UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**TO BE FILED UNDER SEAL**
	:	
v.	:	Hon. Mark Falk
	:	
TREVONTAE WASHINGTON	:	Mag. No. **20-1146**
	:	
	:	**CRIMINAL COMPLAINT**

I, Bryan DeBon, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the United States Secret Service, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Bryan DeBon, Special Agent
United States Secret Service

Special Agent DeBon attested
to this Complaint by telephone
pursuant to FRCP 4.1(b)(2)(A) on
September 25, 2020 in the
District of New Jersey

HONORABLE MARK FALK
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

COUNT ONE
(Conspiracy to Commit Wire Fraud)

From in or around December 2017 through in or around April 2019, in Bergen County, in the District of New Jersey and elsewhere, defendant

TREVONTAE WASHINGTON

did knowingly and intentionally conspire with others to devise and intend to devise a scheme and artifice to defraud individuals, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Sections 1349 and 2.

COUNT TWO
(Conspiracy to Commit Computer Fraud and Abuse)

From in or around December 2017 through in or around April 2019, in the District of New Jersey and elsewhere, defendant

TREVONTAE WASHINGTON

did knowingly and intentionally conspire with others to commit computer fraud and abuse, namely, to intentionally access a computer without authorization and to exceed authorized access, and thereby obtain information from any protected computer, for purposes of commercial advantage and private financial gain, contrary to Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i).

In violation of Title 18, United States Code, Sections 371 and 2.

ATTACHMENT B

I, Bryan DeBon, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS" or "Secret Service"), and have been so employed since July 2017. I am authorized and have received training to investigate violations of the laws of the United States, and to execute warrants under the authority of the United States. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland. My training and experience as a Secret Service agent has included the investigation of cases involving counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have participated in investigations resulting in the seizures of criminally derived property.

2. This Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a federal criminal complaint and arrest warrant. Accordingly, I have not included each and every fact known by the Government concerning this investigation. Except as otherwise indicated, the actions, conversations, and statements of others identified in this Affidavit – even where they appear in quotations – are reported in substance and in part. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents.

BACKGROUND

3. At various times relevant to this Complaint:

   A. The defendant Trevontae Washington ("WASHINGTON") was a resident of Louisiana.

   B. "Victim-1" was a professional football player, who was employed by a National Football League ("NFL") franchise, and was living in New Jersey.

   C. "Victim-2" was a professional basketball player, who was employed by a National Basketball Association ("NBA") franchise, and was living in New Jersey.

   D. "Victim-3" was a professional football player, who was employed by an NFL franchise, and was living in Massachusetts.

FACTS SUPPORTING PROBABLE CAUSE

4. The operators of a social media and email account hacking scheme, including WASHINGTON, targeted semi-professional and professional athletes across the United States, including Victims-1, -2 and -3. As part of the scheme, WASHINGTON and others gained unauthorized access to the social media and email accounts of the victim-athletes and used or attempted to use that access for their personal financial gain, including by selling access to others who would further exploit the compromised accounts.

Victim-1

5. Between on or about May 27, 2018 and on or about May 30, 2018, Victim-1 received a direct message on his Instagram account (the "Victim-1 Instagram Account") from an unknown account. The direct message contained a clickable link to a Facebook site that purported to solicit community support from professional athletes. Victim-1 used his personal cell phone to click on the link, which brought him to what he believed was a Facebook login page (the "Bogus Facebook Page"). Following instructions on the Bogus Facebook Page, Victim-1 entered his Facebook user name and password. Shortly after entering this data, Victim-1 was locked out of multiple of his accounts on social media platforms, including Facebook, Twitter, Instagram, and Snapchat.

6. On or about June 3, 2018, Victim-1 was advised by email by Yahoo, Inc. ("Yahoo") that changes had been made to his Yahoo email account (the "Victim-1 Yahoo Account"). Victim-1 did not make or authorize the changes to the Victim-1 Yahoo Account. Shortly thereafter, Victim-1 found that he was locked out of the Victim-1 Yahoo Account.

7. According to records provided by Yahoo, the Victim-1 Yahoo Account had been accessed without authorization prior to June 3, 2018. For example, on or about June 1, 2018, the Victim-1 Yahoo Account was accessed by a computer assigned the cookie[1] eeepriddg3qgg (the "3qgg Cookie") from IP Address 71.88.129.58 (the "58 IP Address").

8. According to records provided by Charter Communications, at the time of the unauthorized access to Victim-1's social media and email accounts, the

[1] Browser cookies, also known as a "bcookies" or, simply, "cookies," are small, unique pieces of data stored on a user's computer by a web browser while browsing a website. Cookies were designed to be a reliable mechanism for websites to remember information or to record the user's browsing activity. They can also be used to remember pieces of information that the user previously entered into form fields, such as names, addresses, passwords, and payment card numbers.

58 IP Address was assigned to WASHINGTON'S home address at the time in Thibodaux, Louisiana (the "Thibodaux Address").

9. Further analysis revealed that the computer associated with the 3qgg Cookie also accessed Yahoo accounts belonging to at least three additional professional athletes between May 20, 2018 and May 29, 2018. Information provided by Yahoo regarding these accounts further revealed that a computer assigned the cookie 72n66j5c5gv9i (the "gv9i Cookie") also accessed two of the three accounts.

10. According to information provided by Yahoo, on or about August 15, 2017, the computer associated with the gv9i Cookie also accessed the Yahoo email account wtravontaa@yahoo.com (the "Wtravontaa Yahoo Account"). According to Yahoo records, the Wtravontaa Yahoo Account was subscribed to by WASHINGTON and listed a verified phone number ending in 8260 (the "8260 Number"). According to records provided by Sprint, the 8260 Number was subscribed to by WASHIGNTON at the Thibodaux Address.

11. Based on the above information, as well as my training and experience, there is probable cause to believe that WASHINGTON was responsible for gaining unauthorized access to the Victim-1 Instagram and Yahoo Accounts and the additional athlete accounts referenced in Paragraph 9.

Victim-2

12. On or about January 16, 2018, Victim-2 learned that the 8260 Number had been added to Victim-2's Instagram account (the "Victim-2 Instagram Account") and reported it to Facebook, the parent company for Instagram. In addition, according to records obtained from Yahoo, on or about January 17, 2018, the Wtravontaa Yahoo Account received an automated email from Instagram with the subject line "Help Secure Your Account...." The "Account" referenced in the email was the Victim-2 Instagram Account. According to Facebook records, the Wtravontaa Yahoo Account had been added to the Victim-2 Instagram Account as a means of contact. Victim-2 did not execute or authorize these modifications to the Victim-2 Instagram Account.

13. According to Facebook records, on or about January 31, 2018, a Facebook account subscribed to by WASHINGTON (the "WASHINGTON Facebook Account") was linked to the Victim-2 Instagram Account. On the same date, the name on the Victim-2 Instagram Account was changed to "tre," the first three letters of "Trevontae." This investigation has revealed multiple instances in which, after gaining unauthorized access to a victim's account, WASHINGTON changed the subscriber name on the account to "tre."

14. According to Yahoo records, on or about February 2, 2018, the computer associated with the gv9i Cookie accessed a Yahoo account belonging to Victim-2 (the "Victim-2 Yahoo Account") from the 58 IP Address.

15. Based on the above information, as well as my training and experience, there is probable cause to believe that WASHINGTON was responsible for gaining unauthorized access to the Victim-2 Instagram and Yahoo Accounts.

Victim-3

16. According to Facebook records, on or about December 3, 2017, the 8260 Number was added to an Instagram account belonging to Victim-3 (the "Victim-3 Instagram Account").

17. Facebook records further revealed that, on or about December 3, 2017, a computer using an IP Address ending in 73e5 (the "73e5 IP Address") was used to access the Victim-3 Instagram Account. The 73e5 IP Address resolved to the Thibodaux Address. At the time of the login from the 73e5 IP Address, Victim-3 resided in Massachusetts.

18. After the 8260 Number was added to the Victim-3 Instagram Account, the WASHINGTON Facebook Account was linked to the Victim-3 Instagram Account.

19. Following the unauthorized access of the Victim-3 Instagram Account, on or about December 3, 2017, the Google email account gebear11@gmail.com (the "Gebear Google Account") was added to the Victim-3 Instagram Account. According to Google records, the Gebear Google Account is subscribed to by "George Bear" and was accessed from an IP address that resolved to Thibodaux, Louisiana. According to records provided by PayPal, the Gebear Google Account was associated with a PayPal Account subscribed to by WASHINGTON (the "WASHINGTON PayPal Account") at the Thibodaux Address. PayPal records listed the 8260 Number as a means of contact for the WASHINGTON PayPal Account and showed at least one login from the 58 IP Address.

20. According to Yahoo records, a computer using the 58 IP Address logged into the Yahoo email account wtravonta@yahoo.com (with one "a") (the "Wtravonta Yahoo Account") on numerous occasions, including on or about January 24, 2018, on or about April 13, 2018, and on or about June 12, 2018. The Wtravonta Yahoo Account was subscribed to by WASHINGTON at the Thibodaux Address and listed the 8260 Number as a verified telephone number.

Interview of WASHINGTON

21. On or about April 30, 2019, WASHINGTON was arrested by authorities in Louisiana on charges related to the conduct described herein. WASHINGTON was advised of his rights, and voluntarily submitted to an interview by law enforcement. During the interview, WASHINGTON admitted to using phishing techniques to fraudulently acquire passwords associated with social media and email accounts belonging to victims of the scheme. WASHINGTON stated that after taking over the victim accounts, he sold access to the accounts to others for between approximately $500 and $1000 per account. WASHINGTON also admitted that he had purchased unauthorized access to stolen accounts, which he re-sold for a profit.

22. A review of a Chase bank account to which WASHINGTON is the signatory (the "WASHINGTON Chase Account") revealed numerous transfers consistent with the statement made by WASHINGTON to law enforcement, including transfers made at or around the time of the intrusions involving Victims-1, -2, and -3.