AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Jersey

ORIGINAL FILED

SEP - 3 2019

WILLIAM T. WALSH, CLERK

United States of America
v.
RUBBIN SARPONG

Case No. 19-2059 (JS)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Jan. 2016 through Sept. 3, 2019 in the county of Cumberland in the _____ District of New Jersey, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 1349	Wire fraud conspiracy, as more fully described in Attachment A

This criminal complaint is based on these facts:

See Attachment B.

☑ Continued on the attached sheet.

Complainant's signature

Special Agent Dean J. DiPietro, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/03/2019

Judge's signature

City and state: Camden, NJ

Hon. Joel Schneider, U.S. Magistrate Judge

Printed name and title

CONTENTS APPROVED

UNITED STATES ATTORNEY

By:_____
DIANA VONDRA CARRIG
Assistant U.S. Attorney

Date: September 3, 2019

ATTACHMENT A

CONSPIRACY TO COMMIT WIRE FRAUD
(18 U.S.C. § 1349)

From at least as early as January 2016 through on or about September 3, 2019, in the District of New Jersey, and elsewhere, the defendant

RUBBIN SARPONG,

did knowingly and intentionally conspire and agree with uncharged co-conspirators, Co-Conspirator 1, Co-Conspirator 2, Co-Conspirator 3, and others in the devise of scheme and artifice to defraud Victims 1 through 30, and others, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, including but not limited to, the wire transactions set forth below and as further described in Attachment B:

VICTIM	DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
Victim 1	12/6/17	$10,000	Santander	-2889	SARPONG
Victim 1	12/13/17	$20,000	Santander	-2889	SARPONG
Victim 1	12/19/17	$17,400	Santander	-2889	SARPONG
Victim 1	1/3/18	$48,000	Santander	-2889	SARPONG
Victim 1	1/10/18	$39,850	Santander	-2889	SARPONG
Victim 2	5/22/18	$2,860	Santander	-1851	SARPONG

VICTIM	DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
Victim 2	5/30/18	$5,600	Santander	-1851	SARPONG
Victim 2	6/1/18	$28,400	Santander	-1851	SARPONG
Victim 2	6/11/18	$15,150	Santander	-1851	SARPONG
Victim 2	6/12/18	$22,800	Santander	-1851	SARPONG
Victim 5	5/7/18	$18,300	Santander	-2889	SARPONG
Victim 5	5/8/18	$14,890	Santander	-2889	SARPONG
Victim 5	5/15/18	$18,900	Santander	-2889	SARPONG
Victim 5	5/31/18	$25,500	Santander	-2889	SARPONG
Victim 5	6/5/18	$17,800	Santander	-2889	SARPONG
Victim 8	11/18/16	$2,800	M&T Bank	-7517	SARPONG
Victim 8	11/23/16	$7,800	M&T Bank	-7517	SARPONG
Victim 8	11/28/16	$5,460	M&T Bank	-7517	SARPONG
Victim 8	12/02/16	$13,500	M&T Bank	-7517	SARPONG
Victim 8	12/03/16	$7,900	M&T Bank	-7517	SARPONG
Victim 8	12/09/16	$46,800	M&T Bank	-7517	SARPONG
Victim 8	12/27/16	$10,000	Fulton Bank of NJ	-5749	SARPONG
Victim 8	01/09/17	$1,500	Fulton Bank of NJ	-5749	SARPONG
Victim 8	01/23/17	$2,000	Fulton Bank of NJ	-5749	SARPONG

Contrary to Title 18, United States Code, Section 1343, in violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Dean J. DiPietro, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since June 1998. I am currently assigned to the Newark Division, Atlantic City Resident Agency's White Collar Crime squad, where my primary assignment is to investigate complex financial crimes. I was previously assigned to an Organized Crime/Drug squad where I was the Task Force Commander for the South Jersey Violent Incident and Gang Task Force for approximately 10 years. During my 21-year career in federal law enforcement, I have participated in, and conducted, many criminal investigations involving violations of the laws of the United States, including but not limited to laws relating to false, fictitious, and fraudulent claims, wire fraud, mail fraud, money laundering, and computer-related offenses. I have completed specialized training through the Federal Bureau of Investigation, Economic Crimes Unit and the Asset Forfeiture/Money Laundering Unit. Through this training and experience, I have become familiar with a wide variety of fraudulent schemes and the federal statutes proscribing such fraudulent activity. I have not included every detail or every aspect of my training, education, and experience but have highlighted those areas most relevant to this application.

2. The information contained in this Affidavit is based upon my

personal knowledge and observation, my training and experience, conversations with other law enforcement officers (including officers who have engaged in numerous investigations involving fraud, money laundering, and computer-based crimes), victim interviews, and the review of documents and records. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to issue a complaint, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to support the charge in the complaint. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part.

SUMMARY OF ROMANCE FRAUD SCHEME

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that RUBBIN SARPONG (hereafter "SARPONG") and uncharged CO-CONSPIRATOR 1 (hereafter "CC1"), CO-CONSPIRATOR 2 (hereafter "CC2"), CO-CONSPIRATOR 3 (hereafter "CC3"), and others (hereafter collectively referred to as "the co-conspirators"), knowingly participated in an online romance fraud scheme, in which they defrauded unsuspecting victims in New Jersey and elsewhere, and then laundered the proceeds through various bank accounts in New Jersey and elsewhere to avoid detection and distribute proceeds from the scheme to co-conspirators in Ghana.

4. From at least as early as January 2016 through the present, the

investigation has identified more than 30 victims,[1] with a collective loss amount exceeding $2.1 million. Based upon the investigation to date, the conduct of the co-conspirators and the nature of the conspiracy, I have probable cause to believe that the conspiracy is ongoing.

5. In general, the co-conspirators committed the scheme by setting up dating profiles on various dating websites using fictitious or stolen identities posing as United States military personnel who were stationed overseas. They contacted victims through the dating websites and then pretended to strike up a romantic relationship with them, wooing them with words of love. As part of their scheme, the co-conspirators also created numerous email accounts and Voice over Internet Protocol (hereafter "VoIP") phone numbers, which they used to communicate with victims.

6. After establishing virtual romantic relationships with victims on the online dating platforms and via email, the co-conspirators asked for money from victims, often for the purported purpose of paying to ship gold bars to the United States. Although the stories varied, most often the co-conspirators claimed to be members of the United States military stationed in Syria who received, recovered, or were awarded gold bars. The co-conspirators told many victims that their money would be returned once the gold bars were received in the United States.

7. The co-conspirators used a myriad of email accounts they created

---

[1] When described separately the victims will be referred to as VICTIM 1, VICTIM 2, etc.

to provide victims with instructions on where to wire money, including recipient names, addresses, financial institutions, and account numbers. The co-conspirators also provided various email accounts to financial institutions in conjunction with opening bank accounts used in the fraud, and in communicating with such banks.

8. Defendant SARPONG was one of several recipients in the United States who received victim funds. As instructed, victims wired money to bank accounts held by SARPONG and others, at financial institutions in the United States. Occasionally, victims also mailed personal checks and/or cashier's checks to the co-conspirators and also transferred money to the co-conspirators via money transfer services, such as Western Union and MoneyGram. A review of financial records obtained in conjunction with the investigation revealed the fraudulently obtained funds were not used for the purposes claimed by the co-conspirators – that is, to transport non-existent gold bars to the United States, but were instead withdrawn in cash, wired to other domestic bank accounts, and wired to other co-conspirators in Ghana.

THE DEFENDANT AND HIS CO-CONSPIRATORS

RUBBIN SARPONG

9. SARPONG resides in an apartment in Millville, New Jersey (the "SARPONG RESIDENCE"). SARPONG was born in Ghana and is a legal permanent resident of the United States.

10. Per records obtained by subpoena from Comcast, as of July 16, 2019, SARPONG was using phone number (XXX) XXX-5318 (hereafter "the

SARPONG PHONE"). As recently as July 10, 2019, SARPONG used the SARPONG PHONE to correspond with CC1, a co-conspirator residing in Ghana.

11. SARPONG used several email accounts in perpetrating the fraudulent scheme, including a gmail email account (hereinafter "SARPONG EMAIL 1"), from which he corresponded with banks, co-conspirators, and on at least one occasion a victim.

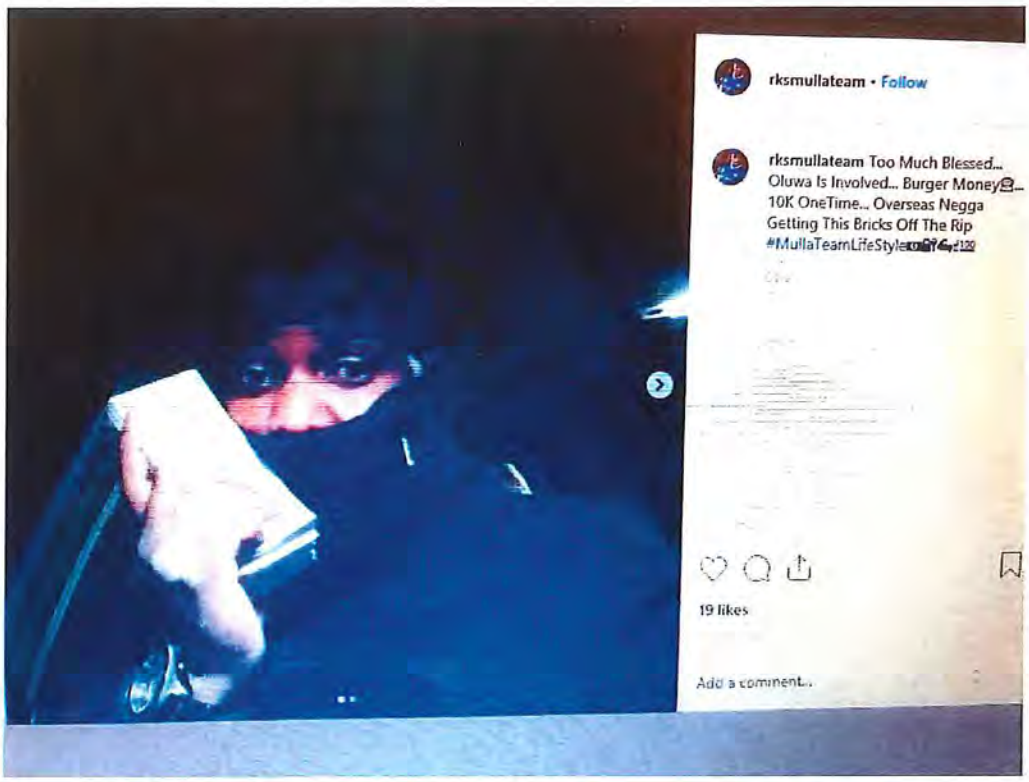
12. During the course of the conspiracy, SARPONG opened numerous bank accounts in his own name and a business name. SARPONG is also believed to have opened accounts in the names of others, including his father's name.

13. Of the 30 victims identified to date, 27 victims sent approximately $823,386 directly to SARPONG, primarily by wiring monies directly to bank accounts controlled by SARPONG or by transferring monies directly to SARPONG through money transmit services. SARPONG received much of the fraudulently obtained proceeds via bank wire transfer, and sometimes bank counter deposit, into a myriad of bank accounts he established at several financial institutions.

14. A review of bank records revealed that SARPONG transferred approximately $454,159 of victim proceeds to CC1, CC2 and others in Ghana.

15. In Facebook and Instagram accounts, SARPONG bragged about the money he was making by posting photographs of himself posing with large amounts of cash, as well as photographs of luxury vehicles and expensive designer clothing.

16. For example, on or about April 10, 2018, SARPONG posted a photograph on one of his Instagram accounts (hereafter, "SARPONG INSTAGRAM 1") of a picture of himself holding a large stack of cash with the caption "Too Much Blessed... Oluwa[2] Is Involved...Burger Money...10K OneTime...Overseas Negga Getting This Bricks Off The Rip#MullaTeamLifeStyle."



17. Per a review of bank records, a day earlier, on April 9, 2018, VICTIM 15 wired $21,441.72 to a bank account controlled by SARPONG. On April 10, 2018, SARPONG withdrew $8,000 in cash from the account. There is probable cause to believe that the stack of cash in the Instagram photograph was the $8,000 in victim proceeds that SARPONG withdrew from one of his

[2] Oluwa means "God" and originates from the Yoruba language in Nigeria.

bank accounts that morning.

CC1

18. CC1 resides in Ghana. Per a review of records from MoneyGram, CC1 used two phone numbers when receiving money transfers in Ghana from SARPONG and others in the United States.

19. From May 1, 2018 to September 6, 2018, SARPONG wired approximately $111,520 to bank account number ending in -1220, held by CC1 at Guaranty Trust Bank Ghana Ltd. SARPONG sent international outgoing wire transfers to CC1 within days of receiving money from victims.

20. For example, on or about June 1, 2018, SARPONG received a $28,400 incoming domestic wire transfer from VICTIM 2. On the same day, SARPONG sent an international outgoing wire transfer of $17,500 to CC1's bank account in Ghana. The purported purpose of the outgoing wire was "car payments."

21. A review of records obtained during the investigation, including bank records, email contents, subscriber information and IP logs, revealed that CC1 operated numerous email accounts, including a hotmail account (hereafter, CC1 EMAIL 1) and a gmail account (hereafter, CC1 EMAIL 2).

22. Based upon the investigation, there is probable cause to believe that CC1 controlled many of the Google and Mail.com email accounts described herein, which were used to correspond with victims. Specifically, correspondence was found between CC1's known email accounts (CC1 EMAIL 1 and CC1 EMAIL 2) and several of the email accounts used to communicate with victims.

CC2

23. CC2 resides in Ghana. From approximately October 2, 2017, to June 1, 2018, SARPONG wired approximately $239,700 to account numbers ending -3230 and -3220 at Guaranty Trust Bank Ghana Ltd., both held by CC2.

24. SARPONG sent international wire transfers to CC2 within days of receiving money from victims. For example, on or about May 7, 2018 and May 8, 2018, SARPONG received two incoming wire transfers from VICTIM 5 for $18,300 and $14,890, respectively. On May 9, 2018, SARPONG sent an international outgoing wire transfer of $16,000 to CC2 in Ghana. The purported purpose of the outgoing wire was "car payment."

CC3

25. CC3 is an American citizen and resides in southern New Jersey. CC3 received money and/or expensive electronic items from at least five victims. For example, from October 7, 2016 to October 20, 2016, CC3 received six MoneyGram transfers, totaling $6,900, from VICTIM 10 who also sent money to SARPONG. Additionally, on May 26, 2017, CC3 received a wire transfer of $9,650 from VICTIM 21. Then, on June 19, 2017, CC3 received a wire transfer of $9,200 from VICTIM 19.[3] Both victims wired funds to TD Bank account number ending in -1446, an account held by CC3 and for which CC3 had sole signatory authority. In sum, CC3 received approximately $28,750 from five victims.

[3] VICTIM 19 and VICTIM 21 also sent wire transfers to bank accounts held by SARPONG.

26. In addition to receiving victim money, a review of search warrant email records revealed that the co-conspirators instructed victims to send expensive electronic items to CC3. For example, the co-conspirators instructed VICTIM 12 to mail a computer to CC3, their "secretary," promising that the computer would be delivered to a soldier in Syria. On or about May 12, 2017, VICTIM 12 sent the computer to CC3 via United Parcel Service ("UPS"). The co-conspirators then requested that VICTIM 12 wire an additional $580 to CC3 to cover the cost of carrying the electronic equipment on the plane. In addition, the review of records from money transmit services, including MoneyGram, Western Union, and TransFast, revealed that CC3, like SARPONG, sent international money transfers to CC2, and others, in Ghana. For example, on July 6, 2019 and July 8, 2019, CC3 transferred $340 and $290, respectively, to CC2.

THE VICTIMS

27. Victim interviews reveal that the co-conspirators initially established contact with victims through various online dating websites, including but not limited to Plenty of Fish ("pof.com"), Ourtime.com, and Match.com. The co-conspirators often fraudulently represented themselves to be United States service members stationed in Syria. On at least one occasion, the co-conspirators emailed the victim a copy of a fictitious military Common Access Card (hereafter "CAC") as proof of military status. Victims reported communicating with the co-conspirators via both email and phone.

28. I have included summaries of five of the more than 30 identified victims. As explained below in the VICTIM 1 section, federal law enforcement agents and I have linked each of the victims with SARPONG and his co-conspirators by numerous means, including but not limited to an examination of email content obtained by search warrants, subscriber information for phones and email accounts, IP addresses, bank and other financial records.

VICTIM 1

29. On or about October 25, 2017, VICTIM 1 began corresponding with an individual purporting to be a United States soldier stationed in Syria having the initials AST[4] (hereafter, "AST") on the dating website pof.com. VICTIM 1 initially communicated with AST via the pof.com platform, and later via AST's email account referred to herein as "SCAM EMAIL 1," as well as by telephone.

30. Per subscriber information, SCAM EMAIL 1 was created on or about October 25, 2017, by an individual purporting to be AST from an IP address hosted by an internet service provider in Ghana. A review of IP logs for SCAM EMAIL 1 reveal it was accessed from IP addresses hosted by internet service providers in Ghana and the United States. A comparison of IP logs for SCAM EMAIL 1 and CC1 EMAIL 2 reveal common login dates, times, and IP addresses for both email accounts, indicative of the same user or group of users. For example, below is a sampling of the logins to CC1 EMAIL 2 and

[4] Throughout this Affidavit, I have used initials to protect the names of persons whose identities have been stolen and used by the co-conspirators in perpetrating this fraud.

SCAM EMAIL 1, showing logins to both email accounts from the same IP addresses within just seconds of each other on multiple days:

CC1 EMAIL 2	SCAM EMAIL 1
1/30/19 06:58:40 UTC 154.160.7.134	1/30/19 06:58:38 UTC 154.160.7.134
1/31/19 17:40:10 UTC 69.65.31.101	1/31/19 17:40:04 UTC 69.65.31.101
2/01/19 21:44:46 UTC 154.160.3.61	2/01/19 21:44:44 UTC 154.160.3.61
2/02/19 01:46:01 UTC 154.160.3.61	2/02/19 01:45:59 UTC 154.160.3.61
2/03/19 17:18:30 UTC 154.160.5.179	2/03/19 17:18:28 UTC 154.160.5.179

31. Based upon subscriber information, IP records, and the use of CC1's nickname and phone number I believe that CC1 was the user of AST's SCAM EMAIL 1, which was used to communicate with VICTIM 1.

32. AST told VICTIM 1 that he was working with a diplomat named EARLE LITZENBERGER (hereafter "LITZENBERGER"), an individual purportedly assisting AST in getting gold to the United States. AST provided VICTIM 1 with LITZENBERGER's email address, SCAM EMAIL 2. Per VICTIM 1, most of the requests for money and wiring instructions supposedly came from LITZENBERGER.

33. Per subscriber information, SCAM EMAIL 2 was created on or about July 18, 2017, by an individual purporting to be EARLE LITZENBERGER. SCAM EMAIL 2 was last accessed on June 15, 2018 from the same internet provider in Ghana used to access both the CC1 EMAIL 2 and SCAM EMAIL 1 accounts. Additionally, the comparison of IP logs for SCAM EMAIL 1 and SCAM EMAIL 2 reveal that on June 15, 2018, both accounts were accessed from the same IP address in Ghana. There is probable cause to believe that CC1, and/or his associates, corresponded with VICTIM 1 from

SCAM EMAIL 2 while purporting to be EARL LITZENBERGER, and that LITZENBERGER is a fictitious person.

34. Per email correspondence obtained from VICTIM 1, LITZENBERGER also corresponded with VICTIM 1 from SCAM EMAIL 3. For example, on or about December 3, 2017, VICTIM 1 received an email from SCAM EMAIL 3 directing her to wire $9,400 to pay for the airway bill for the gold shipment, as well as for airfare and hotel accommodations for LITZENBERGER.

35. Per subscriber information, SCAM EMAIL 3 was created on or about November 5, 2017, by an individual purporting to be EARLE LITZENBERGER from an IP address hosted by an internet provider in Ghana. Like both SCAM EMAIL 1 and SCAM EMAIL 2, SCAM EMAIL 3 was also accessed on June 15, 2018 from the same IP address in Ghana. There is probable cause to believe that CC1 and/or his associates corresponded with VICTIM 1 from SCAM EMAIL 3 while purporting to be LITZENBERGER.

36. Per VICTIM 1, LITZENBERGER also communicated with her via telephone number XXX-XXX-5212. Phone records obtained from TextNow, Inc. (hereafter "TextNow"), a Canadian-based telecommunications company, reveal that on or about November 1, 2017, the co-conspirator phone number was registered to ALWIN LYSS,[5] using the email address CC1 EMAIL 2. A review of emails received from Google pursuant to a search warrant of CC1 EMAIL 2

[5] CC1 also used the name ALWIN ROLF LYSS when defrauding other victims, including VICTIM 2 and VICTIM 4.

revealed the receipt of numerous emails from TextNow to CC1 EMAIL 2 notifying CC1 of incoming text and voice mail messages, several of which were from victims identified in this investigation. Therefore, there is probable cause to believe that CC1 used TextNow to correspond with victims via telephone and text message.

37. From approximately December 4, 2017 to January 10, 2018, at the direction of CC1, VICTIM 1 wired approximately $144,650 to various domestic bank accounts. Of that, approximately $135,250 were wired to a Santander Bank account number ending in -2889 (hereafter "Santander Bank account -2889", controlled by SARPONG, as indicated in the following table:

DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
12/6/17	$10,000	Santander	-2889	SARPONG
12/13/17	$20,000	Santander	-2889	SARPONG
12/19/17	$17,400	Santander	-2889	SARPONG
1/3/18	$48,000	Santander	-2889	SARPONG
1/10/18	$39,850	Santander	-2889	SARPONG

38. A review of bank records reveal that SARPONG opened Santander Bank account -2889 on or about February 24, 2017.

VICTIM 2

39. On or about May 18, 2018, an individual purporting to go by a name having the initials KC (hereafter "KC") sent an email to VICTIM 2 from SCAM EMAIL 4 claiming that as a United States service member stationed in Syria, his unit had recovered millions of dollars in gold bars and that he was awarded one of the boxes of gold valued at over $12 million dollars. During

their communications, KC asked for VICTIM 2's assistance in getting the gold to the United States and requested money to pay for the fees and taxes associated with shipping. KC told VICTIM 2 that the funds would be returned to her once the gold was received in the United States. KC also told VICTIM 2 he was working with a diplomat named ALWIN ROLF LYSS (hereafter "LYSS") to help KC get the gold to the United States.

40. LYSS then began communicating with VICTIM 2 from SCAM EMAIL 5 and provided VICTIM 2 with wire instructions from SCAM EMAIL 5. For example, on May 20, 2018, VICTIM 2 received an email from SCAM EMAIL 5 requesting that funds be wired to a bank account held by SARPONG at Santander Bank. VICTIM 2 responded to SCAM EMAIL 5 and asked, "Can you please tell me who this person is?" On May 21, 2018, LYSS responded he was not an American citizen and therefore used his secretary SARPONG's bank account when arranging deliveries for people. VICTIM 2 then asked for SARPONG's phone number. On the same date, LYSS provided VICTIM 2 with SARPONG's phone number, XXX-XXX-5318. On May 27, 2018 at 6:34am, LYSS emailed VICTIM 2 stating he was flying from Syria to New York, then to Maryland the following day. LYSS attached a copy of a fictitious airway bill indicating that two trunks with "family treasure" were being shipped to VICTIM 2, that LYSS was the delivery agent, that the cost of the shipment was $4,850, and that the trunks would be sent from Syria, to New York, and then to

Baltimore/Washington International (BWI) airport.[6] LYSS also told VICTIM 2 that she owed him additional money for the shipment. LYSS also attached a copy of a fictitious United Nations Identity Card, indicating that LYSS was an Israeli citizen and delivery agent for the United Nations. In the body of the email, LYSS stated he attached the identification card so she would recognize him when she picked him up at the airport.

41. From approximately May 22, 2018 to June 12, 2018, at the direction of the co-conspirators, VICTIM 2 wired approximately $93,710 to two domestic bank accounts. Two days later, on June 14, 2018, VICTIM 2 committed suicide. According to VICTIM 2's daughter, on June 13, 2018, VICTIM 2 stated she was going to BWI airport to meet LYSS with the gold. The following day, June 14, 2018, VICTIM 2 was found dead.

42. Of that $93,710, VICTIM 2 wired $74,810 to a Santander Bank account number ending in -1851 (hereafter "Santander Bank account -1851"), controlled by SARPONG, on the dates listed in the following table:

DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
5/22/18	$2,860	Santander	-1851	SARPONG
5/30/18	$5,600	Santander	-1851	SARPONG
6/1/18	$28,400	Santander	-1851	SARPONG
6/11/18	$15,150	Santander	-1851	SARPONG
6/12/18	$22,800	Santander	-1851	SARPONG

[6] Approximately 15 minutes prior to sending the fictitious airway bill to VICTIM 2 from SCAM EMAIL 5, the fictitious airway bill was sent from SCAM EMAIL 6 to CC1 EMAIL 2.

43. A review of bank records reveal that SARPONG opened Santander Bank account -1851 on or about December 4, 2017, in the name RUBBIN SARPONG AUTOSALES. SARPONG had sole signatory authority on the account and stated that the business was a used car dealership. Per information obtained from the New Jersey Division of Motor Vehicles, SARPONG was not a licensed used car dealer in the state of New Jersey during the period from 2016 through 2018.

VICTIM 5

44. In approximately February of 2018, VICTIM 5 began corresponding with an individual purporting to have a name corresponding to the initials CC (hereafter "CC") on an internet-dating website.

45. CC told VICTIM 5 that she lived in Jacksonville, Florida with her father. In or around April 2018, CC told VICTIM 5 that her father passed away and she was due a large inheritance, mostly in gold, from her father's estate. CC further told VICTIM 5 that an attorney named MUMUNI MUHAMMAD (hereafter "MUHAMMAD") would help get the inheritance to the United States, but that she needed funds in advance to cover the court costs, airway bills, document fees, export fees, and taxes. MUHAMMED communicated with VICTIM 5 from SCAM EMAIL 9.

46. The review of emails received from Google pursuant to a search warrant of SCAM EMAIL 9 reveal that MUHAMMAD introduced himself as an attorney in Ghana and provided VICTIM 5 with two cell phone numbers which are known phone numbers used by CC1, and asked for money to be wired. In response, on April 12, 2018, VICTIM 5 sent an email to SCAM EMAIL 9, in

which VICTIM 5 forwarded an email he received from MoneyGram with the subject line, "There was a problem with your transaction." In the body of the email, VICTIM 5 told MUHAMMAD that the money transfer VICTIM 5 had attempted to send to CC2 was declined. MUHAMMAD then instructed VICTIM 5 to wire the money to SARPONG, whom MUHAMMAD referred to as "one of my boys in New Jersey..." and provided SARPONG's bank account information. When VICTIM 5 asked why MUHAMMAD's son had a different last name, MUHAMMAD responded, "I didn't say in the email he is my son but I said one of my boys not even my relative because he is one of old workers that's why I am using his account to receive the funds."

47. MUHAMMAD also referred VICTIM 5 to a purported diplomat named EDWARD BOATENG (hereafter "E. BOATENG"), at email address SCAM EMAIL 10 and the same telephone number used to defraud VICTIM 4, to arrange for transfer of funds from VICTIM 5. E. BOATENG communicated with VICTIM 5 from SCAM EMAIL 10 and from that same telephone number.

48. From approximately April 25, 2018 to June 8, 2018, at the direction of the co-conspirators, VICTIM 5 wired approximately $301,490 to four domestic bank accounts. Of that, approximately $95,390 was wired to a Santander Bank account -2889, controlled by SARPONG.

49. The wire transfers from VICTIM 5 to SARPONG are listed in the following table:

DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
5/7/18	$18,300	Santander	-2889	SARPONG
5/8/18	$14,890	Santander	-2889	SARPONG
5/15/18	$18,900	Santander	-2889	SARPONG
5/31/18	$25,500	Santander	-2889	SARPONG
6/5/18	$17,800	Santander	-2889	SARPONG

50. A review of bank records reveal that SARPONG opened Santander Bank account -2889 on or about February 24, 2017.

VICTIM 8

51. In approximately November of 2016, VICTIM 8 began corresponding with an individual purporting to have the initials KB (hereafter "KB") on the internet dating website pof.com. VICTIM 8 communicated with KB via the pof.com email and Google Hangouts.

52. KB told VICTIM 8 he was an American service member stationed in Syria, and that he needed assistance in getting approximately $10 million dollars in gold bars and cash out of Syria. KB told VICTIM 8 the money was found in an abandoned house and gifted to him, but that he needed financial assistance to pay for transfer fees, documentation, and airfare for a diplomat named WILLIAM PALMER who was assisting him. KB provided VICTIM 8 with PALMER's email address, SCAM EMAIL 8.

53. From approximately November 18, 2016 to February 10, 2017, at the direction of the co-conspirators, VICTIM 8 wired approximately $198,960 to domestic bank accounts. Of that, VICTIM 8 wired approximately $97,760 to bank accounts controlled by SARPONG, including SARPONG'S M&T Bank

account number ending in -7517 (hereafter "M&T Bank account -7517") and SARPONG'S Fulton Bank of NJ account -5749. The wire transfers from VICTIM 8 to SARPONG are listed in the table below:

DATE OF WIRE	AMOUNT OF WIRE	RECIPIENT BANK	RECIPIENT ACCOUNT NUMBER LAST 4 DIGITS	RECIPIENT NAME
11/18/16	$2,800	M&T Bank	-7517	SARPONG
11/23/16	$7,800	M&T Bank	-7517	SARPONG
11/28/16	$5,460	M&T Bank	-7517	SARPONG
12/02/16	$13,500	M&T Bank	-7517	SARPONG
12/03/16	$7,900	M&T Bank	-7517	SARPONG
12/09/16	$46,800	M&T Bank	-7517	SARPONG
12/27/16	$10,000	Fulton Bank of NJ	-5749	SARPONG
01/09/17	$1,500	Fulton Bank of NJ	-5749	SARPONG
01/23/17	$2,000	Fulton Bank of NJ	-5749	SARPONG

54. A review of bank records reveal that SARPONG opened the M&T Bank account -7517 on or about July 5, 2016 and the Fulton Bank of NJ account -5749 on or about September 2, 2016.

55. Investigation revealed that VICTIM 8 was also directed by co-conspirators to make two wire transfers, totaling $36,800, to a bank account at Sun Trust Bank account number ending in -2153 (hereafter "Sun Trust Bank account -2153"), held by a recipient business believed to be owned by another co-conspirator. VICTIM 8 sent the wires to the Sun Trust Bank account -2153 on the following dates and in the following amounts: (a) on December 1, 2016 – $30,000; and (b) on January 5, 2017 – $6,800.

56. The co-conspirators also directed VICTIM 8 to send $2,000 to CC3 via MoneyGram. Per a review of MoneyGram records, VICTIM 8 sent CC3 $2,000 on June 12, 2017.

VICTIM 9

57. VICTIM 9 stated that in or about January 2016, she began corresponding with an individual who claimed to be a petty officer in the United States Navy, stationed in Canada and identified himself by a name having the initials JO (hereafter "JO"). As directed by JO, in or about January 2016, VICTIM 9 attempted to send $3,000 to SARPONG via PayPal, but the transaction did not go through. VICTIM 9 stated she was then instructed to wire the money to one of SARPONG's bank accounts, which she did. Although she did not recall all of the specifics, VICTIM 9 estimated that she ultimately lost approximately $50,000 to this fraudulent scam.

58. A review of email search warrant records obtained from Google for SARPONG EMAIL 1 reveal that SARPONG knowingly participated in the fraudulent scheme from as early as January 31, 2016. For example, on or about January 31, 2016, VICTIM 9 sent an email to SARPONG EMAIL 1, confirming that VICTIM 9 had attempted to make a requested payment via PayPal.[7] Specifically, VICTIM 9 forwarded an email from PayPal to SARPONG with the subject line "You sent a payment," which stated that VICTIM 9 had

[7] A review of search warrant records also revealed that on January 29, 2016, two days before corresponding with VICTIM 9, SARPONG received an email from PayPal with the subject line "Confirm your bank account with PayPal," which stated in the body of the email "Now that you've linked your bank account, please confirm this account..."

sent $2,999 to SARPONG for "[JO]'s plane tickets." In the body of the email to SARPONG, VICTIM 9 stated, "Here you go! Let's get him home!" On the same date, SARPONG responded via email, stating, "Am trying my best for him to get home to u. But the money u sent to me on my PayPal account is still pending so u have to get hold [sic] at PayPal for them to release the money to me. Thanks."

59. When SARPONG was unable to retrieve the funds through PayPal, SARPONG asked VICTIM 9 to send the money via Western Union. VICTIM 9 responded she did not have the time or the extra money to send the payment via Western Union and asked SARPONG, "Can you just get him into a safe country for now and we shall see if he can get out from there." SARPONG responded via email, "Okay can u put it in my bank account. That's free. Or transfer it into my bank account." At approximately 8:37pm on January 31, 2016, SARPONG sent an email from SARPONG EMAIL 1 and provided VICTIM 9 with SARPONG's TD Bank account ending in -9153 (hereafter TD Bank account -9153), opened on October 14, 2015 and held solely by SARPONG.

SARPONG'S STATEMENTS ON SOCIAL MEDIA

60. During the investigation, federal law enforcement agents located a Facebook account ("SARPONG FACEBOOK") and two Instagram accounts used by SARPONG ("SARPONG INSTAGRAM 1" and "SARPONG INSTAGRAM 2").

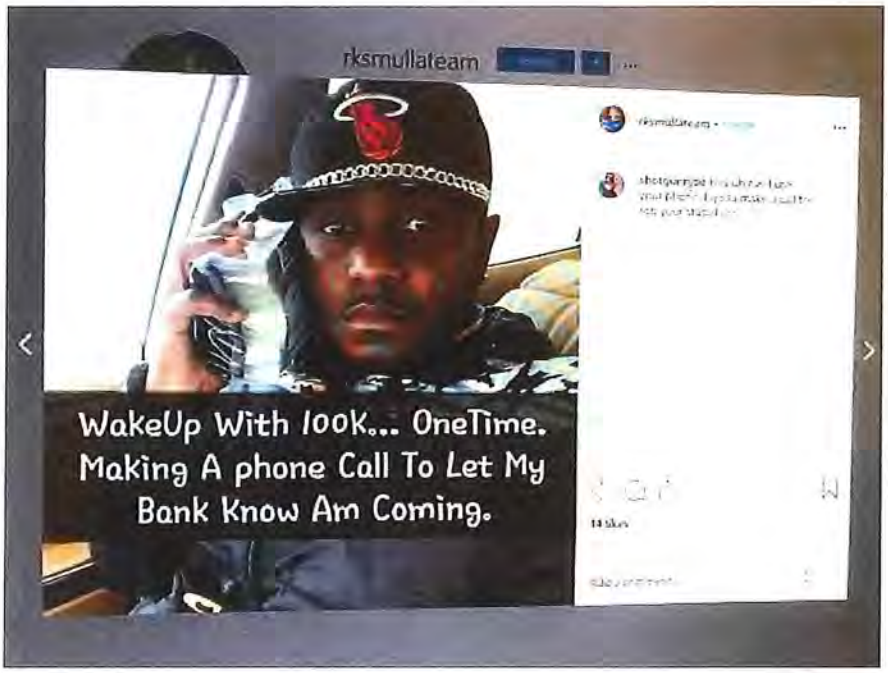
61. A review of SARPONG's social media accounts reveal that SARPONG uses social media to communicate with CC1 and other co-

conspirators about the conspiracy and its proceeds through comments and photographs.

62. A review of SARPONG's social media accounts revealed the following posts, among others, in which SARPONG posted photographs of himself with cash, cars and/or jewelry, and bragged about his wealth:

1) On February 8, 2017, SARPONG posted two photographs of himself holding a large stack of cash;

2) On March 2, 2017, SARPONG posted a photograph of himself sitting in a car with a large stack of cash held up to his ear like a cell phone, with the caption "WakeUp With 100k... OneTime. Making A phone Call To Let My Bank Know Am Coming;"



4) On May 2, 2017, SARPONG posted a photograph of a hand holding a large stack of $100 dollar bills;

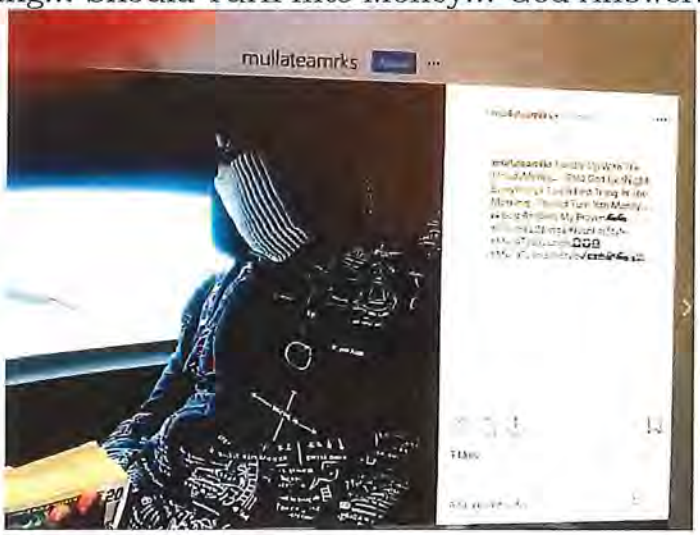
5) On May 29, 2017, SARPONG posted a photograph of himself standing in front of a white Mercedes, with the comment "BloodyMoney;"

6) On April 10, 2018, SARPONG posted a photograph of himself holding a large stack of cash, with the comment "Too Much Blessed...Oluwa Is

Involved...Burger Money...10K OneTime...Overseas Negga Getting This Bricks Off The Rip."

7) On October 8, 2018, SARPONG posted a photograph of various pieces of jewelry and a computer, with the comment "30K Worth Of A Rolex Watch...10K Worth Of A Gold Chain...1K Worth Of A Ring...I Was Blessed By A Dubai Millionaire... Real Recognize Real."[8]

8) On December 6, 2018, SARPONG posted a photograph of himself in a car holding a large stack of money, with the comment "Bundle Up With The BloodyMoney... I Told God LastNight... Everything I Touch First Thing In the Morning... Should Turn Into Money... God Answers My Prayers;"



9) On December 12, 2018, SARPONG posted a photograph of himself with an unknown black male, with the comment "BigBusiness Done...Now We Waiting For The Checks To Clear;"

10) On February 15, 2019, SARPONG posted a photograph of steak and potatoes, with the comment "All Thanks To Pengo...TMF EO... Gang and Play...CBF CEO And Gang...We Really Going To War Together...As Long As Am Alive And Living This Country... TMF + CBF = MullaTeam;" and

11) On March 9, 2019, SARPONG posted a photograph of himself in a car, with the comment "I Stayed Down Till The Money Came...God Answered My Prayers... NiceOut #OverSeasNegga #LivingHighLIfeStyle#CBF#TMF#MullaTeamJungle."

---

[8] A review of CC1 INSTAGRAM 1 revealed that CC1 traveled to Dubai on March 29, 2018, posting a photograph of himself and the comment "Having fun at Man made Island Dubai," to which SARPONG then posted the comment "TMF...CEO LifeStyle."