


Approved:   
SAGAR K. RAVI  
Assistant U.S. Attorney

18 MAG 3831

Before: HONORABLE DEBRA FREEMAN  
United States Magistrate Judge  
Southern District of New York

----- x

SEALED COMPLAINT

UNITED STATES OF AMERICA :  
 :  
 - v. - : Violations of  
 : 18 U.S.C. §§ 1030 and 2  
  
BILLY RIBEIRO ANDERSON, :  
 a/k/a "Anderson Albuquerque," : COUNTY OF OFFENSE:  
 a/k/a "AlfabetoVirtual," : NEW YORK  
  
Defendant. :

----- x

SOUTHERN DISTRICT OF NEW YORK, ss.:

GEORGE F. MURPHY, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE

(Computer Fraud - Causing Damage to a Protected Computer)

1. On or about October 4, 2016, in the Southern District of New York and elsewhere, BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, which caused loss to one and more persons during any one-year period aggregating at least \$5,000 in value, and damaged a computer used by and for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security, to wit, ANDERSON accessed without authorization a computer owned and used by the United States Military Academy in West Point, New York ("West Point") and defaced a website for the Combating Terrorism Center at West Point by modifying the website to display content generated by ANDERSON, which impaired the

integrity and availability of that website, and caused over \$5,000 in damages.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I) & (V), 1030(c)(4)(B)(i), and 2.)

COUNT TWO

(Computer Fraud - Unauthorized Access to a United States Government Computer)

2. On or about October 4, 2016, in the Southern District of New York and elsewhere, BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, intentionally and without authorization to access any nonpublic computer of a department or agency of the United States, accessed a computer of that department or agency that was exclusively for the use of the Government of the United States, to wit, ANDERSON accessed without authorization a computer owned and used exclusively by West Point and defaced a website for the Combating Terrorism Center at West Point by modifying the website to display content generated by ANDERSON.

(Title 18, United States Code, Sections 1030(a)(3), 1030(c)(2)(A), and 2.)

COUNT THREE

(Computer Fraud - Causing Damage to a Protected Computer)

3. On or about July 10, 2015, in the Southern District of New York and elsewhere, BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, which caused loss to one and more persons during any one-year period aggregating at least \$5,000 in value, to wit, ANDERSON intentionally and without authorization accessed a computer owned and used by the New York City Comptroller (the "NYC Comptroller") and defaced the website for the NYC Comptroller by modifying the website to display content generated by ANDERSON,

which impaired the integrity and availability of that website, and caused over \$5,000 in damages.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

4. I am a Special Agent with the FBI, and have been employed in this capacity for more than three years. This affidavit is based upon my personal participation in the investigation of this matter, my conversations with law enforcement agents, witnesses, and others, as well as my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

#### Overview

5. Based on my training and experience, I know that website defacements are acts of computer intrusion during which a hacker obtains unauthorized access to computers hosting Internet websites, and then replaces the publically available contents of the website with content generated by the hacker, thereby "defacing" the website. Hackers frequently accept responsibility for defacements by listing their online pseudonym as part of the defaced content.

6. As set forth in detail below, from in or about 2015 up to and including at least March 13, 2018, BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, has taken responsibility for obtaining unauthorized access to and committing more than 11,000 defacements of various military, government, and business websites around the world under the online pseudonym "AlfabetoVirtual," including websites for the Combating Terrorism Center at West Point and the NYC Comptroller.

7. BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, has also committed unauthorized intrusions of thousands of web servers located around the world by surreptitiously installing malicious code on victim web servers that provided ANDERSON with administrative rights to the victimized web servers, thereby enabling ANDERSON to commit defacements and to otherwise maintain persistent unauthorized access to the victimized web servers.

### The New York City Comptroller Defacement

8. Based on my review of reports and documents provided to the FBI by the NYC Comptroller, I have learned the following, in substance and in part:

a. On or about July 10, 2015, a website owned by the NYC Comptroller was defaced (the "NYC Comptroller Defacement"), and a hacker using the online pseudonym "AlfabetoVirtual" took public responsibility for the intrusion and defacement.

b. The contents of the NYC Comptroller website were modified to display the text "Hacked by AlfabetoVirtual," "#FREEPALESTINE" and "#FREEGAZA." The following is a screenshot of the defacement of the NYC Comptroller website:



c. The NYC Comptroller Defacement was performed by an unauthorized actor who exploited security vulnerabilities associated with the version of a plugin being used on the website.

d. The cost to the NYC Comptroller of responding to the defacement, conducting a damage assessment, and remediating the defacement was greater than \$5,000.

#### The West Point Defacement

9. Based on my review of reports and documents provided to the FBI by the United States Army Criminal Investigation Command, Computer Crime Investigative Unit, I have learned the following, in substance and in part:

a. On or about October 4, 2016, a website for the Combating Terrorism Center (the "CTC") at West Point was defaced (the "CTC Website Defacement"), and a hacker using the online pseudonym "AlfabetoVirtual" took public responsibility for the intrusion and defacement.

b. Based on a forensic review conducted by the U.S. Army after the CTC Website Defacement was detected, the content of the CTC website was modified to display the text "Hacked by AlfabetoVirtual."

c. The CTC Website Defacement was performed by an unauthorized administrative account which exploited a known cross site script vulnerability, thereby enabling the attacker to bypass access controls and target an internal CTC website address.

d. The cost to the U.S. Government of responding to the defacement, conducting a damage assessment, and remediating the defacement was greater than \$7,000.

#### Other Defacements by "AlfabetoVirtual"

10. Based on my participation in this investigation and my experience, I know that Zone-H.org ("Zone-H") is a website used by cyber criminals to post evidence of their network intrusions and website defacements. Hackers who post to Zone-H claim responsibility for their intrusions and defacements under their

online pseudonyms, and frequently post screenshots of defaced webpages. Based on my review of Zone-H, I have learned the following, in substance and in part:

a. Between on or about October 8, 2016 and at least on or about March 13, 2018, Zone-H listed over 11,000 website defacements by a hacker using the online pseudonym "AlfabetoVirtual." The defacements featured, among other things, comments in English, Spanish, and/or Portuguese, as well as music playing in English or Spanish.

b. The defacements by "AlfabetoVirtual," which were mirrored with screenshots on Zone-H, involved government, business, and charitable websites around the world, including in the United States. More than 300 of the over 11,000 defacements were assigned a star on Zone-H, which, according to the Zone-H website, denote a "special defacement (special defacements are important websites)." Those defacements that were assigned a star largely involved government websites with a ".gov" domain, including, for example, a defacement of the website for the Ronald Reagan Presidential Library that occurred in or about January 2016.

c. On or about July 10, 2015, the NYC Comptroller Defacement was listed on Zone-H and attributed to "AlfabetoVirtual."

d. On or about October 4, 2016, the West Point Defacement was listed on Zone-H and attributed to "AlfabetoVirtual." The following is a screenshot of the CTC Website Defacement posted on Zone-H:

**Mirror saved on:** 2016-10-04 06:53:58

**Notified by:** AlfabetoVirtual      **Domain:** [https://www.ctc.usma.edu/wp-content/\\_input\\_3\\_.txt](https://www.ctc.usma.edu/wp-content/_input_3_.txt)      **IP address:** 54.172.227.89 

**System:** Linux      **Web server:** nginx      [Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2016-10-04 06:53:58

Hacked by AlfabetoVirtual

e. An email address with the username "alfabetovirtual" (the "AlfabetoVirtual Email Account") was listed in at least one of the defacements attributed to "AlfabetoVirtual" on Zone-H.

Identification of "AlfabetoVirtual" as BILLY RIBIERO  
ANDERSON, the Defendant

11. Based on my review of a U.S. passport application submitted for BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, to the U.S. Department of State on or about June 10, 2015 (the "Passport Application"), I have learned the following, in substance and in part:

a. "Anderson Albuquerque" was listed under "Other Names" for ANDERSON.

b. The mailing address listed for ANDERSON was an apartment in Los Angeles, California.

c. An email address with the username "technician.usa" (the "Technician Email Account") was listed as the email address for ANDERSON.

d. A phone number ending in 1087 (the "Anderson Phone Number") was listed as the phone number for ANDERSON.

e. The birthdate for ANDERSON was August 9, 1976.

f. The place of birth for ANDERSON was Rio de Janeiro, Brazil.

12. Based on public Internet searches conducted by law enforcement, I have learned the following, in substance and in part:

a. On or about May 12, 2011, a YouTube video-sharing channel titled "Rio Hunter" was created with a Uniform Resource Locator ("URL") containing "analfabetovirtual" (the "Rio Hunter YouTube Channel"). The Rio Hunter YouTube Channel had a banner containing the text "Analfabeto Virtual" and a cartoon image of a person wearing a red cape and a mustached devil mask and holding a trident. The trident appears to be piercing a flaming

image of a black and white suit with a question mark in the place of a head, which is a known emblem used by Anonymous, a hacker group responsible for cyberattacks against governments, businesses and other victims around the world ("Anonymous").

b. On or about June 20, 2013, a YouTube video-sharing channel titled "analfabetovirtual" was created with a URL containing "anaIfabetovirtual"<sup>1</sup> (the "AnalfabetoVirtual YouTube Channel"). The AnalfabetoVirtual YouTube Channel has a banner containing the text "Analfabeto Virtual" and a cartoon image of the same mustached devil mask that was in the banner of the Rio Hunter YouTube Channel. The AnalfabetoVirtual YouTube Channel posted a video of an individual driving a car with sunglasses and speaking in Portuguese. Based on my review of known images of BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, I believe the individual in the video is ANDERSON.

c. A Google+ social networking profile registered with the username "analfabetovirtual" and a Google+ social networking profile registered with the username "AlfabetoVirtual" both featured photos of a male individual. I have compared the photos of the male individual from those Google+ profiles with known images of ANDERSON, and I believe that they are the same individual.

d. There is an Instagram account in the name of "AlfabetoVirtual" (the "AlfabetoVirtual Instagram Account").

13. Based on my review of subscriber records regarding the AlfabetoVirtual Instagram Account, I have learned that an email address with the username "analfabetovirtual" ("the "Analfabetovirtual Email Account") is the registered email address for the AlfabetoVirtual Instagram Account.

14. Based on my review of subscriber records for the Technician Email Account, the Analfabetovirtual Email Account, the AlfabetoVirtual Email Account, and an email address with the username "mr--billy" (the "Billy Email Account," and collectively, the "Anderson Email Accounts"), I have learned the

---

<sup>1</sup> "anaIfabetovirtual" contains an "I" in lieu of an "L," which is the only difference from the URL for the Rio Hunter YouTube Channel.



following, which indicate that the Anderson Email Accounts were all used and controlled by BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant:

a. *The Technician Email Account*

i. The "Name" listed for the Technician Email Account was "Billy Anderson."

ii. The short message service ("SMS") number, or text messaging number, listed for the Technician Email Account was the Anderson Phone Number.

iii. Between at least on or about December 19, 2016 and at least on or about April 20, 2017, the Technician Email Account was accessed using an Internet Protocol ("IP") address ending in 124.24 (the "124.24 IP Address") at least eight times.<sup>2</sup>

iv. On or about December 20, 2016, the Technician Email Account was accessed using an IP address ending in 64f5 (the "64f5 IP Address," and together with the 124.24 IP Address, the "Anderson IP Addresses").

b. *The Analfabetovirtual Email Account*

i. The "Name" listed for the Analfabetovirtual Email Account was "Rio Hunter," which was the same moniker used for the Rio Hunter YouTube Channel.

ii. Between at least on or about October 6, 2016 and at least on or about July 14, 2017, the Analfabetovirtual Email Account was accessed using the 124.24 IP Address more than 35 times.

iii. On or about December 20, 2016, the same day the Technician Email Account was accessed using the 64f5 IP

---

<sup>2</sup> Based on my training and experience, each electronic device connected to the Internet must be assigned a unique IP address so that communications from or directed to that electronic device are routed properly.

Address, the Analfabetovirtual Email Account was accessed using the 64f5 IP Address.

iv. The Analfabetovirtual Email Account and the Technician Email Account were linked by web cookies<sup>3</sup> to each other and to seven additional email accounts, including three email accounts that contain ANDERSON's full legal name ("Billy Anderson"), indicating that each of these accounts were accessed from the same Internet browser.

c. *The Billy Email Account*

i. The "Recovery e-mail"<sup>4</sup> listed for both the Technician Email Account and the Analfabetovirtual Email Account was the Billy Email Account, indicating that the same individual has control and dominion over all three of those accounts.

ii. The "First Name" and "Last Name" listed for the Billy Email Account was "Rio" and "Hunter," respectively, which was the same moniker used for the Rio Hunter YouTube Channel.

iii. The state and postal code listed for the Billy Email Account was California, 90034.

iv. Between at least on or about February 6, 2017 and at least on or about August 21, 2017, the Billy Email Account was accessed using the 124.24 IP Address more than 475 times.

---

<sup>3</sup> A "web cookie" or "cookie" allows the service provider for an online account to determine whether multiple online accounts are accessed during the same browser session and thus are controlled by the same user.

<sup>4</sup> Based on my training and experience, I know that email providers allow subscribers to register "recovery" accounts to assist with password recovery. Providers maintain these verified recovery accounts to be able to communicate with the subscriber in cases in which the user forgets his or her password, to assist with password resets.

d. *The AlfabetoVirtual Email Account*

i. The "Full Name" listed for the AlfabetoVirtual Email Account was "alfabetovirtual zone-h."

ii. The "Alternate Communication Channel" listed for the AlfabetoVirtual Email Account was the Anderson Phone Number.

iii. The "Time Zone" listed for the AlfabetoVirtual Email Account was "pt," which I believe was a reference to the Pacific Time Zone, which includes California.

iv. The "Birthday" listed for the AlfabetoVirtual Email Account was August 9, 1998, which is the same date and month as the birthdate for ANDERSON.

v. On at least on or about December 9, 2016, the AlfabetoVirtual Email Account was accessed using the 124.24 IP Address.

15. Based on my review of records from the service provider for the Anderson IP Addresses, I have learned that from on or about October 2, 2016 through at least on or about July 5, 2017, the Anderson IP Addresses were subscribed to an individual named "Anderson Albuquerque" with the Anderson Phone Number and an address at an apartment in Torrance, California. As discussed in detail above, the Technician Email Account, Analfabetovirtual Email Account, AlfabetoVirtual Email Account, and Billy Email Account have all been accessed by at least one of the Anderson IP Addresses.

16. On or about March 29, 2012, BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, filed a complaint with the FBI against individuals he stated were associated with Anonymous. In this complaint, ANDERSON stated the following, in substance and in part: "I am against any of these anonymous hacker, and I am willing to help." In connection with this complaint, ANDERSON signed his name as "Anderson Albuquerque" and provided the Anderson Phone Number, the Technician Email Account, and an address in Los Angeles, California.

17. Based on my review of the contents of the Anderson Email Accounts obtained pursuant to Court-authorized search warrants, I have learned the following, in substance and in part<sup>5</sup>:

a. On or about June 23, 2013, an unidentified individual ("UNK-1") sent the following chat messages to the Analfabetovirtual Email Account, which appear to reference Anonymous:

UNK-1: I am eager to contribute with you in any way I can and really be considered as a legitimate anonymous

UNK-1: Later on I would like to talk to you about the Anonymous

b. On or about June 26, 2014, an unidentified individual ("UNK-2") exchanged the following chat messages with the Analfabetovirtual Email Account (referred to as "ANALFABETO" below), which appear to discuss UNK-2 visiting the United States from Brazil:

ANALFABETO: brother you have to come even if just for tourism

ANALFABETO: this is the country of opportunities, Brazil we just get screwed

ANALFABETO: ☺ [ . . . ]

UNK-2: If I was at least 30, I would do that [ . . . ]

---

<sup>5</sup> The Billy Email Account contained copies of emails to and from the Analfabetovirtual Email Account which were themselves not in the contents of the Analfabetovirtual Email Account produced to the Government in response to a search warrant. In addition, the original email and chat messages excerpted herein were largely in Portuguese and have been translated into English. The translations are preliminary and subject to revision.

ANALFABETO: You could get your Portuguese passport  
and ente[r] here the USA [ . . . ]

ANALFABETO: by the last name

ANALFABETO: that is why the Americans call me  
Anderson [ . . . ]

ANALFABETO: My real name is Billy Anderson

c. On or about July 13, 2015, the Analfabetovirtual  
Email Account sent the following email from "Andrew Josh" to an  
administrator at Zone-H:

Is everything alright . . . .?

I think my last e-mail was either sent to the  
spam folder or you were off the zone-h duty.

I found this new vulnerability and you can  
confirm, by the defaced that I'm doing, they  
are all on home and contain the keywords  
Hacked by AlfabetoVirtual or Hacked by  
AlfabetoVirtual. Also, they are all at the  
onhold. I thought the robot would quickly  
detect a new exploit, but I see now that's not  
the case. Could you tell me exactly what to do  
to quickly pass by onhold? I've done 300  
sites already and just from running a list of  
700 sites the problem is with WordPress and  
millions of blogs that use this plugin.

After you help me, I'll run Finger and place  
Brazil at the Top of defaces again.

Regards.

d. On or about August 14, 2015, the  
Analfabetovirtual Email Account sent the following email from  
"Andrew Josh" to an administrator at Zone-H: "[B]rother, I  
closed with the guys from Fatal Error and we created a new  
group, parallel to ProntoWave. This deface here, did it deserve  
a star or not? [inserts mirror of defacement]." In response,  
the administrator at Zone-H stated the following, in substance

and in part: "Only famous companies, top 50 univ or government sites get a star."

e. On or about September 20, 2015, the Analfabetovirtual Email Account sent the following email from "Andrew Josh" to an administrator at Zone-H:

Good afternoon brother

So, I found another bypass because of a glitch already known by Zone-H's bot the jDownload, where a gif file is uploaded. My question is: do I have to add anything else for the bot to detect it? And accept my onholds?

AlfabetoVirtual - my name at Zone-H.

Regards.

f. On or about December 20, 2015, the Technician Email Account was used to send a resume for "Billy Anderson," which listed a position of "Cyber Security Analyst, Information Security Researcher and Part-time hacker" in Torrance, California for the period of "2013 - Present." The description for the position further stated the following, in substance and in part: "Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence. Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software (Wordpress, Joomla, Drupal)."<sup>6</sup>

g. On or about April 15, 2016, the Technician Email Account sent the following email, in substance and in part, to the Analfabetovirtual Email Account, which appears to reference Anonymous:

We have not forgotten. Wait for us!!  
Brazilian people, YouTube watchers. We are anonymous, we are an idea, and we are a legion. Once again in the name of digital transparency and of information, against all the

---

<sup>6</sup> Joomla is a free and open-source content management system for publishing web content.

corruption, in all the segments of society, we are going to show again some truths about the virtual scenario of the Brazilian YouTube. The objective of this video is to prove the real intent of some channels that take advantage of their audience naivety, an audience that does not have a minimal discernment or intellectual capacity or mental wisdom.

#### Use of Web Shells to Commit Intrusions and Defacements

18. Based on a review of source code of victimized websites and open source material, the FBI has identified two email addresses with the username "feofeoz443" (the "Feofeoz Email Accounts") associated with the unauthorized implantation of a malicious data file on web servers. Once executed, the malicious data file initiated attempts to contact various URLs (i.e., web addresses) in order to download other malicious content to facilitate further exploits on the victimized web server. In particular, the code that has been found embedded in victim websites initiated attempts to download a web shell, which is a programming tool commonly used to interface with a web server and provides someone with administrative rights to the computer system (i.e., ability to read, write and modify data). Once the shell was downloaded and such access was provided, the code included commands to send emails to the Feofeoz Email Accounts to provide notifications regarding the successful installation of a web shell on victim websites. Once the emails to the Feofeoz Email Accounts were sent, the code prompted a deletion of the code from the victimized web server and its corresponding logs. The emails to the Feofeoz Email Accounts reported the existence and location of the web shell, therefore allowing the individual in control of the Feofeoz Email Accounts to have what is commonly referred to as back-door access to the victimized web servers.

19. Based on my review of the contents of the Feofeoz Email Accounts obtained pursuant to a Court-authorized search warrant and my review of defacements on Zone-H attributed to "AlfabetoVirtual," I believe that BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, was in control of the Feofeoz Email Accounts and used the web

shells installed on victimized web servers to commit defacements of the websites. For example:

a. On or about November 24, 2015, August 23 and 25, 2016, and October 1, 2016, the Feofez Email Accounts received emails regarding the successful installation of a web shell on the website of a medical billing company located in New Jersey (the "Medical Company"). On or about November 27, 2016, Zone-H listed a defacement of the Medical Company's website by "AlfabetoVirtual," which modified the website to display the text "Hacked by AlfabetoVirtual."

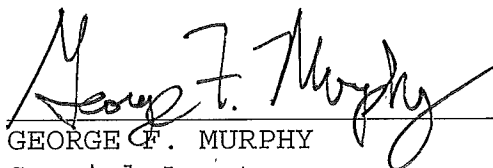
b. On or about August 23 and 25, 2016, the Feofez Email Accounts received emails regarding the successful installation of a web shell on the website of a marketing company located in Illinois (the "Marketing Company"). On or about December 3, 2016, Zone-H listed a defacement of the Marketing Company's website by "AlfabetoVirtual," which modified the website to display the text "Hacked by AlfabetoVirtual."

c. On or about November 30, 2015, December 1, 2015, and September 2, 2016, the Feofez Email Accounts received emails regarding the successful installation of a web shell on the website of a magazine company located in France (the "Magazine Company"). On or about October 4, 2016, Zone-H listed a defacement of the Magazine Company's website by "AlfabetoVirtual," which modified the website to display the text "Hacked by AlfabetoVirtual."

d. In total, from at least on or about September 23, 2015 through at least on or about November 8, 2016, the Feofez Email Accounts received over 17,000 emails regarding the successful installation of web shells on the websites of government entities and businesses located around the world, many of which were associated with defacements listed on Zone-H attributable to "AlfabetoVirtual."



WHEREFORE, I respectfully request that a warrant be issued for the arrest of BILLY RIBEIRO ANDERSON, a/k/a "Anderson Albuquerque," a/k/a "AlfabetoVirtual," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



GEORGE F. MURPHY  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
4th day of May, 2018



THE HONORABLE DEBRA FREEMAN  
United States Magistrate Judge  
Southern District of New York

