “@yandex.ru” a bank statement in the name of **GIULIANI NITA** of address Bradetu 9, Bradulet, Arges, Romania 117147.

62. On or about March 3, 2015, **GIULIANI NITA** e-mailed a third party using the domain “@slogold.net” stating, “wire transfer has been sent . You should receive it . Wire sent

from Dawis Multi Service , HSBC HK, Please confirm after receive.” A review of the e-mails back and forth between these two parties shows that **GIULIANI NITA** paid for a company to be incorporated in the Seychelles and a bank account to be opened. **GIULIANI NITA** initially specified that he wanted a bank account outside of Europe and the parties discussed options in Mauritius, St. Vincent, Belize, and Latvia. One of the e-mails sent by **GIULIANI NITA** included an attachment labeled “Business Plan” for “Cryptar Services Ltd” and listed “Dawis Multi Service Ltd.” as a “main supplier”.

63. On or about January 5, 2012, **GIULIANI NITA** e-mailed himself what appears to be an excerpt of a chat. Included in this chat is the banking information for Dawis Multi Service Limited, including the full account number, SWIFT code, and bank address.

64. On or about April 10, 2014, **GIULIANI NITA** e-mailed a third party using the domain “@europacbank.com.” **GIULIANI NITA** was attempting to transfer funds into a newly opened bank account for Cryptar Services Ltd. **GIULIANI NITA** asked why his wire transfer was taking two-to-five business days when in Romania and Belgium his transfers would be completed the following business day, even if the transfer came from United States, China, Australia or Europe. **GIULIANI NITA** included the wire details from HSBC in the e-mail, which shows **GIULIANI NITA** transferred, on or about April 8, 2014, \$1,000 USD from the Dawis Multi Service Limited HSBC Hong Kong account to a Cryptar Service Ltd. account held at Euro Pacific Bank St. Vincent and the Grenadines.

65. On or about January 5, 2012, **GIULIANI NITA** received an e-mail from a third party using the domain “@wm-center.com,” which stated “Hello Dawis Multi Service Limited!” and informed **GIULIANI NITA** that his recent order was accepted and would be processed.

66. On or about January 25, 2012, and again on or about May 26, 2012, GIULIANI NITA e-mailed himself (at a different e-mail address associated with his moniker "juliensweiss"). The first e-mail included information about an address in Romania, the name "Nita Sergio [sic]" and details regarding a wire transfer. The second e-mail included information about co-branded pre-paid cards with a particular bank.

67. On or about June 6, 2013, GIULIANI NITA received an e-mail from a third party using the domain "dagensia.eu." This e-mail included answers to questions GIULIANI NITA appears to have submitted online. In response to GIULIANI NITA's question regarding "where do I make the login for ecardone banking?" the response was "https://banking.dagensia.eu". In response to GIULIANI NITA's question regarding "Have you been required to give users personal information to the US GOV in the past or plan to. . . ?" The response was "NO, we didn't and we wont". GIULIANI NITA's submitted questions ended with the statement "Sorry for some direct questions but I need to know all this information for future use of service. Regards, Sergio".

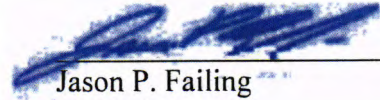
#### **IDENTIFICATION AND LOCATION**

68. GIULIANI NITA is a male with blue eyes and black hair. He was born on 23 October 1981, in Romania. Photographs of GIULIANI NITA are attached to the affidavit of Assistant U.S. Attorney Christopher Browne. GIULIANI NITA is the holder of a Romania passport, issued on 30 January 2012 with passport number 051145183. Investigators are not aware of any updated or current passport.

69. According to information received from Greek authorities, GIULIANI NITA was arrested on a Red Notice while traveling to the Greek island of Zakynthos and is currently detained at a jail within Greece.

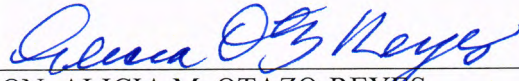
**CONCLUSION**

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



Jason P. Failing  
Special Agent  
IRS Criminal Investigation, Cyber Crimes Unit

Attested to by the applicant in accordance with the requirements of Fed.R.Crim.P. 4.1 by Face Time this 30<sup>th</sup> day of July 2021.



HON. ALICIA M. OTAZO-REYES  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF FLORIDA