

<p>LODGED CLERK, U.S. DISTRICT COURT</p> <p>06/25/2020</p> <p>CENTRAL DISTRICT OF CALIFORNIA BY: <u>DM</u> DEPUTY</p>

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

RAMON OLORUNWA ABBAS,
aka "Ray Hushpuppi,"
aka "Hush,"

Defendant

Case No. 2:20-mj-02992

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning no later than October 15, 2019 and continuing through at least October 17, 2019, in the county of Los Angeles, in the Central District of California, and elsewhere, the defendant conspired to launder proceeds fraudulently obtained from a law firm, in violation of:

Code Section

18 U.S.C. § 1956(h)

*Offense Description*Conspiracy to Engage in Money
Laundering

This criminal complaint is based on these facts:

Please see attached affidavit. Continued on the attached sheet.

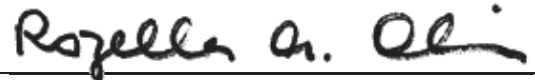
/S/

Complainant's signature

Andrew John Innocenti, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 06/25/2020

*Judge's signature*City and state: Los Angeles, California

Hon. Rozella A. Oliver, U.S. Magistrate Judge

Printed name and title

Table of Contents

I. INTRODUCTION 1

II. SUMMARY OF PROBABLE CAUSE 2

III. STATEMENT OF PROBABLE CAUSE 3

 A. Identification of ABBAS..... 3

 B. The Victim Law Firm..... 14

 C. The Foreign Financial Institution..... 18

 D. Additional Fraudulent Schemes and Attempted Money
 Laundering..... 22

IV. CONCLUSION..... 26

AFFIDAVIT

I, ANDREW JOHN INNOCENTI, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been so employed since approximately March 2015. I am currently assigned to the Los Angeles Field Office, High-Tech Organized Crime Squad, where I primarily investigate cyber-enabled fraud and business email compromise (“BEC”) schemes. Between approximately August 2015 and December 2018, I was assigned to a cyber-crime squad in the Chicago Field Office, where I investigated cyber-related crimes, including BEC cases. During my career as an FBI Special Agent, I have participated in numerous computer-crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations, computer technology, and white-collar fraud.

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for, RAMON OLORUNWA ABBAS, also known as (“aka”) “Ray Hushpuppi,” aka “Hush” (“ABBAS”), for violation of 18 U.S.C. § 1956(h) (Conspiracy to Engage in Money Laundering).

3. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and does not purport to set forth all of my knowledge of the government’s investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates set

forth below are “on or about” the dates indicated, and all amounts or sums are approximate.

II. SUMMARY OF PROBABLE CAUSE

4. RAMON OLORUNWA ABBAS is a Nigerian national living in the United Arab Emirates (the “U.A.E.”), whose social media accounts frequently show him in designer clothes, wearing expensive watches, and posing in or with luxury cars and charter jets. The FBI’s investigation has revealed that ABBAS finances this opulent lifestyle through crime, and that he is one of the leaders of a transnational network that facilitates computer intrusions, fraudulent schemes (including BEC schemes),¹ and money laundering, targeting victims around the world in schemes designed to steal hundreds of millions of dollars. ABBAS participated in these fraudulent schemes and money laundering in coordination with multiple coconspirators, including the persons referred to herein as Coconspirator 1 and Coconspirator 2.

5. This affidavit discusses several fraudulent schemes involving ABBAS. First, messages found on the iPhone of Coconspirator 1 (reviewed pursuant to a federal search warrant issued in this District) reflect that ABBAS, Coconspirator 1, and Coconspirator 2, with others, committed a BEC scheme that defrauded a victim in the United States of approximately \$922,857.76, including

¹ BEC fraud schemes often involve a computer hacker gaining unauthorized access to a business-email account, blocking or redirecting communications to and/or from that email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a “spoofed” email account) to communicate with personnel from a victim company and to attempt to trick them into making an unauthorized wire transfer. The fraudster will direct the unsuspecting personnel of the victim company to wire funds to the bank account of a third party (sometimes referred to as a “money mule”), which is often a bank account owned, controlled, and/or used by individuals involved in the scheme based in the United States. The money may then be laundered by wiring or transferring it through numerous bank accounts to launder the money, or by quickly withdrawing it as cash, by check, or by cashier’s check.

approximately \$396,050 that ABBAS, Coconspirator 1, and Coconspirator 2 laundered while Coconspirator 2 was in Los Angeles, California.

6. Second, ABBAS and Coconspirator 1 conspired to launder funds intended to be stolen through fraudulent wire transfers from a foreign financial institution (the “Foreign Financial Institution”), in which fraudulent wire transfers, totaling approximately €13 million (approximately USD \$14.7 million), were sent to bank accounts around the world in February 2019. Coconspirator 1 conspired with the persons who initiated the fraudulent wire transfers, and also conspired with a number of others, including ABBAS, to launder the funds that were intended to be stolen. ABBAS, specifically, provided Coconspirator 1 with two bank accounts in Europe that ABBAS anticipated would each receive €5 million of the fraudulently obtained funds.

7. Other communications between ABBAS and Coconspirator 1 indicate that, in addition to these schemes, ABBAS and Coconspirator 1 conspired to launder tens, and at times hundreds, of millions of dollars that were proceeds of other fraudulent schemes and computer intrusions, including a fraudulent scheme to steal £100 million from an English Premier League football club.

III. STATEMENT OF PROBABLE CAUSE

A. Identification of ABBAS

8. Analysis of Coconspirator 1’s iPhone and other online accounts showed that Coconspirator 1 operated and tasked money mule crews for a number of fraudulent schemes, including BEC schemes and cyber-heists. Analysis also showed that Coconspirator 1 communicated with the U.A.E. phone number +971543777711 (“Phone Number 1”) about multiple fraudulent schemes and money laundering. As described below, Phone Number 1 was one of the phone numbers ABBAS used during 2019 and 2020.

9. Based on my review (pursuant to federal search warrants obtained in this District) of data from Coconspirator 1's iPhone and from an online account connected to that phone (the "Online Account"), other law enforcement personnel's review of that digital data, and from discussions with United States Secret Service ("USSS") and FBI personnel, I know the following:

a. Coconspirator 1's iPhone listed Phone Number 1 (+971543777711) with the contact name "Hush." The phone also contained a contact for Snapchat username "hushpuppi5," which listed the Snapchat contact name "The Billionaire Gucci Master!!!"

b. Searches of Phone Number 1 and the contact name "Hush" in Coconspirator 1's iPhone revealed messaging conversations between "Hush," using Phone Number 1, and Coconspirator 1. (For ease of reference, communications with this moniker and Phone Number 1 are referred to as communications with ABBAS in the remainder of this affidavit.)

10. In or around December 2019, April 2020, and June 2020, I reviewed the publicly viewable Instagram account of "hushpuppi" at www.instagram.com/hushpuppi. Based on information available on the profile page, the user of that account made more than 500 posts and had 2.3 million followers as of June 2020.

11. This Instagram account included numerous publicly viewable images of a man who appeared to be ABBAS, based on comparisons to photographs of ABBAS in passports and other identification documents referenced below in paragraphs 16.c to 16.c.iv. Hundreds of these images on the Instagram account showed ABBAS in designer clothing and shoes, posing on or in luxury vehicles, wearing high-end watches, or possessing other luxury items, indicating substantial wealth.

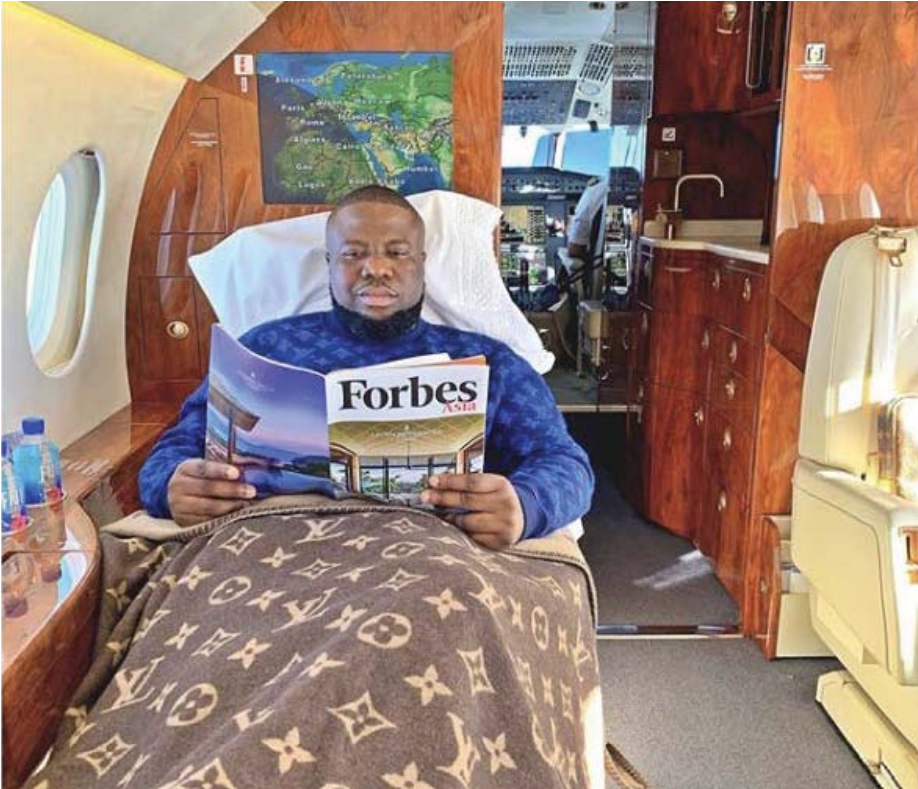
a. For example, on June 6, 2020, ABBAS posted a photograph of a white Rolls Royce Cullinan that included the hashtag “#AllMine.” On February 27, 2019, ABBAS posted a photograph of himself in front of two vehicles, one of which he described as his new Rolls Royce Wraith. Based on review of publicly available pricing information, the starting price for each of these vehicles is approximately \$330,000.

b. More than two dozen images showed ABBAS in front of, on top of, or inside other luxury vehicles, including multiple models of Bentley, Ferrari, Mercedes, and Rolls Royce.

c. On numerous occasions, ABBAS posted photos of himself wearing items and/or holding shopping bags from luxury stores such as Gucci, Louis Vuitton, Chanel, Versace, Fendi, and more.

d. On multiple dates, including April 17, 2020, June 19, 2019, and July 1, 2019, ABBAS posted images of himself inside or in front of private jets. Multiple photographs also appeared to show ABBAS posing in locations around the world (such as Dubai and Paris).

e. The following photographs are from review of ABBAS' Instagram account.





12. This Instagram profile also claimed that the user was a real estate developer and listed the user's Snapchat account as "Hushpuppi5," which is the same Snapchat account name that was saved in Coconspirator 1's iPhone (see paragraph 9.a).

13. Based on records from Instagram received in June 2020, the Instagram account was subscribed with the name "RAY," the email address rayhushpuppi@gmail.com, and the verified phone number +971502818689 ("Phone Number 2"). The Instagram account was created on October 10, 2012, and recent account history from 2020 showed logins from Internet Protocol ("IP") addresses located in the U.A.E.² (ABBAS lives in the U.A.E., based on

² Based on my training and experience, I know that an Internet Protocol version 4 address, also known as an "IPv4 address," or more commonly "IP address," is a set of four numbers, each ranging from 0 to 255 and separated by a period (".") that is used to route traffic on the internet. A single IP address can

information from his email and social media accounts, financial records, and internet research, some of which is further discussed below.)

14. Based on subscriber records from Snap Inc., the Snapchat account “Hushpuppi5” used the phone number +971565505984 (“Phone Number 3”) and the email address rayhushpuppi@gmail.com (i.e., the same email as the Instagram account). The Snapchat account used the display name “The Billionaire Gucci Master!!!,” which was the same Snapchat contact name saved in Coconspirator 1’s phone for the Snapchat account “Hushpuppi5.”

15. Records from Apple Inc. showed the following:

a. The email account rayhushpuppi@gmail.com was used to create an Apple account on March 29, 2014, which was active as of May 2020, and used the subscriber name “Ray Hushpuppi.”

b. The same email account was used in subscriber records of another Apple account, which account records also listed the email address rayhushpuppi@icloud.com and another Google account.

c. Phone Number 1 was listed in the subscriber records of a third Apple account, which was created on November 7, 2019. The account listed the subscriber name “Godisgood Godson” and the verified email address godisgoodallthetime0007@gmail.com. Despite using that subscriber name, the name “Ramon Abbas” (i.e., ABBAS) was listed in account records in December 2019 and January 2020. Apple records further listed a user’s address as 1706 Palazzo Versace, in Dubai, U.A.E. (the “Palazzo Versace” address).

manage internet traffic for more than one computer or device, such as when a router in one’s home routes traffic to one’s desktop computer, as well as to one’s tablet or smartphone, while all using the same IP address to access the internet. IP addresses can be used to establish a person’s approximate—or, at times exact—geographic location.

i. Records from Google for ABBAS' email address rayhushpuppi@gmail.com, which are described more below, included a lease renewal/tenancy contract for the Palazzo Versace address for April 4, 2020 through May 3, 2021, which also listed Phone Number 3. Posts on ABBAS's Instagram page also suggested that he lived at the Palazzo Versace apartments in Dubai, U.A.E., including one that listed the location "Palazzo Versace Dubai."

ii. Google records, in turn, indicated that the email account godisgoodallthetime0007@gmail.com, which used the subscriber name "Godisgoodallthetime GraciousGod," was both created and last logged into on November 7, 2019. This email account was accessed on November 7, 2019 from an IP address that geo-locates to the U.A.E. Google records for this account also included several Apple invoices billed to ABBAS, which used the Palazzo Versace address as the billing address.

16. Based on my review and an FBI computer scientist's review of Google account records for rayhushpuppi@gmail.com, obtained through legal process and a federal search warrant in this District, I know the following:

a. The account used the subscriber name "Ray HushPuppi" and was created on September 19, 2013. Additionally, the recovery email listed was rayhushpuppi@icloud.com, and the recovery phone number was Phone Number 2.

b. Multiple emails in the email account rayhushpuppi@gmail.com confirmed that ABBAS used Phone Number 1, Phone Number 2, and Phone Number 3.

i. As noted above, on April 6, 2020, an email sent to rayhushpuppi@gmail.com contained a tenancy contract for the Palazzo Versace address, with ABBAS listed as the tenant and Phone Number 3 as his phone number.

ii. On February 6, 2020 and March 3, 2020, rayhushpuppi@gmail.com was used to send Phone Number 1 to other persons, which the account user described as “my mobile number” and “my phone number,” respectively.

iii. On December 13, 2019, a booking confirmation sent to rayhushpuppi@gmail.com contained ABBAS’ full name, the Palazzo Versace address, and Phone Number 3.

iv. On August 14, 2019, an email sent to rayhushpuppi@gmail.com containing a flight itinerary for ABBAS also listed Phone Number 2.

v. On July 11, 2019, an order receipt sent to rayhushpuppi@gmail.com contained ABBAS’ name, the Palazzo Versace address, and Phone Number 2.

vi. On May 26, 2019, rayhushpuppi@gmail.com was used to send an email containing ABBAS’ name as well as Phone Number 1 and Phone Number 2 as contact numbers.

vii. On May 25, 2019, rayhushpuppi@gmail.com was used to send an email (regarding a U.A.E. bank transaction that was blocked) and the sender listed Phone Number 2.

viii. On February 5, 2019, an online order confirmation email sent to rayhushpuppi@gmail.com included both ABBAS’ name and Phone Number 1.

ix. On November 4, 2018, an email containing a flight itinerary for ABBAS also listed Phone Number 3.

c. Multiple emails in the email account also contained photographs or scans of several foreign identification documents for ABBAS.

i. On September 12, 2017, rayhushpuppi@gmail.com sent a photograph of the Federal Republic of Nigeria passport of ABBAS, with a passport number ending in 2132. The passport was issued in Malaysia in 2015, stated that ABBAS is a Nigerian citizen, and listed ABBAS' birthday as October 11, 1982.

(I) The photograph of this Nigerian passport was included with a photograph of a U.A.E. Resident Identity card in ABBAS' name, containing his picture and an ID number ending in 9431. The email transmitting both photographs stated that they were the sender's "identity and passport page followed by my real Instagram page." Consistent with that statement, the email also included a screenshot of the Instagram account @hushpuppi, which also showed the Snapchat username "Hushpuppi5."

ii. On February 23, 2020, rayhushpuppi@gmail.com sent an email containing a photograph of a different Federal Republic of Nigeria passport of ABBAS, with a passport number ending in 5915, as well as a U.A.E. visa with the same resident ID number ending in 9431. Both the passport and U.A.E. visa are pictured below.

iv. The photographs on these four identifications were consistent with each other and were also consistent with photographs I have seen of ABBAS, including photographs on his publicly viewable social media accounts described in this affidavit.

d. The email account rayhushpuppi@gmail.com also contained photographs or scans of foreign identification documents of approximately 13 persons other than ABBAS, of different nationalities (including Nigeria, U.K., Kenya, U.A.E., U.S.A., and Pakistan).

e. Based on bank statements and transaction confirmations found in the email account rayhushpuppi@gmail.com from June 2016 to April 2020, ABBAS had financial accounts in Nigeria and the U.A.E. in his name. Moreover, emails from rayhushpuppi@gmail.com also showed that ABBAS conducted financial transactions and/or transfers with individuals believed by the FBI to be coconspirators, including a target of an investigation by the FBI in Chicago. Transaction confirmation emails included transfer amounts and the name of the sending or receiving accounts for those transfers.

f. The email account rayhushpuppi@gmail.com also contained emails with attachments relating to wire transfers in large dollar values, including wire transfers in February 2018 in the amounts of \$250,000 and \$2,397,000. Based on the context of the emails, as well as other information gathered during the FBI investigation about one of the sender email accounts, it appears that these emails were related to fraudulent transactions.

17. Other financial records corroborate ABBAS' identity.

a. Records from Western Union indicate that two money transfers—one listing Phone Number 1 and one listing Phone Number 3—occurred in UAE in 2018, in which the sender was listed as ABBAS, with a birthdate of October 11, 1982, and using an identification bearing the same

number (ending in 9431) as the U.A.E. Resident Identity card, referenced in paragraph 16.c.i(I).

b. That same U.A.E. Resident Identity card was also used in connection with two MoneyGram transactions in 2018, in which ABBAS, who again listed a birthdate of October 11, 1982 and address in U.A.E., received funds. In those two transactions, as well as several other transactions through MoneyGram, ABBAS listed Phone Number 3.

18. Other evidence corroborates that ABBAS' birthdate is October 11, 1982, and that he is "Ray Hushpuppi."

a. A United States non-immigrant visa application submitted in December 2012 listed ABBAS' full name and his birthdate as October 11, 1982.

b. Moreover, on April 14, 2020, I reviewed information publicly viewable on the profile of the above-referenced "hushpuppi" Instagram account that is consistent with ABBAS' birthdate being on or about October 11. Specifically, on October 12, 2018, the account posted an image of a birthday cake with the inscription "Happy Birthday" and included the caption "Thank you all so much for the love you showed me yesterday till now. I love you all and thanks @fendi @mohammedabdelnabi for the cake. God bless you all." I also saw a post, on October 11, 2017, by that Instagram account of a birthday cake with the inscription "Happy Birthday Ramon" and the caption "Thanks so much @gucci for this special. God bless you guys at the Dubai Mall Gucci Store!!!"

B. The Victim Law Firm

19. In reviewing data from Coconspirator 1's iPhone, I and another FBI employee saw messages reflecting that, in or around October 2019, ABBAS had conspired with Coconspirator 1 and Coconspirator 2 to commit a fraudulent wire transfer and money-laundering scheme, in which a U.S. victim (the "Victim Law

Firm”) lost approximately \$922,857.76. The messages reflected that part of the scheme, including acts in furtherance of the conspiracy, occurred while Coconspirator 2 was physically present in the Central District of California.

20. Records obtained from JPMorgan Chase Bank (“Chase”) for a bank account held in the U.S. (the “Chase Account”) reflect that the Chase Account received a wire transfer on October 15, 2019 for approximately \$922,857.76 from the Victim Law Firm. On October 17, 2019, there was a wire transfer from the Chase Account to an account at Canadian Imperial Bank of Commerce (“CIBC”), in Toronto, Ontario, for approximately \$396,050. Bank records reflect that the specific account at CIBC ended in 1716 (the “CIBC Account”), consistent with what is discussed below in paragraphs 21, 24, and 25. The remaining funds in the Chase Account were transferred to other accounts.

21. Based on review of data from Coconspirator 1’s iPhone, on or around October 17, 2019, ABBAS, using what appeared to be the Snapchat account “hushpuppi5,” sent an image of a Chase wire confirmation to Coconspirator 1. The image appeared to show a wire transfer form related to a transfer of approximately \$396,050 from the Chase Account to the CIBC Account, which, based on other messages on Coconspirator 1’s iPhone, appears to have been held by Coconspirator 2.³

22. On April 14, 2020, I interviewed S.R., owner of the Victim Law Firm, about the above-referenced wire sent on October 17, 2019. On April 16, 2020, I interviewed N.C., who was an attorney and co-worker of S.R., and on May 21, 2020, I interviewed K.C., a paralegal of the Victim Law Firm. Based on these interviews, I learned the following:

³ The “Sender” information in the image was blocked by a Chase bank business card, but other bank records show that this transaction involved the Chase Account.

a. The Victim Law Firm, which is located in New York State, was representing a client, A.D., in the refinance of real estate.

b. A.D. was refinancing his/her property with Citizens Bank. As part of the closing for this refinance, on October 15, 2019, K.C. sent a verification email to what appeared to be a Citizens Bank email address (later identified as a “spoofed” email address) requesting wire instructions. Per internal policy of the Victim Law Firm, all wire verifications were to be sent to their firm via fax and followed-up by a phone call. K.C. received a fax message in response to her verification email with what was later determined to be fraudulent wire instructions to transfer the loan payoff amount of their client A.D. to the Chase Account. K.C. then called the phone number listed on the fax to verify the wire instructions.

c. On October 15, 2019, K.C. initiated the wire transfer to the Chase Account for approximately \$922,857.76.

d. Neither the Victim Law Firm, nor their client A.D., realized the funds had been fraudulently transferred to the Chase Account until later in October 2019, when A.D. checked his/her account and realized that the funds for the refinance had not been credited. By this time, all of the funds had been depleted from the Chase Account. (I further understand from K.C. that, as of June 25, 2020, no funds had been recovered.)

23. Messages on Coconspirator 1’s iPhone reflect that, at approximately the same time on October 17, 2019 that ABBAS sent Coconspirator 1 an image of the wire transfer confirmation for the transaction from the Chase Account to the CIBC Account, Coconspirator 1 was communicating with another phone number to confirm the wire had been deposited into the CIBC Account. Based on other messages on the iPhone and records obtained by the FBI, that phone number was used by Coconspirator 2.

24. The communications between Coconspirator 1 and Coconspirator 2 on October 17, 2019 included the following messages:

Coconspirator 1: Keep lookout for the 396 and so ur
thing till u hear from me

Coconspirator 2: Ok will do

Coconspirator 2: I'm in La so how can I make sure??⁴

25. Coconspirator 2 also sent Coconspirator 1 a photograph showing a secure login to the CIBC Account in Coconspirator 2's name. The account number ended in 1716, consistent with the account number that ABBAS sent to Coconspirator 1 in an image on October 17, 2019.

26. I reviewed international travel records from a law enforcement database, which showed that Coconspirator 2 traveled from Toronto, Canada to Los Angeles, California on October 16, 2019. This was one day before the wire transfer from the Chase Account to the CIBC Account in Coconspirator 2's name. Further, as referenced above, Coconspirator 2 messaged Coconspirator 1 on October 17, 2019 that "I'm in La." Travel records also show that Coconspirator 2 departed Los Angeles around October 23, 2019 for Canada. Taken together, this indicates that Coconspirator 2 was in Los Angeles at the time of the wire transfer.

27. Later in the day on October 17, 2019, while still in Los Angeles, Coconspirator 2 appeared to confirm the wire transfer in an iMessage found on Coconspirator 1's iPhone:

Coconspirator 1: Did the big hit?

Coconspirator 2: Yessir

⁴ Where there are grammatical and spelling errors in the text when this affidavit quotes ABBAS, Coconspirator 1, and Coconspirator 2, those errors are in the original messages.

28. After Coconspirator 2 appeared to confirm to Coconspirator 1 that the money was transferred to the CIBC Account, Coconspirator 1 appeared to provide confirmation back to ABBAS, within a minute:

ABBAS: Sup bro
Coconspirator 1: Confo u sent me today
Coconspirator 1: Landed
Coconspirator 1: Just nown

29. Coconspirator 1 then wrote that he was on an airplane and had just landed. A few seconds later, ABBAS asked, “Money came in?,” and Coconspirator 1 responded, “Yes [¶] For Canada.”

30. ABBAS then demanded, “Give me a screenshot.” Coconspirator 1 stated that he was not able to because his Wi-Fi signal was not strong enough, but promised to send a screenshot.

a. I know, based on my training and experience, that persons involved in fraudulently obtaining and laundering funds from BEC schemes and other online fraud schemes often request confirmation of fraudulent transactions, including in the form of screenshots or photographs showing proof that the funds were transferred.

31. Based on my review of messages, Coconspirator 1 ultimately did not send that screenshot. I know from law enforcement agents that Coconspirator 1 was arrested on or about October 17, 2019, in a U.S. airport, on a federal arrest warrant, shortly after sending his last message to ABBAS.

C. The Foreign Financial Institution

32. Based on information from FBI agents investigating the cyber-heist from the Foreign Financial Institution, I know that, on February 12, 2019, the Foreign Financial Institution suffered a computer intrusion and cyber-heist in

which approximately €13 million (approximately \$14.7 million) was fraudulently wired from the Foreign Financial Institution to bank accounts in multiple countries.

33. Coconspirator 1 and ABBAS, who used Phone Number 1 in these communications, exchanged messages discussing the cyber-heist from the Foreign Financial Institution. Based on my review of data from Coconspirator 1's iPhone and his Online Account, and discussions with FBI special agents and other law enforcement personnel familiar with this investigation, I know the following:

a. In a message on January 16, 2019, Coconspirator 1 contacted ABBAS asking for two European bank accounts that could receive "5m euro" (€5 million), which he said would be from the country in which the Foreign Financial Institution is located (the "Foreign Financial Institution Country"). Coconspirator 1 stated several times that the "hit" would occur on February 12.

b. After some discussion, ABBAS sent Coconspirator 1 the account information for a Romanian bank account, which he said could be used for "large amounts."

c. ABBAS further said he could provide another account, and Coconspirator 1 said that it would be a payment of "5m"—i.e., €5 million—to each account.

d. On February 1, 2019, Coconspirator 1 told ABBAS that a coconspirator said that "12th February they doing it[.] I have 4 spots Available[.] u gave me 1/4[.] try to get me a next one pls it will both done at once."

Coconspirator 1 also sent ABBAS a photograph of a computer screen containing a messaging conversation which discussed a February 12 "drop" and a "cashout."

e. On February 7, 2019, Coconspirator 1 told ABBAS, "12th feb they lunching [sic "launching"] the swift I need 1 more from you pls."

Coconspirator 1 later explained, "I have 6 slots in total [¶] All 5m Euro [¶] Big hit in 12th feb [¶] They will all credit same time."

i. SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized, and reliable environment. SWIFT also sells software and services to financial institutions, much of it for use on the SWIFTNet network. SWIFT does not facilitate funds transfers. Rather, it sends payment orders, which must be settled by correspondent accounts that the institutions have with each other. Each financial institution, to exchange banking transactions, must have a banking relationship by either being a bank or affiliating itself with one (or more) bank(s) so as to enjoy those particular business features.

ii. I further know, based on my experience with this investigation, and from FBI agents investigating Coconspirator 1 and other targets, that hackers sometimes will attempt to conduct cyber-heists by gaining access to a bank's computer network and then sending fraudulent and unauthorized SWIFT messages.

f. On February 10, 2019, Coconspirator 1 told ABBAS, "Brother tonight is my dead line to submit anything more," and then asked, "Do u want add one more or just stick to that one u gave me ?" The next day, ABBAS responded, and provided account information for another bank account in Bulgaria.

g. A photograph, dated February 13, 2019, found in Coconspirator 1's Online Account showed a computer screen with a messaging conversation in which Coconspirator 1 and another person discussed a number of "drops," *i.e.*, bank accounts that could receive fraudulent funds. One participant said that there could only be "1 euro" drop, and they then discussed how many of Coconspirator 1's drops would be used. The username known to be used by Coconspirator 1 stated, "I have 3 euro 1 usa [¶] 2 romania 1 bulgaria 1 usa."

h. On February 12, 2019, Coconspirator 1 told ABBAS, “Wire is completed . . . We did it [¶] 500k euro [€] [¶] Should be on ur side by now.”

i. In the conversation that followed, Coconspirator 1 told ABBAS that there was only one wire to the account in Romania, “Sender name : tipico group limited [¶] Country : [Foreign Financial Institution Country] [¶] Amount : 500k euro. . . It’s there now my other crew confirmed it’s there as well[.]” Later, while they were trying to figure out whether the wire had been successful, Coconspirator 1 added, “They did me 3 wires (2 to euro 1 to USA) . . . Bank it came from is :[Foreign Financial Institution] . . . Brother, we still have access and they didn’t realize , we gonna shoot again tomoro am.” ABBAS then confirmed that Coconspirator 1 was saying that the new wire would be sent to the second bank account he provided to Coconspirator 1, in Romania.

j. An image of a conversation saved in Coconspirator 1’s Online Account, dated February 12, 2019, with a person other than ABBAS, discussed a payment specifically from the Foreign Financial Institution. The conversation in the image stated, “my guy also deleted history logs at the bank so they won’t even c the transaction.”

k. The next day, February 13, 2019, after ABBAS sent screenshots showing that the funds had not arrived in the Romanian bank account, Coconspirator 1 responded, “Today they noticed and pressed a recall on it , it might show and block or never show.” Coconspirator 1 then sent an image of a news article to ABBAS detailing the theft of funds from the Foreign Financial Institution, followed by a message stating “Look it hit the news.” ABBAS then replied “damn.”

l. Coconspirator 1 then wrote to ABBAS: “Next one is in few weeks will let U know when it’s ready. to bad they caught on or it would been a nice payout.”

D. Additional Fraudulent Schemes and Attempted Money Laundering

34. In addition to participation in those fraudulent schemes, ABBAS and Coconspirator 1 discussed additional BEC frauds and/or other fraudulent schemes in 2019. These included schemes where ABBAS and Coconspirator 1 sought to fraudulently obtain millions—and, at times, hundreds of millions—of U.S. dollars and U.K. pounds sterling, as described below.

35. On March 10, 2019, Coconspirator 1 requested a bank account in the U.A.E. from ABBAS into which approximately \$5 million could be deposited from a victim in the United States. Coconspirator 1 told ABBAS that the “job” would be “Monday am USA time,” and, after some discussion, wrote, “Brother I need it now or we will lose our chance pls.” ABBAS responded by providing bank account information for an account at Commercial Bank International in Dubai, U.A.E.

36. On April 30, 2019, Coconspirator 1 told ABBAS, “Brother I have 4 company’s in uk ready to switch bank acc on file but acc has to be open beneficiary.” After some discussion, Coconspirator 1 further stated, “I have a room working for me , we have leads and company contracts . My guy r changing acc on file for 100m contracts and there payment are once or twice a week 1-5m [¶] I have 4 ready to switch up.”

a. Based on my training and experience, it appears Coconspirator 1 was referring to a BEC scheme, because BEC schemes often involve a hacker or fraudster tricking a victim into sending a payment to a coconspirator’s account by switching bank account information on payment instructions provided to the victim. I also know that an “open bene” or “open beneficiary” account is a bank

account where a different business account name can be substituted to help in deceiving the victim into sending funds.

b. It thus appears that Coconspirator 1 was telling ABBAS that coconspirators were fraudulently obtaining \$1 million to \$5 million through a BEC scheme once or twice a week, and was asking ABBAS for a bank account that could be used to receive such funds.

37. On May 3, 2019, Coconspirator 1 told ABBAS, “I need uk open beneficiary acc for Monday bro !!!!! [¶] Today I they paid me.” Coconspirator 1 also sent ABBAS an image of a message from another person saying, “Yo [¶] 3 invoices totaling 1.1 M going into that account today . . . 346k 256k and 507k.” Coconspirator 1 then said, “Bro I have a room ready.” In the resulting discussion, Coconspirator 1 told ABBAS that he was “doing invoice account swap” and needed “account open beneficiary.” When ABBAS asked, “Which country,” Coconspirator 1 responded, “U tell me what country is best i attack [¶] But [¶] I have uk [¶] Ready live.”

38. On May 7, 2019, Coconspirator 1 sent ABBAS a photograph of an apparent banking website showing a transaction “due to be paid” of approximately 1,110,447 of some currency, which is around the same amount as the discussion described in the prior paragraph. Coconspirator 1 then wrote, “I sent 1.1m pound to acc they said open ben in uk money landed and now they asking questions ♂ I have other companies ready to swap bro pls help me out I am losing millions.” ABBAS then stated, “I will paste u one today,” and Coconspirator 1 responded, “When we swap bro the only thing we change is iban or acc on file and we keep all other info as original but we can put acc name on the memo , u need acc that can handle millions and not block.” The next day, after Coconspirator 1 stated, “Brother my guy can do refund to any visa debit card [¶] Just need card number exp and name,” ABBAS and Coconspirator 1 had some additional discussion that

appeared to be about credit card numbers, culminating with ABBAS providing bank account information for an account in Mexico.

39. On May 12, 2019, Coconspirator 1 wrote to ABBAS, “Brother tonight we are gonna swap ur acc on a big contract payments will be 3-6m every week [¶] I give u confirmation in 12he [¶] From uk.” After ABBAS acknowledged the message, Coconspirator 1 wrote on May 13, 2019, “Your acc has been updated on file , give me 2hr I will send unall details my workers just went to sleep.” ABBAS responded, “Waiting.”

40. Coconspirator 1 then sent messages to ABBAS about the apparent victims. First, Coconspirator 1 sent the name of an English Premier League football club, listing the club’s address as the stadium where the club plays. Coconspirator 1 also wrote, “Amount 100M £,” indicating that the fraudulent transaction would be for £ 100 million. Second, Coconspirator 1 sent the name of a U.K. company with an address in Edinburgh, Scotland, and wrote, “Amount 200m £.” Coconspirator 1 then added, “We swapped ur acc under 2 contracts . Tomorrow morning we will send u the previous payment and amount with future paymanet and amount [¶] Can I have 1 more for tomorow to swap pls.”

41. In response, ABBAS stated, “Bro [¶] I can’t keep collecting houses n not give them a feed back n keep asking for more [¶] This things cost a lot of money now to open.” ABBAS and Coconspirator 1 then discussed the use of the account, and Coconspirator 1 sent a photograph of a computer screen showing the Mexican bank account information with the name of a U.K. company, with a U.K. address, substituted as the beneficiary information. ABBAS responded, “When it’s done let me know.”

a. I know based on my training and experience, and from other FBI agents who have experience with these matters, that Nigerian-origin subjects sometimes use the words “aza” (sometimes “azar,” “azza,” or “azah”) or “house”

to refer to a bank account used to receive proceeds of a fraudulent scheme. The word “house” is also sometimes used to refer to a bank itself. I observed that, in other messages with ABBAS, Coconspirator 1 used the term “azza,” in addition to using the term “house.” (While Coconspirator 1 is not Nigerian, he is known to have communicated with multiple Nigerian-origin coconspirators.)

42. On July 3, 2019, Coconspirator 1 reported to ABBAS, “Brother I can’t send from uk to Mexico they keep finding out , but uk 2 uk these guy keep paying and I can show u my last week cashout.” He also added that another coconspirator “has acces to a European bank and want to initiate a MT103/202 10-50 million if u know about it.”

a. I know based on my training and experience that MT103 and MT202 are types of SWIFT messages. It thus appears that Coconspirator 1 was referencing a cyber-heist scheme in which a coconspirator would be able to make fraudulent transfers of 10 million to 50 million in dollars or euros.

//

//

//

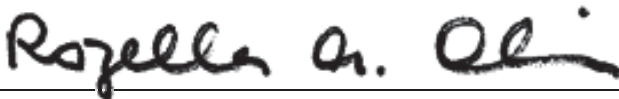
IV. CONCLUSION

43. For all the reasons described above, there is probable cause to believe that ABBAS has committed a violation of 18 U.S.C. § 1956(h) (Conspiracy to Engage in Money Laundering).

/S/

ANDREW JOHN INNOCENTI
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on June 25, 2020.



THE HONORABLE ROZELLA A. OLIVER
UNITED STATES MAGISTRATE JUDGE