

COPY

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

VALENTINE IRO, aka "Iro Enterprises," aka  
 "Valentine Obinna Iro," aka "Obinna Iro,"  
 CHUKWUDI CHRISTOGUNUS IGBOKWE, aka  
 "Chris Kudon," aka "Atete," aka "Christogunus C.  
 Igbokwe," aka "Still Kudon,"  
 JERRY ELO IKOGHO, aka "J Man,"  
 IZUCHUKWU KINGSLEY UMEJESI, aka "Armenian  
 Man," aka "Kingsley LA," aka "Izukung Aka Aku,"  
 ADEGOKE MOSES OGUNGBE, aka "P & P Motors,"  
 aka "Pp,"  
 ALBERT LEWIS CATHEY, aka "Alb," aka "Abert  
 Jag," aka "Al,"  
 TITYAYE MARINA MANSBANGURA, aka "Tityaye  
 Igbokwe," aka "Marina Mansour," aka "Marina  
 Mansaray" aka "Marina Tityaye Mans Bangura,"  
 CHUKWUDI COLLINS AJAEZE, aka "Thank You  
 Jesus,"  
 EKENE AUGUSTINE EKECHUKWU, aka "Ogedi  
 Power," aka "Power,"  
 COLLINS NNAEMEKA OJIMBA, aka "Collins Emeka  
 Ojimba," aka "Ojimba Collins," aka  
 "Charly.africa,"  
 CHUKS EROHA, aka "Nassa," aka "Prince Chuddy,"  
 aka "Chuks Nassa Iro,"  
 SAMUEL NNAMDI ONWUASOANYA, aka "Sammy  
 Lee Nnamdi," aka "Onwuasoanya Samuel  
 Nnamdi," aka "Enugu Ogo,"  
 MACWILLIAM CHINONSO CHUKWUOCHA, aka  
 "Chiboy,"  
 EMMANUEL ONYEKA UZOKA, aka "Emmanuel  
 Mansion," aka "Mansion," aka "Son of God," aka  
 "Ezirim Uzoma,"  
 JOSHUA ANIEFIOK AWAK, aka "Joe Awk," aka  
 "Kwee Tin Law,"  
 GEORGE UGOCHUKWU EGWUMBA, aka "George  
 Ugo," aka "Ugo Aunty Scholar,"  
 CHIJOKE CHUKWUMA ISAMADE, aka "Mr CJ,"  
 aka "CJ,"  
 FIEDEL LEON ODIMARA, aka "Fidel Odimara," aka  
 "Ndaa," aka "Dee Dutchman,"

FILED  
 CLERK, U.S. DISTRICT COURT  
 MAY 31 2019  
 CENTRAL DISTRICT OF CALIFORNIA  
 BY DEPUTY

Case No.

19MJ 02316

BY: [Signature]  
 2019 MAY 31 AM 10:21  
 -FEDERAL U.S. DISTRICT COURT  
 CENTRAL DISTRICT OF CALIFORNIA  
 LOS ANGELES

LODGED

ASA

KENNEDY CHIBUEZE UGWU, aka "Kennedy David,"  
IFEANYICHUKWU OLUWADAMILARE  
AGWUEGBO, aka "BO\$\$ IFFY,"  
VICTOR IFEANYI CHUKWU, aka "Ifeannyi Soccer,"  
aka "Vic Chux,"  
CHIDI EMMANUEL MEGWA, aka "Cantr," aka  
"Canta Jr.,"  
PRINCEWILL ARINZE DURU, aka "Arnzi Prince  
will," aka "Arinze,"  
MUNACHISO KYRIAN UKACHUKWU, aka "Muna,"  
NWANNEBUIKE OSMUND, aka "Osmund  
Nwannebuike," aka "Olivite," aka "Nikky Bro,"  
OBI ONYEDIKA MADEKWE, aka "Odu Invest," aka  
"Obi Soccer,"

Defendants.

### CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning no later than September 1, 2014 and continuing through at least May 2, 2018, in the county of Los Angeles, in the Central District of California, the defendants violated:

*Code Section*

18 U.S.C. § 1956(h)  
18 U.S.C. § 1349

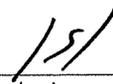
*Offense Description*

Conspiracy to Engage in Money Laundering  
Conspiracy to Commit Wire Fraud and  
Bank Fraud

This criminal complaint is based on these facts:

*Please see attached affidavit.*

Continued on the attached sheet.

  
\_\_\_\_\_  
*Complainant's signature*

\_\_\_\_\_  
Kimberly C. Anderson, Special Agent, FBI  
*Printed name and title*

Sworn to before me and signed in my presence.

Date:

5/31/19

**JEAN P. ROSENBLUTH**

\_\_\_\_\_  
*Judge's signature*

City and state: Los Angeles, California

\_\_\_\_\_  
Hon. Jean P. Rosenbluth, U.S. Magistrate Judge  
*Printed name and title*

## Table of Contents

I.	INTRODUCTION .....	1
II.	PURPOSE OF AFFIDAVIT.....	1
III.	STATEMENT OF PROBABLE CAUSE.....	4
	A. Operation of the Conspiracy .....	4
	B. Search Warrants at IRO’s Apartment .....	12
	C. Interviews of IRO, EROHA, and IGBOKWE.....	14
	D. Forensic Extraction of Phones Seized at IRO’s Apartment.....	16
	E. Identification of Defendants .....	18
	1. IKOGHO.....	18
	2. UMEJESI .....	19
	3. OGUNGBE.....	20
	4. CATHEY .....	22
	5. MANSBANGURA .....	23
	6. AJAEZE.....	24
	7. EKECHUKWU.....	25
	8. OJIMBA.....	26
	9. ONWUASOANYA.....	27
	10. CHUKWUOCHA .....	28
	11. UZOKA.....	29
	12. AWAK .....	30
	13. EGWUMBA .....	31
	14. ISAMADE .....	32
	15. ODIMARA .....	33
	16. UGWU .....	34
	17. AGWUEGBO .....	35
	18. CHUKWU.....	36

19.	MEGWA.....	36
20.	DURU .....	37
21.	UKACHUKWU.....	38
22.	OSMUND .....	39
23.	MADEKWE.....	40
F.	Use of Nigerian Pidgin and Code Words.....	41
G.	Roles of Conspirators in the Conspiracy .....	42
1.	ONWUASOANYA.....	43
2.	CHUKWUOCHA .....	43
3.	UZOKA.....	44
4.	AWAK .....	44
5.	EGWUMBA .....	44
6.	ISAMADE .....	45
7.	ODIMARA .....	46
8.	UGWU .....	47
9.	AGWUEGBO .....	47
10.	CHUKWU.....	48
11.	MEGWA.....	49
12.	UKACHUKWU.....	50
13.	OSMUND .....	50
14.	MADEKWE.....	51
H.	Victims of the Conspiracy .....	52
1.	Victim Company 1—September 2014 BEC Fraud (involving IRO and ONWUASOANYA) .....	52
2.	M.S.—August and September 2015 Fraud Scam (involving IRO and Coconspirator 2).....	54
3.	Victim Company 2—February 2016 BEC Fraud (involving IRO) .....	56
4.	R.B.—March and April 2016 Romance Scam (involving IRO and	

	AWAK).....	58
5.	F.K.—May and July 2016 Romance Scam Victim (involving IGBOKWE and MANSBANGURA) .....	60
6.	J.G.—October 2016 Check Fraud Scheme (involving IGBOKWE and MANSBANGURA) .....	64
7.	Victim Company 3—December 2016 BEC Fraud (involving IGBOKWE and MANSBANGURA) .....	66
8.	B.Z.—March 2017 Elder Fraud Victim (involving IRO, IGBOKWE, and MANSBANGURA) .....	68
9.	Victim Company 4—March 2017 BEC Fraud (involving IGBOKWE, UMEJESI, and OJIMBA) .....	70
10.	Victim Company 5—April and June 2017 Attempted Bank Account Takeover (involving IRO, IGBOKWE, and MANSBANGURA).....	72
11.	A.V.—April and May 2017 Elder Fraud Victim (involving IGBOKWE and MANSBANGURA) .....	74
12.	Victims Je.F. and Jo.F.—April 2017 Escrow Fraud (involving IRO and EKECHUKWU).....	77
13.	Victim Company 6—April 2017 BEC Fraud (involving IRO and CATHEY).....	78
14.	Victim Company 7 and Victim Company 8—April 2017 BEC Fraud (involving IRO) .....	81
15.	D.J.—May 2017 Romance Scam Victim (involving IGBOKWE, MANSBANGURA, and DURU).....	83
16.	L.B.—May 2017 Romance Scam Victim (involving IRO, IGBOKWE, and AWAK).....	88
17.	Victim Company 9—April 2017 BEC Fraud (involving IRO, IGBOKWE, IKOGHO, UMEJESI, OGUNGBE, and UZOKA)...	90
18.	Victim Law Firm May 2017 BEC Fraud (involving IRO, IGBOKWE, and CATHEY) .....	95
19.	D.V.—May 2017 Romance Scam (involving IGBOKWE and MANSBANGURA).....	99
20.	Victim Company 10—May 2017 BEC Fraud (involving IRO, IGBOKWE, CATHEY, and Coconspirator 20).....	100
21.	Victim Company 11—June 2017 BEC Fraud (involving IRO, IKOGHO, UMEJESI, CATHEY, and EROHA) .....	104

22.	B.P.—June & July 2017 Elder Fraud (involving IGBOKWE and MANSBANGURA).....	109
23.	Victim Solicitor Firm—June 2017 BEC Fraud (involving IRO, IGBOKWE, CATHEY, IKOGHO, and CHUKWUOCHA) .....	112
24.	Victim Company 12—June 2017 (involving IRO and CATHEY).....	118
25.	D.A.—June 2017 (involving IGBOKWE and MANSBANGURA).....	120
26.	M.G.—July 2017 through May 2018 Romance Scam Victim (involving IRO, IGBOKWE, AJAEZE, EROHA, and CHUKWUOCHA).....	121
27.	Victim Company 13—August 2017 BEC Fraud (involving IRO, CATHEY, UMEJESI, EKECHUKWU, IGBOKWE, and OGBUNGBE).....	125
28.	Victim Company 14—January and February 2018 BEC Fraud (involving IRO and AJAEZE) .....	129
29.	Victim Company 15—February 2018 BEC Fraud (involving IRO, IKOGHO, and AJAEZE).....	131
30.	Victim Company 16—February 2018 BEC Fraud (involving IRO and AJAEZE).....	133
IV.	CONCLUSION.....	134

## **AFFIDAVIT**

I, Kimberly Anderson, being duly sworn, declare and state as follows:

### **I. INTRODUCTION**

1. I am a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”) and have been so employed since June 2014. I am currently assigned to a Los Angeles Field Division Cybercrimes Squad, which is responsible for investigating computer and high-technology crimes, including computer intrusions and other types of malicious computer activity. Since joining the FBI in 2014, I have received 22 weeks of formal training at the FBI Training Academy in Quantico, Virginia. During the time I have been employed by the FBI, I have participated in investigations relating to computer crime, human trafficking, and organized crime. Prior to being employed by the FBI, I served as a strategic intelligence analyst for five years supporting investigations involving human trafficking, transnational crime, and threats to port security. I have been a case agent for this investigation since its initiation in April 2016.

### **II. PURPOSE OF AFFIDAVIT**

2. This affidavit is made in support of a criminal complaint against, and arrest warrants for, the following individuals, for violations of 18 U.S.C. § 1956(h) (Conspiracy to Engage in Money Laundering) and 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud and Bank Fraud):

a. VALENTINE IRO, also known as (“aka”) “Iro Enterprises,” aka “Valentine Obinna Iro,” aka “Obinna Iro” (“IRO”), a Nigerian citizen with legal permanent resident (“LPR”) status in the United States, believed to be residing in Carson, California, within the Central District of California;

b. CHUKWUDI CHRISTOGUNUS IGBOKWE, aka “Chris Kudon,” aka “Atete,” aka “Christogunus C. Igbokwe,” aka “Still Kudon” (“IGBOKWE”), a Nigerian citizen believed to be residing within the Central District of California;

c. JERRY ELO IKOGHO, aka “J Man” (“IKOGHO”), a naturalized United States citizen and former resident of Nigeria, believed to be residing in Carson, California, within the Central District of California;

d. IZUCHUKWU KINGSLEY UMEJESI, aka “Armenian Man,” aka “Kingsley LA,” aka “Izuing Aka Aku” (“UMEJESI”), a Nigerian citizen believed to be residing in Los Angeles, California, within the Central District of California;

e. ADEGOKE MOSES OGUNGBE, aka “P & P Motors,” aka “Pp” (“OGUNGBE”), a Nigerian citizen with LPR status, believed to be residing in Fontana, California, within the Central District of California;

f. ALBERT LEWIS CATHEY, aka “Alb,” aka “Abert Jag,” aka “Al” (“CATHEY”), a United States citizen currently in federal custody in Illinois;

g. TITYAYE MARINA MANSBANGURA, aka “Tityaye Igbokwe,” aka “Marina Mansour,” aka “Marina Mansaray” aka “Marina Tityaye Mans Bangura” (“MANSBANGURA”), a naturalized United States citizen and former resident of Sierra Leone, believed to be residing in Los Angeles, California, within the Central District of California;

h. CHUKWUDI COLLINS AJAEZE, aka “Thank You Jesus” (“AJAEZE”), a Nigerian citizen believed to be residing in Los Angeles, California, within the Central District of California;

i. EKENE AUGUSTINE EKECHUKWU, aka “Ogedi Power,” aka “Power” (“EKECHUKWU”), a Nigerian citizen believed to be residing in Los Angeles, California, within the Central District of California;

j. COLLINS NNAEMEKA OJIMBA, aka “Collins Emeka Ojimba,” aka “Ojimba Collins,” aka “Charly.africa” (“OJIMBA”), a Nigerian citizen with LPR status, believed to be residing in Los Angeles, California, within the Central District of California;

k. CHUKS EROHA, aka “Nassa,” aka “Prince Chuddy,” aka “Chuks Nassa Iro” (“EROHA”), a naturalized U.S. citizen, believed to be residing in Nigeria;

l. SAMUEL NNAMDI ONWUASOANYA, aka “Sammy Lee Nnamdi,” aka “Onwuasoanya Samuel Nnamdi,” aka “Enugu Ogo” (“ONWUASOANYA”), a Nigerian citizen currently in the United States on an F1 student visa;

m. MACWILLIAM CHINONSO CHUKWUOCHA, aka “Chiboy” (“CHUKWUOCHA”), a Nigerian citizen believed to be residing in Florida;

n. EMMANUEL ONYEKA UZOKA, aka “Emmanuel Mansion,” aka “Mansion,” aka “Son of God,” aka “Ezirim Uzoma” (“UZOKA”), a Nigerian citizen believed to be residing in Marietta, Georgia;

o. JOSHUA ANIEFIOK AWAK, aka “Joe Awk,” aka “Kwee Tin Law” (“AWAK”), a Nigerian citizen believed to be residing in the Central District of California;

p. GEORGE UGOCHUKWU EGWUMBA, aka “George Ugo,” aka “Ugo Aunty Scholar” (“EGWUMBA”), a Nigerian citizen believed to be residing in Cypress, California, within the Central District of California;

q. CHIJIKE CHUKWUMA ISAMADE, aka “Mr CJ,” aka “CJ” (“ISAMADE”), a Nigerian citizen currently in federal custody within the Central District of California;

r. FIEDEL LEON ODIMARA, aka “Fidel Odimara,” aka “Ndaa,” aka “Dee Dutchman” (“ODIMARA”), a Nigerian citizen with LPR status, believed to be residing in Texas;

s. KENNEDY CHIBUEZE UGWU, aka “Kennedy David” (“UGWU”), a Nigerian citizen with LPR status, believed to be residing in Massachusetts;

t. IFEANYICHUKWU OLUWADAMILARE AGWUEGBO, aka “B🌐\$\$ IFF¥” (“AGWUEGBO”), a Nigerian citizen believed to be residing in Texas;

u. VICTOR IFEANYI CHUKWU, aka “Ifeanyi Soccer,” aka “Vic Chux” (“CHUKWU”), a naturalized U.S. citizen believed to be residing in Hawthorne, California, within the Central District of California;

v. CHIDI EMMANUEL MEGWA, aka “Cantr,” aka “Canta Jr.” (“MEGWA”), a Nigerian citizen believed to be residing within the Central District of California;

w. PRINCEWILL ARINZE DURU, aka “Arnzi Prince will,” aka “Arinze” (“DURU”), a Nigerian citizen with LPR status, believed to be residing in California, outside the Central District of California;

x. MUNACHISO KYRIAN UKACHUKWU, aka “Muna” (“UKACHUKWU”), a Nigerian citizen believed to be residing in California, outside the Central District of California;

y. NWANNEBUIKE OSMUND, aka “Osmund Nwannebuike,” aka “Olivite,” aka “Nikky Bro” (“OSMUND”), a Nigerian citizen believed to be residing in the Central District of California; and

z. OBI ONYEDIKA MADEKWE, aka “Odu Invest,” aka “Obi Soccer” (“MADEKWE”), a naturalized U.S. citizen, believed to be residing in Nigeria.

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 warrants, 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.

### **III. STATEMENT OF PROBABLE CAUSE**

#### **A. Operation of the Conspiracy**

4. The FBI has been investigating an extensive conspiracy involving multiple types of fraud and the laundering of the proceeds of that fraud. In general, the subjects and targets of the investigation who are perpetrating the fraud reside abroad—many in Nigeria—while those who assist in receiving and laundering the proceeds of the fraudulent schemes through various bank accounts (most of whom are from Nigeria) live in the United States, including many who

reside in the Los Angeles area. The targets and subjects of the investigation have obtained and laundered millions of dollars fraudulently obtained from victims in the United States and abroad, and attempted to obtain and launder many millions more. The fraudulent schemes include business email compromise (“BEC”) frauds, escrow fraud, romance scams, other online fraud schemes—particularly schemes targeting elderly victims—bank fraud, and check fraud, and laundering funds obtained through those fraudulent schemes.

a. BEC frauds often involve a computer hacker gaining unauthorized access to a business email account, blocking or redirecting communications to and/or from the email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a “spoofed” email account)<sup>1</sup> to communicate with personnel from a victim company and 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(s) 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.

b. Escrow fraud is a variation of a BEC scheme, in which a hacker typically gains unauthorized access to the email account of an escrow company or real estate agent, and then communicates with an unsuspecting person who is seeking to purchase property, directing that person to make a down payment for purchase of property to a fraudulent bank account, rather than the legitimate bank account of an escrow company.

c. Romance scams generally take advantage of persons looking for romantic partners by targeting victims on dating websites and other social media platforms. The

---

<sup>1</sup> One way of spoofing an email address is to create an account at a fraudulent domain, where the domain name is altered to appear identical to a real company domain but where it is in essence misspelled by a letter or character. For example, a BEC fraudster might spoof the email address of “John” at a fictitious ACME, Inc. (john@acmecorpany.com) by creating email accounts at a fraudulent domain (e.g., john@acmecorpany.com (with “rn” replacing the “m” in “company”) or john@acmecorpanies.com). BEC fraudsters sometimes also will create a fraudulent email account at a legitimate email provider (e.g., john\_acmecorpany@yahoo.com).

scammers create profiles using fictitious or fake names, locations, images, and personas. This allows scammers to cultivate relationships with prospective romance scam victims. Victims are often convinced to provide money or gifts to the scammers, or are asked to conduct transactions on their behalves believing they are in a romantic relationship. In addition to themselves being victims of fraud, romance scam victims may thus become unwitting “money mules” for other fraudulent schemes when scammers ask them to transfer money through their bank accounts.

d. Romance scams and other online fraud schemes often target victims who are elderly or otherwise vulnerable to fraudulent schemes, with fraudsters pretending to be U.S. armed services members or employees of oil companies working on offshore rigs (i.e., persons who cannot easily be reached by phone or met in person). These schemes sometimes involve promises by fraudsters that the victims will receive, or receive a share in, a large payment or property of value—for example, a bag of jewels or box of treasure purportedly discovered by a U.S. armed services member in the Middle East—upon the payment of a small fee. After the victim makes a small initial payment—often a few hundred or thousand dollars—the fraudster will employ a series of different personas to trick the victim into making additional payments, such as for fees, taxes, or other invented charges. Some romance scam and elderly online fraud victims, including victims discussed in this affidavit, have lost hundreds of thousands of dollars to these schemes.

5. IRO and IGBOKWE would communicate with fraudsters, or middle-men for the fraudsters, who sought bank accounts into which they could fraudulently induce victims to deposit funds. ONWUASOANYA, CHUKWUOCHA, UZOKA, AWAK, EGWUMBA, ISAMADE, ODIMARA, UGWU, AGWUEGBO, CHUKWU, UKACHUKWU, and OSMUND were among the numerous coconspirators who asked IRO and/or IGBOKWE for accounts that could be used for fraud and laundering the proceeds of fraud. Additionally, while IKOGHO, UMEJESI, OGUNGBE, EKECHUKWU, and MEGWA were among IRO and/or IGBOKWE’s Los Angeles-based money laundering network, they too sometimes asked IRO and/or IGBOKWE about bank accounts that could receive fraudulently-obtained funds.

6. Based on information obtained through search warrants and examination of seized digital devices, described below, IRO and IGBOKWE were known to middle-men and fraudsters world-wide, and communicated with coconspirators primarily through messaging applications and phone calls. Some knew IRO and/or IGBOKWE from Owerri, Nigeria, since many of the coconspirators were from Nigeria, and Owerri specifically. Others were directed to IRO and/or IGBOKWE through coconspirators or middle-men. Still others knew of IRO or IGBOKWE by their reputations for laundering fraudulently-obtained funds. As IRO told the person referred to later as Coconspirator 21 through a messaging application, “I am known all over the world. Even people I never meet before call me and give me better business. . . . I never see am before. [Is] just phone calls.”<sup>23</sup>

7. Either before or after negotiating with the fraudster or middle-man about the fee they would pay—that is, the “cut” of the fraudulent proceeds that IRO and/or IGBOKWE would receive for receiving and laundering the funds—IRO and IGBOKWE would select, find, or assist in opening a bank account to be used. IRO and IGBOKWE were, essentially, a clearinghouse for fraudulent bank accounts. They would collect bank account information (some from Los Angeles and some from coconspirators in other cities or countries), field requests for bank

---

<sup>2</sup> End of sentence/quote punctuation, such as periods or commas, have, at times, been added to defendants’ statements quoted in this affidavit for ease of reading. That punctuation is not intended to alter the meaning of the quoted text.

<sup>3</sup> Evidence indicates that IRO was an active participant in some fraud schemes, as discussed in more detail in Section III.H.1, below. He also appears to have engaged in hacking. As discussed in Section III.G.1, IRO discussed the use of “viruses” and “crypters,” which are software that can encrypt and hide malware. Other evidence indicates that IRO was also actively involved in hacking. For example, in a Yahoo instant messenger conversation with a coconspirator, on May 2, 2013, IRO asked the coconspirator for help in obtaining “links” for Yahoo, Hotmail, Google, and “virus,” and “socks” for himself to use in connection with making a “virus . . . work.”

IRO was also directly involved in romance scams. On November 12, 2013, in a Yahoo instant messaging conversation, IRO advised the coconspirator how to set up a fake online profile using Facebook and said he could use it to earn \$10,000 per month. IRO further appeared to advise the coconspirator that the fake profile should be for a male, 45–48 years old, white, not too attractive, and healthy, and that the fake persona should be married but divorced with one child and an occupation within real estate or with an oil firm. IRO stated that those industries should be chosen because they “take[] you around the world.” At the beginning of that conversation, IRO stated, in “012’ my japan wife game [i.e., gave] me 270k.”

account information from coconspirators all over the world, and then send out bank account information to multiple coconspirators. It was not uncommon for IRO and IGBOKWE to send out the same bank account information to five or more different coconspirators for use in their respective fraudulent schemes. These coconspirators who were seeking bank or money service accounts would therefore benefit from IRO's and IGBOKWE's central roles in the conspiracy, experience in laundering, established laundering network, and infrastructure to create and maintain bank accounts for receiving and laundering funds from fraudulent schemes.

8. For romance scams and schemes targeting the elderly, IRO and IGBOKWE would sometimes use a bank account or money service account that they controlled personally or an account opened in the name of a relative. IRO and IGBOKWE reserved certain accounts for these fraud schemes and actively attempted to keep funds derived from other fraudulent schemes from these accounts, because romance scam and elder fraud victims sometimes do not learn, or at least fully accept, that they are victims of fraudulent schemes until confronted with the evidence by law enforcement or other persons. In fact, even when confronted by law enforcement with evidence that they are victims, it is not uncommon for a romance scam or elder fraud victim to refuse to believe that the person with whom the victim has been corresponding is responsible for defrauding the victim. Even if the victim does learn that he or she has been defrauded, the victim may be unwilling or unlikely to report it to law enforcement due to several factors, including embarrassment.

9. In contrast, victims of BEC frauds and escrow frauds often become aware that they have been victimized soon after sending a wire when (a) the legitimate party that was expecting the transaction does not receive it or, alternatively, (b) the victim asks the legitimate company for confirmation of the wire transfer (which did not in fact go to the legitimate company). Thus, a bank account receiving romance scam or elder fraud funds is less likely to be quickly closed by a bank based on fraudulent activity, than is a bank account receiving proceeds of BEC fraud, escrow fraud, or other fraudulent schemes targeting businesses and banks.

10. IRO and IGBOKWE would direct romance scam and elder fraud payments into accounts in the name of IGBOKWE, Coconspirator 12 (a relative of IGBOKWE), and MANSBANGURA, who was sometimes referred to as IGBOKWE’s “American wife.”<sup>4</sup> (MANSBANGURA, likewise, controlled and used the bank and money accounts in the names of several persons, including some of her relatives.) Similarly, IRO reserved bank accounts opened in the name of Coconspirator 26 for receipt of funds from romance scams and other online fraud schemes, which accounts listed IRO’s apartment as the address on file.<sup>5</sup>

11. For BECs, escrow fraud, and other business fraud schemes, IRO and IGBOKWE would attempt to locate an appropriate bank account—often a business bank account—into which fraudulent funds could be deposited. If they themselves did not have access to a bank account that could be used for the fraud and/or laundering, IRO and IGBOKWE would ask coconspirators, including IKOGHO and UMEJESI, for a bank account.<sup>6</sup>

12. If a bank account with a specific name was required (rather than what the conspirators referred to as an “open bene” or “open beneficiary” account, where a different account name could be substituted to trick the sender of the funds), IRO and IGBOKWE would at times coordinate with money mules, or individuals who directed money mules, to open accounts that could receive fraudulently-obtained funds. The coconspirators would attempt to make the business name mirror the name of the company with which a victim company was

---

<sup>4</sup> Prior to arriving in the United States in January 2017, it appears that IGBOKWE married another woman—described later as Coconspirator 18—in Nigeria.

<sup>5</sup> In one messaging conversation, when providing the account information to a coconspirator for a payment by a romance scam victim (referred to in their conversation as a “client”), IRO threatened: “[L]et me tell you in black and white and I need you to tell them this [¶] If they pay this and is not client. I will not send it back. We will withdraw it and eat it. . . . If it’s not a client. WOMAN. they will not see the money.” In other words, IRO threatened the coconspirator that he would not provide any of the fraudulently-obtained funds to that coconspirator if the funds turned out to be from a BEC fraud rather than a romance scam.

<sup>6</sup> IRO and IGBOKWE were typically careful not to do U.S.-to-U.S. wire transfers in BEC schemes or other business fraud schemes for fear of law enforcement scrutiny and they warned other coconspirators that they would not do such “local,” *i.e.*, U.S.-to-U.S., wires for fear of detection and scrutiny by law enforcement, and specifically by the FBI.

corresponding about a business transaction. This often included the filing of a fictitious business name statement with the Los Angeles County Registrar/Recorder's Office (hereinafter described as having registered the business name with "L.A. County"), which could be done for a small fee. This step was necessary because banks would often require official documentation indicating the existence of the business before opening the business account. Defendants UMEJESI, CATHEY, MANSBANGURA, AJAEZE, EKECHUKWU, EROHA, OJIMBA, and AWAK were among those who assisted with registering business names with L.A. County and opening bank accounts, including by directing the activities of others or opening accounts in the names of other persons.

13. Once such an account designed to receive BEC or escrow fraud funds was open, IRO, in particular, would provide Los Angeles-based coconspirators with advice about how to "service" the bank account—that is, establishing a regular pattern of activity such that the receipt, and, in particular, the withdrawal, of fraudulent funds would not raise suspicions at the bank. For example, IRO would instruct coconspirators to deposit money into the account and then to start using the debit card connected to the account so that there was spending activity associated with the account.<sup>7</sup> He also discussed with coconspirators that fraudulent funds should be allowed to "sit" for at least two days before they were withdrawn, and how to dress and act if a coconspirator had to go into a bank to meet with a representative regarding the funds—all to avoid raising suspicions at the bank.

14. Once a victim deposited funds into a fraudulent bank account or a money service account, IRO and IGBOKWE would coordinate with other coconspirators to withdraw or move the funds, and then to further launder the funds. This sometimes involved sending the funds to

---

<sup>7</sup> For example, on April 25, 2017, IRO told OJIMBA, "Please I need you to start servicing in. [¶] Is about to happen . . . 1.7m." When OJIMBA told IRO that he opened the bank account with \$100, IRO told him, "You need to put some money inside [¶] Like 500 or 1k [¶] And start using it with card [¶] I will send some money inside tomorrow [¶] So you can build it [¶] You feel me?" OJIMBA responded, "I always feel u my oga [¶] But make we start small small before goin higher oga." IRO replied, "Oga calm down [¶] You no wan make money??" OJIMBA retorted, "I won mAKE money but i dey fear for the millions oga [¶] I beg small small." (As discussed in paragraph 87, "oga" is a term of respect, similar to "boss.")

other bank accounts used or controlled by coconspirators—such as IKOGHO, UMEJESI, OGUNGBE, CATHEY, MANSBANGURA, AJAEZE, and OJIMBA—through wires, or withdrawing funds through cashier’s checks, checks, or as cash.

15. IGBOKWE and IRO would take a cut of roughly 40 to 50 percent for BEC transactions in which they assisted with laundering, a portion of which would be paid to the money mule who was opening the account and assuming the risk of receiving fraudulent funds into his or her account. IRO and IGBOKWE would collect less for romance scams (generally between 20 and 30 percent), where there was less risk and often fewer middle men to pay.

16. IRO and IGBOKWE were prolific in receiving and laundering fraudulently-obtained funds, and they were successful. Evidence indicates that IRO and IGBOKWE were, together, involved in schemes resulting in the fraudulent transfer of at least \$6,000,000 and the attempted theft of at least \$40,000,000 more.

17. Once funds were withdrawn as cash, IRO and IGBOKWE frequently used illicit money exchangers who would assist in transferring money overseas, generally without directly transferring those funds internationally. To do this, IRO or IGBOKWE would coordinate withdrawal of funds from a fraudulent bank account or bank account used to launder funds, and then deposit the funds into the U.S. bank account of an illicit money exchanger. The illicit money exchanger would then use a Nigerian banking application to transfer other funds in naira, the currency of Nigeria (₦), from his or her own Nigerian bank account to the Nigerian bank account of the coconspirator that IRO or IGBOKWE specified. In that way, IGBOKWE and IRO were able to ensure payment to Nigerian coconspirators without directly transferring funds overseas.

18. In addition to participating in other aspects of the frauds and laundering, IKOGHO and OGUNGBE served as money exchangers for the conspiracy. MADEKWE also was a money exchanger for the conspiracy. On other occasions, IRO and IGBOKWE would themselves serve as the money exchangers for the conspiracy, receiving fraudulent funds and

then directing others, such as family members in Nigeria, to transfer commensurate amounts to a Nigerian bank account of a coconspirator.

19. IRO and IGBOKWE, together, sent millions of dollars to Nigeria. Preliminary forensic accounting indicates that IRO and IGBOKWE together discussed the transfer of at least \$5,000,000 to the Nigerian bank accounts of coconspirators, family members, and themselves, the majority of which occurred between January and July 2017, preceding execution of search warrants at IRO's apartment by the FBI. Evidence from the digital devices seized in this investigation also indicates that both IRO and IGBOKWE were building large houses (and in IRO's case a compound) in Nigeria using fraudulently-obtained funds. IRO, IGBOKWE, and other members of the conspiracy would also launder funds by the purchase of property—such as cars and trucks—which they would then ship to Nigeria. At other times, they would attempt to disguise the fraudulently-obtained funds as payments for vehicles.

20. As described below, evidence indicates that the conspiracy is ongoing. Even after the FBI executed search warrants at IRO's apartment in July 2017—seizing phones used by IRO, IGBOKWE, and EROHA, among other items—the coconspirators continued to defraud victims through at least 2018, including some of the victims discussed below.

#### **B. Search Warrants at IRO's Apartment**

21. On July 19, 2017, the FBI executed warrants issued by the Honorable John E. McDermott, United States Magistrate Judge, in Case Nos. 2:17-MJ-01791 and 2:17-MJ-01792, respectively for searches of IRO and his apartment, located at 21800 Avalon Boulevard, Apt. 334, Carson, California (“IRO's apartment”), respectively. The warrants were based on several suspicious wires into IRO's two bank accounts—an account at J.P. Morgan Chase & Co. (“Chase”) ending in 9837 opened by IRO in the name V.O.I. Enterprises, in Carson, California (the “VOI Enterprises checking account”) and an account at Wells Fargo ending in 6061, opened by IRO in the name Irva Auto Sales & Equip Broker LLC, in Carson, California (the “Irva Auto Sales account”)—and evidence located in searches of IRO's two email accounts, enterprisesiro@gmail.com and valentino\_q2000@yahoo.com (authorized by warrants issued by

the Honorable Alicia G. Rosenberg, United States Magistrate Judge, in Case Nos. 2:17-MJ-00646 and 2:17-MJ-00647).

22. The following facts regarding execution of the search warrants and interviews of IRO, IGBOKWE, and EROHA are based on my personal involvement, review of FBI reports, interviews of agents involved in the search, and/or review of an audio recording of some of the events:

23. SA Ron Manuel knocked on the door of IRO's apartment at approximately 6:00 a.m. on July 19, 2017 and announced the FBI's presence. It was a loud knock, and SA Manuel loudly said something to the effect of "FBI! Search Warrant!" a few times. After receiving no answer, SA Manuel again knocked and announced the FBI's presence in a similar fashion approximately a minute later. After again not receiving a response, agents entered the apartment using a key.

24. When the agents entered the apartment, the doors of the bedrooms on either side of the apartment were closed. At various points over the next few minutes, a black female and a male later identified as IRO came out of the room on the right, and males later identified as IGBOKWE and EROHA came out of the room on the left. All four were handcuffed and led out of the residence so that the agents could conduct a safety sweep of the apartment.

25. At the time the front door team was knocking on IRO's apartment door, other FBI agents and task force officers ("TFOs") were stationed outside the apartment in view of the apartment's balcony to conduct perimeter surveillance. Shortly after the first knock, TFO John Choo saw a black male in a dark shirt, later identified as IGBOKWE, throw two phones from a large sliding door onto the curb of the driveway of the apartment. He then saw a black man in a white shirt, later identified as EROHA, throw a black cell phone into the neighboring property. The two cell phones thrown by IGBOKWE were a gold iPhone and a silver/white Samsung. TFO Choo retrieved those phones and then he and TFO Rochelle Plue retrieved a black iPhone, thrown by EROHA, from the neighboring property. The large glass window from which the

phones were thrown correlates with the bedroom where IGBOKWE and EROHA were, which had a large sliding door and a façade balcony.<sup>8</sup>

26. Agents found other phones and tablet computers inside the apartment, some of which were later determined to belong to IGBOKWE. In addition, two phones were found under the bed in IRO's bedroom, where they appeared to have been hidden. One was a Samsung Galaxy phone that appeared to have been intentionally broken in half: it had been bent almost in half, the screen was shattered, the battery and circuit boards were damaged and visible, and the phone was nonoperational.

27. Agents prepared to interview the occupants and an audio-recording device was started at approximately 6:35 a.m. The recording indicates that the occupants were warned that the agents were federal agents and that it would be a crime to lie to them. It also indicates that the occupants were questioned about throwing phones off of the balcony, and that IGBOKWE and EROHA admitted throwing phones. The recording also indicates that IRO was asked if he would be voluntarily interviewed and that he responded: "That sounds so good." The occupants also began speaking in a foreign language at one point, and were again warned not to speak in another language. During that warning, they were told to sit still. The agents then began escorting IRO outside. After IRO was escorted outside by the agents, IGBOKWE took his wallet and left to purportedly get some money.

### **C. Interviews of IRO, EROHA, and IGBOKWE**

28. As reflected on the audio recording, SA John Palmieri and I asked IRO where he wanted to be interviewed, suggesting a place in the public courtyard of the apartment building. Once we found a seat, IRO was informed that he was not under arrest and that any statements he

---

<sup>8</sup> Once the residence was cleared, all four occupants were escorted back in and their handcuffs were removed. They were told that they were free to leave but that if they were going to stay they needed to sit quietly. The agents then found identifying documents for each of the individuals. After a few minutes, the black males began to converse in another language. An agent told them that they needed to speak in English or they needed to leave while agents conducted the search.

made were voluntary, but that he could be criminally prosecuted for any false statements. During the course of the interview, which was recorded, IRO admitted using and controlling the two email accounts—enterprisesiro@gmail.com and valentino\_q2000@yahoo.com—and the VOI Enterprises accounts at Chase and the Irva Auto Sales account at Wells Fargo.<sup>9</sup> IRO claimed to buy and sell cars, trucks, and equipment.

29. Of note, IRO stated that he broke his Samsung phone in half in the early morning hours of the previous day—July 18, 2017—following a fight with his wife about him speaking to another woman on a video-call. IRO was given an opportunity to correct that statement but repeatedly stated that the phone was broken the prior day and that its breaking was unconnected to the FBI’s execution of search warrants. As discussed below (see paragraph 34), evidence indicates that statement was false.

30. While IRO was being interviewed, SA Manuel and TFO Plue separately interviewed EROHA on the balcony of the apartment. During the interview, EROHA contradicted his previous admission that he had thrown a phone and said that he had not thrown any phone. He also said that he saw IGBOKWE throw phones out of the balcony. He also stated that IGBOKWE had been staying at the apartment since January 2017, although IGBOKWE would occasionally visit his “wife” at her apartment.

31. After IGBOKWE returned to the apartment, he was met in the hallway by agents, who were still conducting the search. SA Jill Mansfield and TFO Choo interviewed him in the hallway. During the interview, IGBOKWE stated that he arrived in the country in January 2017 and that he helped his “wife,” Tityaye Igbokwe (i.e., MANSBANGURA), whom he said he had married upon arriving to the country, with her business buying and selling cars. When

---

<sup>9</sup> Separate from this investigation, IRO was interviewed on October 26 and November 23, 2016 by FBI agents from Long Beach related to a wire of \$100,083.45 from a German victim company into the Chase VOI Enterprises checking account, on December 3, 2015. The interviews were conducted based on a request from authorities in Germany. IRO submitted signed statements on both days. Although the interviews were cursory, the signed statement from the October 26, 2016 interview indicates that IRO was the owner and sole user of the Chase VOI Enterprises checking account. Moreover, it verified that his phone number was (424) 287-9250 and that at the time lived at 412 Gina Drive., in Carson, California, as well as other biographical information.

IGBOKWE was asked why cell phones were thrown, IGBOKWE was evasive but ultimately said that he was very nervous and did not know what to do.

**D. Forensic Extraction of Phones Seized at IRO's Apartment**

32. As noted, numerous digital devices were seized from IRO's apartment. Although most were locked and inaccessible, the FBI was ultimately able to forensically extract contents of the devices, including the phone that IRO broke, the silver/white Samsung Galaxy Note 5 and the gold Apple iPhone 7 Plus thrown by IGBOKWE, and the black iPhone 7 Plus thrown by EROHA. I have reviewed data from the phones, which collectively contained more than 350,000 messages and approximately 150,000 images. A number of digital devices were found to contain evidence, including the following:

- a. A gold Samsung phone, Model Number SM-G925F, used by IRO, which used the phone number +14242879250 (hereinafter "IRO's broken phone" or "IRO's Samsung").<sup>10</sup>
- b. A blue Samsung phone used by IRO, which used the phone number +14243680611.
- c. A silver Samsung Galaxy Note 5 N920T, used by IGBOKWE, which used the phone number +12134258827 and WhatsApp phone number +2348163439916.
- d. A gold Apple iPhone 7 Plus used by IGBOKWE, which used the phone number +13235090012.
- e. A silver Apple iPhone 6S Plus used by IGBOKWE, which used the phone number +13106267033 and WhatsApp phone number +2348161656787.
- f. A black Apple iPhone 7 Plus used by EROHA, which used the phone number +13104069386.

---

<sup>10</sup> Phone numbers described in this affidavit have, at times, been modified to list them in a standardized format that includes the country code—e.g., +1 for the United States or +234 for Nigeria—before the number and excludes internal punctuation (such as parentheses and hyphens).

33. In particular, the process to unlock and/or extract the data from IRO's broken phone took many months because of the damage to the phone, and was accomplished by the FBI's Laboratory in Quantico, Virginia, using advanced forensic techniques.

34. Of note, data extracted from IRO's broken phone indicates that it was operational until the time that the FBI knocked on IRO's apartment. Specifically, data indicated that, on July 19, 2017, IRO sent or received more than 60 messages between 5:00 a.m. and 6:00 a.m., and received and made several calls after 5:00 a.m. (the last being a 14-minute call starting at 5:15 a.m.). The last messages were time-stamped as having been received at 6:00:38 AM (UTC-7) and 6:00:39 AM (UTC-7)—that is, 38 seconds and 39 seconds after 6:00 a.m.—which indicates that the phone had been active at the very minute that the FBI first knocked and announced its presence and intention to execute search warrants, contrary to what IRO said. The phone was bent in half, the glass shattered, and not functional at the time that agents located it later that morning under IRO's bed with another phone used by him.<sup>11</sup>

35. Information on the various phones seized indicates IRO's motive for breaking his phone, as well as IGBOKWE's and EROHA's motives for throwing their phones from the apartment. Forensic examination of the devices revealed extensive evidence of the fraudulent schemes and conspiracies, as well as producing evidence indicating that additional individuals were part of the conspiracies.<sup>12</sup>

---

<sup>11</sup> On April 26, 2018, I obtained a warrant issued by the Honorable John E. McDermott, United States Magistrate Judge, in Case No. 2:18-MJ-01007, to search IRO's broken phone for evidence of violations of 18 U.S.C. §§ 1001 (False Statements) and 2232(a) (Destruction or Attempted Destruction of Property to Prevent Seizure).

<sup>12</sup> Based on my training and experience, and experience in this investigation, I know that text messages and other messages can remain on a digital device for a period of years. In addition, when a messaging application account is activated on a new digital device, some messaging applications can download onto the new digital device earlier conversations associated with the messaging application account conducted using other digital devices. Oftentimes, whether such messages remain on a phone can depend on whether the individual using the phone has deleted the message; if the individual has not deleted the message then the message can remain on the phone indefinitely.

In this investigation, phones seized pursuant to the warrants described above contained some information that was years old. For instance, in a phone used by IRO, there were Facebook

**E. Identification of Defendants**

36. Based on review of the digital devices, each of the other defendants was identified as having communicated with IRO, IGBOKWE, and/or EROHA. This section reviews the phone number(s) they used and some of the evidence of their identities.

1. IKOGHO

37. JERRY ELO IKOGHO primarily communicated with IRO using the phone number “+13233080042,” which was listed in IRO’s phone as “J Man.” Subscriber records from numerous companies indicate that IKOGHO used the phone number +13233080042.

a. For example, T-Mobile records received in September 2018 show that the phone number +13233080042 was subscribed to IKOGHO with an address of 17630 Crabapple Way, Carson, CA 90746, starting on July 11, 2013. This address matches IKOGHO’s DMV record. SA Miguel Luna and I also conducted surveillance at this location on October 18, 2018, and saw IKOGHO leaving the house and driving away in a BMW, and then later again arriving at and reentering the house.

b. The email address ikoghojerry@gmail.com was subscribed to “jerry ikogho” using the phone number +13233080042 and the recovery email account ikoghojerry@yahoo.com. The Google email account, which was created on March 15, 2013, was accessed in 2018 by several Charter Communications IP addresses assigned to IKOGHO, who listed that phone number and the address of 17630 Crabapple Way, Carson, CA 90746-7464 in the Charter Communications records. The Yahoo email account was created on July 23, 2009, registered to “Mr Jerry Ikogho,” and listed ikoghojerry@gmail.com as its alternate email account.

---

Messenger messages from as early as March 2014 — more than three years prior to when the FBI executed search warrants at IRO’s apartment in July 2017 — and WhatsApp messages from July 2015. And, one phone used by IGBOKWE contained messages associated with the Facebook Messenger application from as early as April 2012, while another had messages from as early as 2010. I have observed that the subjects of this investigation have used WhatsApp, Facebook Messenger, Blackberry Messenger (“BBM”), SMS Messages, and text messages, among other means, to communicate about the fraudulent schemes and conspiracies described herein.

c. Moreover, records from Facebook, Uber, and Lyft, showed that active accounts of IKOGHO were registered using the email account ikoghojerry@gmail.com and the phone number +13233080042.

38. There are, likewise, numerous indications that IKOGHO used +16466516077 at times to converse with IRO. When IRO's conversations with +16466516077 and +13233080042 are read side-by-side, they form essentially one seamless conversation discussing receiving fraudulently-obtained funds and money laundering, indicating that IKOGHO was using both phone numbers. The conversational styles of +16466516077 and +13233080042 are also very similar. Finally, in addition to overlap between discussion of money laundering, there was some other overlap between the conversations: on July 2, 2017, +13233080042 sent IRO a 4th of July barbeque invitation ("You are cordially invited to my humble home for barbecue 4th of July, time 3pm till 10pm....Address 17630 crabapple way Carson ca90746"). Then, on July 3, 2017, +16466516077 said to Iro, "I sent u an invite for tomorrow." The invitation from IKOGHO is the only 4th of July invitation I was able to identify on IRO's phone. Additionally, on July 4, 2017, IRO and EROHA discussed how IRO was at a "thing" at "Jerry house."

## 2. UMEJESI

39. Evidence indicates that IZUCHUKWU KINGSLEY UMEJESI used the phone number +13232099682, which was listed in IRO's Samsung as "Armenian Man," in IGBOKWE's iPhone 7 Plus as "Kingsley LA," and in EROHA's phone as "Izukung Aka Aku."

40. First, UMEJESI's messaging conversations with IRO and IGBOKWE themselves contained identifying information.

a. In messages on June 26, 2017, IRO asked "This is izukung ya?," and "Armenian Man" responded, "Yes sir." "Izukung" is a moniker corresponding to parts of UMEJESI's first and middle names that appeared in other account records.

b. In a conversation with IGBOKWE, "Kingsley LA" sent the name "Kingsley umejesi" on February 20, 2017, shortly after the start of their conversation. And, on a

day in 2017, IGBOKWE wished “Kingsley LA” a happy birthday. DMV records indicate that UMEJESI’s birthday was the next day.

41. Financial records show that “Umejesi Kingsley Izuchukwu,” listing an address of 2319 W. Florence Ave., Los Angeles, California, conducted financial transactions on August 16, 2016 and May 18, 2017, and on both instances listed the phone number +13232099682. On one instance the user’s birthdate was entered as the same date on UMEJESI’s driver’s license record. (On another instance, it was listed as a date that would have been a numerical inversion of the month and day of birth.) Financial records similarly indicate that UMEJESI conducted nine transactions using a different service between 2015 and 2018, with several listing his date of birth consistent with the month and day (but a year earlier) listed on his driver’s license record, and one listing his Nigerian passport number.

42. This address and phone number were listed in a February 2, 2018 report that UMEJESI filed with Hawthorne Police Department about a break-in of his Dodge Charger.

43. Following that report, on May 10, 2018 and January 15, 2019, FBI surveillance teams saw UMEJESI and the same Dodge Charger at 2319 W. Florence Ave, Unit 2, Los Angeles, CA 90043, including seeing UMEJESI drive the vehicle.

44. Subscriber records obtained from Uber, Lyft, Oath Holdings, Inc., and Facebook also corroborate UMEJESI’s use of the phone number +13232099682. For instance, Uber records show that the account of “Izuchukwu Umejesi” used that phone number from September 5, 2015 until January 14, 2016, when the account status was changed to “Banned.”

### 3. OGUNGBE

45. Evidence indicates that ADEGOKE MOSES OGUNGBE used two phone numbers to communicate with IRO: +13107565633, which was listed in IRO’s Samsung as “P & P motors,” and +13107738266, which was listed as “Pp.”

46. First, based on the following, I know that OGUNGBE used +13107565633:

a. T-Mobile records show that +13107565633 has been subscribed to OGUNGBE since April 3, 2012. These records, provided in November 2018, indicate that

OGUNGBE's address was 17260 Farwell St., in Fontana, California. In April 2018, FBI TFO Joshua Cogswell conducted surveillance at that address, and saw OGUNGBE leaving the residence with a child. They entered a silver Lexus, which, based on the license plate number, was registered to P/P Motors LLC, at an address in Whittier, California.

b. Records from GoDaddy.com indicate that the username and company "pandpmotorsllc" was created on May 16, 2014, listing OGUNGBE as the owner, the phone number +13107565633, the email address adegoke101@gmail.com, and a different address in Whittier, California.

c. Google records show that the email address adegoke101@gmail.com, created on May 26, 2013, was subscribed to "Moses Adegoke," listed the phone number +13107565633. That email address was also used to create an Instagram account, on February 3, 2014, with the vanity name<sup>13</sup> "pandpmotors" that listed the user's name as "Adegoke Moses Ogungbe."

d. Records from Uber and Facebook also corroborate OGUNGBE's use of the phone number +13107565633.

47. Evidence also indicates that OGUNGBE used +13107738266.

a. First, T-Mobile records show that +13107738266 was subscribed to OGUNGBE from February 6, 2016 to June 12, 2018, listing an address in Orange, California.

b. Second, IRO's conversations with +13107565633 (P & P motors) and +13107738266 (Pp) have numerous parallels, and can be read together as one conversation by a person using two phones.<sup>14</sup> For example, "Pp" discussed with IRO two particular bank accounts located in Houston, Texas, which "P & P motors" provided to IRO and frequently discussed with

---

<sup>13</sup> A "vanity name" on Facebook or Instagram is a custom name that can be created by a user to identify the account, which name can be incorporated into a custom URL. For example, the Instagram page of a person using the Instagram vanity name "John.Doe.7" could be accessed by typing the URL [www.instagram.com/John.Doe.7](http://www.instagram.com/John.Doe.7) into a browser.

<sup>14</sup> On May 10, 2017, after missing a call from IRO on +13107738266, "Pp" explained, "I went out [¶] Na my second phone dey my hand" (roughly meaning, "I went out. It's my second phone in my hand").

him. Additionally, on May 8, 2017, “P & P motors” told IRO that his wife had a baby boy, and on May 15, 2017, “Pp” told IRO that they had just finished the “naming ceremony.”

4. CATHEY

48. Evidence indicates that ALBERT LEWIS CATHEY used at least three phone numbers to communicate with IRO: +13233595052, which was listed as “Alb”; +13104843117, which was listed as “Abert Jag”; and +13102420179, which was listed as “Al.”

49. First, Sprint records indicate that the phone number +13233595052 was subscribed to CATHEY at an address in Inglewood, California. The records indicate that the account of CATHEY was active from October 15, 2012 through June 28, 2017, and that the phone number was active between December 2, 2015 and February 12, 2017, with several periods when the phone number was suspended in between. CATHEY’s DMV record indicates that he lived at the address in Inglewood, California listed in the Sprint records.

50. Apple records show that CATHEY’s iTunes account listed the phone number +13233595052, an email address of ac.lu@aol.com, and the same address in Inglewood. Apple records also show the phone number was also associated with an account subscribed to CATHEY which listed a different physical address and used the email address blueheaven3223@gmail.com, which CATHEY had provided to IRO as his email address.

51. Evidence also indicates that CATHEY used +13104843117:

a. IRO’s messages with both numbers can be read as one conversation, and there are overlapping topics discussed. The conversation between IRO and “Abert Jag” started in September 2016, but primarily was between February 17, 2017 and March 31, 2017. Although IRO and “Alb” talked almost daily, there was a significant gap in their conversation between February 7, 2017 and March 31, 2017—roughly the dates that IRO corresponded with “Abert Jag.” In addition, IRO’s conversations with both numbers discussed overlapping topics, such as an unidentified coconspirator known as “Chike,” paying for a suit to serve as a groomsman in IRO’s wedding, and bank accounts opened in the names of an Indian company

and a Chinese company. Finally, the conversational styles of “Alb” and “Abert Jag” have a number of similarities.

b. Sprint records show that telephone number +13104843117 was active between June 27, 2016 and July 20, 2017, with several periods when the phone number was suspended in between. During the entire time period, a woman, L.S., was listed as the subscriber of the phone, with billing addresses in Lawndale and San Pedro, California. Based on an interview with a person at an apartment, where CATHEY and L.S. lived together between January 2017 and February 2019 in Paramount, California, L.S. was the girlfriend of CATHEY. The person provided the Lawndale address as a forwarding address for L.S. Additionally, on the apartment housing application for L.S., “Albert” was listed as a friend, who used the telephone number +13233595052, which is discussed above.

52. Finally, evidence indicates that CATHEY used +13102420179 (listed as “Al”):

a. IRO’s messages with “Al” spanned May 2016 through August 2016, ending before CATHEY appears to have started using the phone number +13104843117. In addition to similarities in conversational style of “Al” to that of CATHEY, in the conversation there was reference to a Ghanaian oil company (the “Ghanaian Company”), and records from US Bank show that CATHEY opened a business bank account using the name of the Ghanaian Company (i.e., “Albert L Cathey dba [Ghanaian Company]”). CATHEY also filed a fictitious business name statement in this name on April 26, 2016.

b. Separately, records from Comerica Bank showed that CATHEY listed +13102420179 when opening two other bank accounts (both with business names) in 2016.

c. Records from Sprint for +13102420179, show that the number was subscribed to CATHEY, with an address in Inglewood, California from October 15, 2012 through June 28, 2017 with several periods when the phone number was suspended in between.

## 5. MANSBANGURA

53. TITYAYE MARINA MANSBANGURA used numerous phone numbers to communicate with IRO, IGBOKWE, and EROHA. It appears that MANSBANGURA would

use a particular set of phone numbers for a period of several months and then would drop them and pick up an entirely new set of phone numbers. In addition to sometimes including her name in communications with IRO, IGBOKWE, and/or EROHA, MANSBANGURA's communications sometimes also included photographs of herself or her children. The photographs of herself are consistent with MANSBANGURA's DMV photograph.

54. Based on review of the phones, it appears—based on the nature of the conversation, the topics discussed, photographs exchanged, and conversational similarities, among other things—that MANSBANGURA used at least 16 different phone numbers to communicate with IRO, IGBOKWE, and/or EROHA between October 2016 and July 2017, including +13102790880, +13105271235, +13108063646, +13109043858, +13109048073, +13109207285, +13109208666, +13104474893, +14243764052, +14243767261, +14243767260, +14243059393, +13109546109, +14243769179, +14243769219, and +14243768558.

55. In addition to using multiple phone numbers, evidence on the digital devices indicates that MANSBANGURA used a number of different identities as well as names of relatives, including when interacting with banks. This is likely because MANSBANGURA could no longer open her own bank accounts. On March 31, 2017, MANSBANGURA asked IRO about obtaining a fake identification, saying that IGBOKWE had told her that IRO knew of someone who could “help get a new identity,” including possibly a passport and social security number. MANSBANGURA said that she needed the new identity to open a bank account, noting “I can't open account cause all the banks have blocked me.” IRO told her that his contact could provide a new driver's license or social security number. He told her “without ssn. 1500,” but “With ssn. . . . 2000.” IRO stated that it would only take four days for her to obtain the new identification documents.

6. AJAEZE

56. In addition to the evidence described below indicating CHUKWUDI COLLINS AJAEZE's connections to the conspiracy (see Sections III.H.26, III.H.28, III.H.29, and III.H.30),

including photographic and video evidence, evidence indicates that AJAEZE was the person listed in IRO's Samsung as "Thank You Jesus," using the Nigerian phone number +2348185174075.

57. Records from Tango, a cross-platform messaging application, show that the telephone number +2348185174075 was tied to an account registered to "Collins Eze 2," and listed the email address ajaeze@gmail.com. Other records obtained during the investigation also connect AJAEZE to this telephone number.

58. Moreover, Google records received in August 2018 for that email address show the subscriber's name as "Chuckwudi Collins Ajaeze," and those records listed the telephone number +14242270030 and the recovery email account tm.hailey10@yahoo.com. In contrast, Google records received in June 2018, showed the same subscriber name and email address, but listed the telephone number +2348035994415, instead.

a. That U.S. phone number—+14242270030—was listed in account-opening documentation for AJAEZE's U.S. bank accounts, including the Chase account ending in 0038 and the Wells Fargo account ending in 1849 that are discussed in Sections III.H.28 through III.H.30 (relating to Victim Company 14, Victim Company 15, and Victim Company 16). It was also listed in records for Facebook, Uber, and Lyft accounts that appear to be used by AJAEZE, all of which also listed the email address ajaeze@gmail.com.

b. AJAEZE listed IRO's apartment as the address for his bank accounts at Wells Fargo (accounts ending in 3087, 7748, 9123, and 1849); Bank of America (account ending in 5957); and Chase (account ending in 0038).

## 7. EKECHUKWU

59. Evidence indicates that EKENE AUGUSTINE EKECHUKWU used +15623289622 to communicate with IRO and IGBOKWE, which number was listed as "Ogedi Power" in IRO's phone and "Power" in IGBOKWE's.

a. First, when IRO and "Ogedi Power" were discussing a fraudulent wire transfer gone awry in March 2017, their communications reveal that IRO came to the realization

that he had provided the wrong name on bank account information to the fraudster or middleman. IRO asked, “Wait [¶] What’s your name [¶] Ekenne Williams??” Ogedi Power responded, “Ekene Ekechukwu,” and IRO replied, “Ohhh [¶] I gave them ekenne Williams . . . I made a mistake on your name.”

b. In his conversation with IGBOKWE, the first message from “Power” to IGBOKWE stated “Ekene Austine,” which is EKECHUKWU’s first name and a version of his middle name. EKECHUKWU has used the name “Austine” on other occasions, as well. For example, a Facebook account associated with the phone number +15623289622 used the name “Austine Dee,” while an Instagram account used the name “Austine.”

c. Based on records from Uber and Lyft, EKECHUKWU used the phone number +15623289622 and also provided the email address fatherkee@hotmail.com. Moreover, Microsoft subscriber records for fatherkee@hotmail.com showed the subscriber’s name as “Augustine Ekechukwu.”

## 8. OJIMBA

60. Evidence indicates that COLLINS NNAEMEKA OJIMBA communicated with IRO using the phone number +13233177383, which was listed as “Charly.africa” in IRO’s Samsung phone.

a. On April 5 and July 4, 2017, in the context of discussing bank accounts that “Charly.africa” had opened for IRO, “Charly.africa” sent account information to IRO for a bank account in OJIMBA’s name, which “Charly.africa” discussed as being his own account.

b. T-Mobile records indicated that the phone number +13233177383 was subscribed to OJIMBA, and was active since June 4, 2011. The records listed the address of OJIMBA as being in Hawthorne, California, an address that was also listed in other records obtained during the investigation.

c. OJIMBA also used the phone number +13233177383 in connection with opening bank accounts. US Bank records indicate that an account ending in 1837 was opened on March 28, 2017 by OJIMBA, and listed that phone number. Wells Fargo records indicate that,

on March 9, 2017, OJIMBA listed the telephone number +13233177383 on the account opening documents for his business account ending in 7776 doing business as (“dba”) “C and K Business Enerprise” (the account name missing the “t” in “Enterprise” on both the signature card and statements).

9. ONWUASOANYA

61. Evidence indicates that SAMUEL NNAMDI ONWUASOANYA is the person who was using samuelnnamdi@yahoo.com to communicate with IRO by email, and who communicated with IRO by phone using +2348165056552, which was listed in IRO’s phone as “Enugu Ogo.”

a. Google searches, conducted on March 4, 2019, revealed that the website sammylee.com.ng was the website of a Nigerian actor named listing his name as “Onwuasoanya Samuel Nnamdi,” who also went by “Sammy Lee Nnamdi.” The website included biographical information and various photographs of ONWUASOANYA. For example, it indicated that ONWUASOANYA had appeared in more than ten Nigerian films, it listed the month and year of his birthday, and said he could be reached through the email address samuelnnamdi@rocketmail.com.

i. During this investigation, I have observed that persons from Nigeria will sometimes list their names in financial, email account, and social media account records (among other records) with the surname preceding their given names.

b. Yahoo records for samuelnnamdi@rocketmail.com, the email address listed on the website, showed that the account was active as of the last date records were obtained, in March 2019. The subscriber’s name was listed as “Mr Samuel Nnamdi,” located in Nigeria.

c. Records for IRO’s email address, enterprisesiro@gmail.com, obtained through a search warrant referenced above, contained a February 24, 2016 email from samuelnnamdi@rocketmail.com that attached two photographs of wire transfer requests. On February 29, 2016, IRO’s Samsung phone contained a message to a relative of IRO, saying “Pay

in 6” and providing the following account information: “Acc name: Onwuasoanya Samuel N. [ACCOUNT NUMBER REDACTED].” This name is consistent with ONWUASOANYA’s.

d. Contacts for the Facebook account of “Sammy Lee Nnamdi” were listed in IRO’s and EROHA’s phones. Facebook records indicate that this Facebook account used a registered email at an Indian email provider and also had two verified phone numbers, one of which was +2348165056552. This number was also the phone number listed in IRO’s phone as “Enugu Ogo.”

e. LinkedIn records for “Samuel Onwuasoanya” list a birthday in 1987 consistent with the month and year listed on the website, and as well as listing samuelnnamdi@rocketmail.com as its confirmed email address. The profile records included a photograph, which appeared to be the same person pictured on the website for ONWUASOANYA.

#### 10. CHUKWUOCHA

62. Evidence indicates that CHUKWUOCHA is the person who conversed with IGBOKWE using the moniker “Chiboy” (using +14072337717). The person using this phone number also communicated with IRO, and discussed being in Orlando, Florida, but was not identified in IRO’s Samsung by a particular name.

a. On July 7, 2017, in the context of discussing a payment from a romance scam victim (M.G., who is discussed in Section III.H.26), CHUKWUOCHA sent the following information to IGBOKWE, “Name: Macwilliam chinonso chukwuocha [¶] Address : Orlando FL,” and then also sent IGBOKWE his name and Wells Fargo bank account ending in 5736.

b. Records from T-Mobile indicate that the phone number +14072337717 was subscribed to “Amcwilliam Chukwuocha” [sic] from November 25, 2016 through March 20, 2017, from Orlando Florida.

c. IGBOKWE’s iPhone 7 Plus also contained an imo<sup>15</sup> contact for “Macwilliam” listing the phone number +14072337717. That contact also listed the moniker

---

<sup>15</sup> Imo is a messaging application.

“Chiboy.” Records for that imo account indicate that the account was created on December 2, 2016, and used the name “Macwilliam,” the verified email address macwilliam123chukwuocha@gmail.com, and the phone number +14072337717. Google records for that Gmail account showed the subscriber’s name as “macwilliam chukwuocha.”

11. UZOKA

63. Evidence indicates that “Mansion” (using +14703386848) and “Son of God” (using + 16464576954), who communicated with IGBOKWE, were aliases for EMMANUEL ONYEKA UZOKA.

a. On April 9, 2017, in a messaging conversation occurring while IGBOKWE was visiting Atlanta, “Mansion” provided an address of “1405 station club dr 30060.” This matches UZOKA’s address on his Georgia driver’s license: 1405 Station Club Dr. SW, Marietta, Georgia 30060. About 40 minutes after receiving the address, IGBOKWE sent “Mansion” a message saying, “I dey ur house 🏠,”—i.e., roughly, “I’m at your house.”

i. On March 29, 2019, an FBI agent confirmed with an employee at the Ivy Commons Apartment complex that UZOKA resided at 1405 Station Club Dr. SW, Marietta, Georgia 30060. The employee had seen UZOKA in the apartment complex office the day prior.

b. IGBOKWE’s 7 Plus listed two contacts for “Mansion” that had both the +14703386848 phone number used by “Mansion” and the +16464576954 used by “Son of God,” one of which listed a modification date of May 10, 2017, which is when the messaging conversation between “Son of God” and IGBOKWE began.

c. There was also continuity between IGBOKWE’s conversations with “Son of God” and “Mansion.” The “Son of God” conversation ended on June 19, 2017 after discussing a \$52,000 transfer, and then “Mansion” and IGBOKWE picked up the same conversation on June 28, 2017, discussing a transfer of the same amount.

d. T-Mobile records further indicate that +14703386848 was subscribed to UZOKA, with an address of 1405 Station Club Dr Sw, Marietta, GA 30060, from November 15, 2016 through February 18, 2019, when it was suspended for nonpayment.

e. Finally, in the messaging conversation between IGBOKWE and “Mansion,” “Mansion” sent several photos of IGBOKWE and another man. That other man matches the Georgia DMV photograph of UZOKA, and also closely resembles a man pictured in photographs sent by “Son of God” to IGBOKWE. Publicly viewable photos from UZOKA’s Facebook and Instagram pages also confirm that he is the same individual seen in the photos found in IGBOKWE’s phone(s).

12. AWAK

64. Evidence indicates that JOSHUA ANIEFIOK AWAK was the person who used the phone number +2348080265259, which was listed as “Joe Awk” in IRO’s Samsung.

a. On May 13, 2017, “Joe Awk” sent IRO account information for a Nigerian bank account at Guaranty Trust Bank (“GT Bank”): “[ACCOUNT NUMBER REDACTED] Awak Joshua GTB.” On May 14, 2017, told IRO, “I never see your alert,” essentially saying that he did not receive a notification that the funds had been transferred. On June 20, 2017, “Joe Awk” again provided IRO with his GT Bank account information, and then appeared to confirm that he received funds from IRO, saying “I received 4.4. When do I expect the balance ?” “Joe Awk” also discussed receiving alerts for the account when money was transferred, indicating that it was his account.

b. On August 25, 2018, AWAK was interviewed by U.S. Customs and Border Protection (“CBP”) during secondary screening at Los Angeles International Airport (“LAX”), following an inbound flight. AWAK provided CBP a copy of his business card which listed the phone number +2348080265259, and he also wrote down the telephone number on a piece of paper. AWAK stated that he met IRO in college in Lagos, Nigeria and that during his visit to Los Angeles he planned to visit IRO. AWAK provided two of IRO’s phone numbers to CBP, one of which was +14242879250, IRO’s primary phone number.

c. Google records from January 2019, indicate that awak.joshua@gmail.com was registered to “Joshua Awak,” and listed a recovery email address of joshuaawak@icloud.com and phone number of +2348080265259.

d. Yahoo records indicate that joshuaawak@yahoo.com was subscribed to “Joshua Awak” and listed several email addresses and phone numbers, including the phone number +2348080265259. One of those email addresses was ccs03h@gmail.com, which supplied IRO with a fraudulent invoice related to victim R.B. (see Section III.H.4).

e. Finally, following the BEC fraud that victimized an Indian company in September 2018 (discussed below in paragraph 94), I interviewed a Chase investigator, who stated that information in Chase records indicated that AWAK’s telephone number was +17868722885 and his email address was awak.joshua@gmail.com.

### 13. EGWUMBA

65. GEORGE UGOCHUKWU EGWUMBA was listed in IRO’s contacts as “George Ugo” and as using the phone number +17149161760. The same phone number was listed in EROHA’s contacts as “Ugo Aunty Scholar.”

a. Facebook records as of August 29, 2018 indicate that the phone number +17149161760 was verified as being used by the Facebook account of “George Egwumba” along with the email addresses smilinggeorgeconsult@yahoo.com and egwumbag@yahoo.com.

b. Apple records indicate that two Apple IDs were registered to this phone number: egwumbag@yahoo.com and wingaldnigeria.ent@gmail.com. Both were listed as having been used by EGWUMBA, and the email account smilinggeorgeconsult@yahoo.com was listed as being the recovery account for both Apple IDs. Additionally, a Nigerian phone number—08033743079—was also listed in the records as being used by both Apple IDs.

c. Egwumbag@yahoo.com was registered on April 26, 2003, and listed the subscriber’s name as “Mr. George Egwumba,” the verified phone number +2348033743079 (the same Nigerian number listed above), and the alternate email address smilinggeorgeconsult@yahoo.com. That email account, in turn, used the same phone number

and egwumbag@yahoo.com in its subscriber records and listed the subscriber's name as "Mr. George bent."

14. ISAMADE

66. CHIJOKE CHUKWUMA ISAMADE used several telephone numbers to communicate with IRO and IGBOKWE, including the U.S. phone numbers +14155309429 and +17075901571, and the Nigerian phone number +2348091153589.

a. The phone number +14155309429 was listed in IRO's broken phone as being used by "Cj." The phone number +17075901571 was listed in IRO's broken phone, but not associated with a particular contact name.

b. The phone number +14155309429 was listed in one of Igbokwe's phones as being used by "Mr CJ." In that same phone of Igbokwe, "Mr. CJ" was also listed as communicating using the Nigerian phone number +2348091153589.

c. Based on records from AT&T for November 19, 2016 through October 20, 2017, the phone number +14155309429 was subscribed to "Chijioke Isamade" with an address in Sugar Land, Texas.

d. Based on T-Mobile records, the phone number +17075901571 was subscribed to "Chijioke Isamade" between August 31, 2016 and January 5, 2017, and that the phone number was earlier subscribed to a woman with the same last name between February 27 and August 31, 2016.

e. Based on records from Uber, the phone number +17075901571 was associated with two accounts: from January 28, 2016 through October 24, 2018 (the last date for which records were received from Uber), an account in the name "Prince CJ" that used the email address mrprincecj@icloud.com; and from October 16, 2016 through October 24, 2018, an account in the name "Chijoke Isamade" that used the email address princeisamadecj@outlook.com (the "username"<sup>16</sup> of which can be read as "prince isamade cj").

---

<sup>16</sup> The part of an email address before the "@" symbol is often referred to as the "username."

In addition to listing ISAMADE's name, these records also connect ISAMADE with the moniker "CJ," which corresponds to ISAMADE's first name, "Chijioke." Lyft records further show that accounts linked to the phone numbers listed above were subscribed to "Chijioke Isamade," "Prince Isamade," and "Mr Cj."

15. ODIMARA

67. FIEDEL LEON ODIMARA, who communicated with IGBOKWE using +17133666633, was listed in IGBOKWE's iPhone 7 Plus as "Ndaa"; in IGBOKWE's Samsung as "Fidel Odimara," "Dee Dutchman," and "Olubunmi Amusan"; and in IGBOKWE's iPhone 6S Plus as "amusan olubunmi," "dutchman dee," and "Ndaa USA."

a. T-Mobile records show that the phone number +17133666633 was subscribed to "Fidel Odimara," using an address of 10555 Turtlewood Court, Houston, Texas 77072, and that the service started on October 21, 2015. Records indicate that the account was canceled as of January 23, 2016, and other phone records indicate that the phone number was later associated with a pre-paid phone provider.

b. Records from Wallis State Bank indicate that ODIMARA, listing the same phone number, address, and date of birth, and providing a Texas driver's license (listing the same name, date of birth, and address), opened an account on August 9, 2016, claiming to be employed by an "auto dealer" called "General Auto USA."

c. Uber records indicate that "Fidel Odimara" created an Uber account on October 23, 2017, and that the registration information listed the phone number +17133666633 and email address fideleo2005@yahoo.com.

d. Yahoo records show that fideleo2005@yahoo.com, created on February 24, 2005, used the verified phone number +17133666633, and listed generalegroup@yahoo.com as an alternate email address and the subscriber's name as "Mr. fidel Jackson."

e. Yahoo records show that generalegroup@yahoo.com, created on February 4, 2011, also used the verified phone number +17133666633, listed

generaloilservices@yahoo.com as an alternate email, and listed the subscriber's name as "Fidel Odimara."

f. Instagram records indicate that +17133666633 was the verified phone number listed for an account of "De Dutchman," which was created on February 28, 2014 and used the vanity name "dedutchman." The registered email account was generalegroup@yahoo.com.

g. Records from messaging applications Tango and imo indicate use by +17133666633 of the moniker "Dutchman." The Tango account was created on November 22, 2012 using the name "De Dutchman," while the imo account listed the name "Dutchman."

#### 16. UGWU

68. KENNEDY CHIBUEZE UGWU primarily used one phone number— +17816545154—to communicate with IGBOKWE, as well as Facebook Messenger (under the name "Kennedy David" on IGBOKWE's iPhone 6S Plus). IGBOKWE's phones listed two phone numbers for UGWU, +17816545154 and +13473931600, which were associated with the names "Kennedy," "Kennedy Ugwu," "Kennedy USA," and "Kennedy David."

a. On several occasions, UGWU (using +17816545154) provided IGBOKWE with his name so that IGBOKWE could direct payments to him. For example, on December 29, 2017, UGWU provided his name as "Kennedy c ugwu," and stated that he lived in "Brockton Massachusetts." Additionally, on March 21, 2017, UGWU asked for payment to "Kennedy ugwu," and stated that he lived in Boston, Massachusetts.

b. Other records also indicate that UGWU used these phone numbers and the Facebook persona "Kennedy David."

i. Personnel records from Northeast Security Inc. confirm that UGWU, who was employed there from August 2016 through July 2018, used the phone number +17816545154, the email address kennedyugwu22@gmail.com, and an address in Brockton, Massachusetts.

ii. Records from T-Mobile for +17816545154 show that it was subscribed to UGWU through T-Mobile from May 31, 2017 through July 29, 2018, listing the address in Brockton, Massachusetts referenced above.

iii. Finally, Facebook records show that the account of “Kennedy C. David,” created on April 18, 2015, used three verified phone numbers, including +17816545154 and +13473931600. The account used the vanity name kennedy.ugwu.7 and the email address kennedyugwu22@gmail.com.

17. AGWUEGBO

69. IFEANYICHUKWU OLUWADAMILARE AGWUEGBO communicated with IGBOKWE using the phone number +14015360073, which was listed in IGBOKWE’s iPhone 7 Plus as “B🌐\$\$ IFF¥.”

70. Based on information from a Wells Fargo investigator, AGWUEGBO opened a bank account at Wells Fargo in 2016, in connection with which he listed his name as IFEANYICHUKWU AGWUEGBO; his phone number as +14015360073; and his address as 8907 Deer Meadow Dr., Houston, Texas 77071.

71. Other financial records also confirm that AGWUEGBO used this phone number and address. Records show that AGWUEGBO conducted financial transactions on five separate occasions in 2017, each time listing his name as IFEANYICHUKWU AGWUEGBO; his phone number as +14015360073; and his address as 8907 Deer Meadow Dr., Houston, Texas 77071. These transactions were in the same period in which “B🌐\$\$ IFF¥” was using the phone number +14015360073 to converse with IGBOKWE. Moreover, the date of birth provided during these transactions matched the information from AGWUEGBO’s Texas driver’s license and the birthdate he provided to Wells Fargo.

72. More recently, Bank of America (“BOA”) records for an account ending in 1769 show that the account was opened on December 6, 2018 by AGWUEGBO, listing the same address on Deer Meadow Drive.

18. CHUKWU

73. Evidence indicates that VICTOR IFEANYI CHUKWU used the phone number +13232374383. That phone number was listed in IRO's phone as "Ifeanyi Soccer"; in one IGBOKWE's phones as "Vic," "Vic Chux," and "Anyi LA"; and in EROHA's phone as "Ifeanyi," all of which are similar to parts of CHUKWU's name.

a. In a message to IRO on November 28, 2016, "Ifeanyi Soccer" stated: "My name is victor chukwu and I live in Los Angeles, California."

b. T-Mobile records indicate that the phone number +13232374383 was subscribed to VICTOR CHUKWU starting on August 13, 2016 through the date on which records were provided, July 5, 2018.

c. On July 14, 2017, in connection with an investigation by the FBI in Jacksonville, CHUKWU was interviewed by FBI Los Angeles SAs Cody Burke and Joseph Hamer. During that interview, CHUKWU provided his phone number as +13232374383, and his email address as ifydiddy@yahoo.com. Records for that email account indicate that it was created on February 9, 2007, subscribed to "Mr. Ifeanyi Chukwu," and used the verified phone number +13232374383.

d. Uber records indicate that CHUKWU created a driver account on March 25, 2016, using the email address vic.chukwu@yahoo.com (the same date the email address was created) and the phone number +13232374383. Separately, during CHUKWU's interview on July 14, 2017, he stated that he was an Uber driver. (This appears to be false, given that Uber records indicate that as of April 18, 2018, CHUKWU had not actually driven anyone.) Lyft records further connected the phone number +13232374383 to CHUKWU, through the subscriber name on the account (Ifeanyi Chukwu) and the email address ifydiddy@yahoo.com. That email address was also used to create an account using the name "Victor Chukwu."

19. MEGWA

74. CHIDI EMMANUEL MEGWA communicated with IGBOKWE using the U.S. phone number +17542136149, which was listed in IGBOKWE's Samsung as "Cantr" and a

Facebook contact for “Canta Jr. Jr. Emmanuel,” and in IGBOKWE’s iPhone 7 Plus as “Canta Jr.” That entry in the iPhone 7 Plus also listed another U.S. phone number for “Canta Jr.”: +16824141984. That phone number exchanged numerous phone calls with IGBOKWE’s iPhone 7 Plus and iPhone 6S Plus, in addition to several messages with the iPhone 7 Plus.

a. The Facebook account referenced above was created on April 27, 2010, and listed three registered email addresses: jaz\_y2004@yahoo.com, megwaemmanuel@yahoo.com, and kodioluvsu@yahoo.com. Of those, only records for jaz\_y2004@yahoo.com were available, but it is notable that megwaemmanuel@yahoo.com contains part of MEGWA’s name in the account name. Similarly, Yahoo records show that jaz\_y2004@yahoo.com was created on November 20, 2004, and listed the subscriber’s name as “Mr Chidi Megwa.”

b. Lyft records show that the telephone number +17542136149 was registered to two accounts, both with connections to MEGWA. One account, created on February 19, 2017, was subscribed to user name “Chidi Emmanuel DUP,” and used the email address megwachidi@gmail.com. A second account created on October 29, 2016 was subscribed to “Chidi Emmanuel” and listed the email address megwachidi@gmail.com. The account telephone number was listed as +16823470113, but was previously +17542136149.

c. Finally, MEGWA’s DMV photograph is consistent with a person pictured in three photographs that “Cantr” sent to IGBOKWE on February 19, 2017, which show that man with IGBOKWE and EROHA at a club with two other men.

## 20. DURU

75. Beyond the evidence described below (see Section III.H.15) showing that PRINCEWILL ARINZE DURU used +19169979097 to communicate with IGBOKWE, other evidence indicates DURU used that phone number.

a. In a message on IGBOKWE’s iPhone 7 Plus, on January 24, 2017, DURU sent information for his Chase account ending in 2101 to IGBOKWE, stating the name “Princewill Duru A.” Chase records confirm that the account belonged to DURU, who listed an

address in Carmichael, California, and that he also listed the phone number +19169979097 and the email address princeeznira@gmail.com.

b. Similarly, records for a BOA ending in 4859, dba “PD Enterprise,” show the account holder was DURU, with an address in Sacramento, California. The account records indicate that DURU provided the phone number +19169979097, and the email addresses pdenterprise2017@gmail.com and prnceduru22@yahoo.com.

76. Other evidence also indicates that DURU used the phone number +19169979097:

a. Sprint records indicate that the phone number +19169979097 was subscribed to “Princewill Duru,” with an address in Carmichael, California, between December 28, 2016 and September 20, 2018, which is the last date for which records were provided.

b. Records from Uber also indicate that DURU used +19169979097. Specifically, an Uber account was created on September 16, 2017 using the name PRINCEWILL DURU, the phone number +19169979097, and the email address prnceduru22@yahoo.com.

c. Records from Google indicate that princeeznira@gmail.com used the name “King Eznira,” the phone number +19169979097 and the recovery email account prnceduru22@yahoo.com. (“Eznira,” which is in both the subscriber name and email address, is “Arinze” spelled backwards, which is DURU’s middle name.) Records from Facebook, Twitter, and Tango indicate that accounts were created using the email account princeeznira@gmail.com, with the Facebook account also using the name “Princewill Eznira” and the phone number +19169979097.

21. UKACHUKWU

77. MUNACHISO KYRIAN UKACHUKWU communicated with IGBOKWE using the phone number +15104177578. IGBOKWE’s iPhone 7 Plus contained three contacts for “Muna” listing that phone number, and one additional imo application contact listing the name “Muna Ukachukwu” and the phone number +15104177578.

a. Records for the imo contact showed that “Muna Ukachukwu” signed up for imo on December 10, 2015, used the phone number +15104177578, and listed

munaukachukwu@gmail.com as a verified email address. The Twitter account @MunaUkachukwu also used that Gmail account in its subscriber records. (Another Twitter account, @Munachiso18, used the phone number +15104177578.)

b. Google records show that munaukachukwu@gmail.com, which was created on January 21, 2013, was subscribed to “Muna Ukachukwu,” and listed the phone number +15104177578.

c. UKACHUKWU also linked the email account munaukachukwu@gmail.com with a Skype account. That Skype account was created on February 19, 2010, used the name “muna ukachukwu,” and listed the email account munac\_2000@yahoo.com in its records.

d. T-Mobile records indicate that the phone number +15104177578 was subscribed to “Mumchiso Ukachukw” with an address of 366 Ohio Ave., Richmond, California, since December 19, 2018. Before that the account was subscribed to a person with the initials S.M.J. at another address on Ohio Ave., in Richmond, California, which is the same address listed in California DMV records for UKACHUKWU.

e. Lyft records indicate that UKACHUKWU created a driver account using telephone number +15104177578, on March 18, 2018. The account records showed he was a driver as of August 14, 2018 when the records were produced, and listed the user name “Munachiso Ukachukwu” and email address munac\_2000@yahoo.com.

## 22. OSMUND

78. NWANNEBUIKE OSMUND (using +14246720859) was listed in IGBOKWE’s iPhone 7 Plus as “Olivite,” EROHA’s phone as “Nikky Bros.,” and IRO’s Samsung Galaxy 6 Edge as “Nikky Bro.”

a. T-Mobile records indicate that the account of “Osmund Nwannebulke”—associated with the phone number +14246720859—was active from April 3 through June 26, 2017. The records listed the subscriber’s address in Carson, California. California DMV records

for OSMUND list the name “NWANNEBUIKE OSMUND” and show the same address in Carson, California.

b. Yahoo records show that +14246720859 was listed as the verified phone number for nwannebuikesmund@yahoo.com, which was created on May 18, 2017 and subscribed to “Osmund Nwannebuike.”

c. In a message on April 11, 2017, “Nikky Bros” wrote to EROHA, “Osmund Nwannebuike would like to chat with you on Skype. Go to <https://go.skype.com/dwnld>.”

d. A lease signed by OSMUND on February 28, 2018 likewise listed his name as “NWANNEBUIKE OSMUND.”

23. MADEKWE

79. OBI ONYEDIKA MADEKWE communicated with IRO and IGBOKWE using the Nigerian phone number +2347034724857, which was listed in IRO’s Samsung and IGBOKWE’s iPhone 7 Plus as “Odu Invest.” MADEKWE also communicated with IRO using +13106584080, which was listed in IRO’s Samsung as “Obi Soccer.” Records related to an imo messaging application contact in IGBOKWE’s iPhone 7 Plus listed the phone number +2347034724857 as being used by “OBI MADEKWE,” which phone number was also listed in the iPhone 7 Plus as “Obi LA.”

80. MADEKWE identified himself by name, or provided information related to his identity in his conversations with IRO and IGBOKWE. First, in his conversation with IRO, he provided the name “Obi Madekwe.” Second, in other messages with IRO, using his Nigerian phone number, he introduced himself to IRO as “Obi.” Third, during his conversation with IGBOKWE, he provided the Wells Fargo account ending in 1223 of “Obi Madekwe” and IGBOKWE referred to him as “Obi.”

a. Bank records indicate that the Wells Fargo account belonged to MADEKWE with the same address listed on his DMV record, as well as the email address [omadekwe1@gmail.com](mailto:omadekwe1@gmail.com) and phone number +13106584080.

b. Google records indicate that omadekwe1@gmail.com, which was created on April 17, 2009, was subscribed to “obi madekwe” and also used the phone number +2347034724857.

81. Finally, IRO’s and IGBOKWE’s messaging conversations reflect that MADEKWE had traveled to Nigeria, something that is corroborated by travel records. In the conversation with IGBOKWE, MADEKWE discussed being in Nigeria in April and May 2017, while in IRO’s conversation with Coconspirator 21, he discussed—while complaining about IKOGHO—how his “main exchanger” had gone to Nigeria, seemingly a reference to MADEKWE. Travel records from the Department of Homeland Security (“DHS”) indicate that MADEKWE traveled to Nigeria in April 2017.

**F. Use of Nigerian Pidgin and Code Words**

82. Based on my training and on my experience during this investigation (including review of tens, if not hundreds, of thousands of messages between the conspirators) and other investigations, and discussions with agents and linguists who are familiar with Igbo and Nigerian Pidgin, I have learned that Nigerian individuals involved in fraudulent schemes and money laundering sometimes use Igbo, Nigerian Pidgin, or code words while conversing, including through messaging applications. Some of those words are discussed in this section.

83. One such word that I have seen and am familiar with is “dating” (sometimes spelled “daten”) which appears to refer to what I know as a “romance scam.” Similarly, the words “maga,” “mugu,” and “client” often refer to victims of fraudulent schemes—frequently victims of romance scams, but at other times simply victims of scams.

84. The words “ali” or “alibaba” typically refer to what I know as a BEC scheme. The coconspirators sometimes also used the words “wire” or “wire wire” to refer to BEC schemes. They also sometimes use the word “Yankee” to describe a transaction originating in or going to the U.S. (e.g., “yankee to yankee”).

85. I have also observed that the coconspirators sometimes used 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” was also sometimes used to refer to a bank itself, while “warehouse” and “ulo aku” were words also used to refer to banks.

86. The conspirators sometimes used the word “burst” or “spoil” (i.e., a bank account “burst” or “spoil”) to refer to a bank discovering that a transaction was fraudulent. At other times, they would use the word “cast” to indicate that fraud had been detected and that the scheme had failed (e.g., “the job cast”).

87. I have also observed that the word “na” means “is,” “don” roughly means “did,” “wetin” roughly means “what,” “how far” means “hello” or “how is everything,” “abeg” means “please,” “bar” or “baa” sometimes means “money,” “no wahala” means “no problem,” and “naija” or “9ja” refer to Nigeria or a Nigerian phone number. I have also seen that the coconspirators at times use the letter “f” to refer to “funds,” and have observed that the word “oga” is used as a term of respect, similar to “boss.”

#### **G. Roles of Conspirators in the Conspiracy**

88. IRO, IGBOKWE, IKOGHO, UMEJESI, OGUNGBE, CATHEY, MANSBANGURA, AJAEZE, EKECHUKWU,<sup>17</sup> OJIMBA,<sup>18</sup> and EROHA were among the Los Angeles-based core of the conspiracy that facilitated the laundering of funds for numerous middle-men of fraudsters who were seeking bank accounts and money service accounts that

---

<sup>17</sup> In addition to opening accounts for IRO and IGBOKWE, and beyond his role in defrauding Je.F. and Jo.F., as discussed in Section III.H.12, EKECHUKWU was himself a middle-man for fraudsters. EKECHUKWU’s conversation with IRO included discussion of opening multiple bank accounts, “build[ing]” and “servicing” them, and having bank accounts closed, as well as EKECHUKWU asking IRO for bank accounts for “ali” for “100” and “dating of 7k.” EKECHUKWU’s conversation with IGBOKWE included EKECHUKWU asking IGBOKWE for bank accounts for “ali . . . 400k,” and “any uloaku for cable . . . 500k” (i.e., “any bank account for a wire of \$500,000”).

<sup>18</sup> As discussed in n.7, OJIMBA opened bank accounts for IRO and OJIMBA was nervous about drawing scrutiny on those accounts. As another example, on May 8,2017, OJIMBA again asked IRO to keep the incoming funds to “small small money.” IRO retorted, “Small small money. Like how much? 2m....5m...10m.. [¶] ??” When OJIMBA said “Like \$50,000 [¶] More smaller I beg,” IRO responded, “Lol. Bro you funny oo [¶] Do you think I do those kind of jobs??”

OJIMBA and IRO’s conversations also illustrate that OJIMBA also opened bank accounts in coordination with UMEJESI in the name of OJIMBA’s girlfriend, who is referenced in n.30.

could receive and then be used to launder the proceeds of fraudulent schemes. Their conduct is further discussed in Section III.H. Although DURU did not live in Los Angeles, he too, assisted the conspiracy in opening bank accounts into which fraudulent proceeds could be deposited, and was involved in defrauding victim D.J. (see Section III.H.15). The remainder of this section discusses the other defendants at issue in this complaint.

1. ONWUASOANYA

89. ONWUASOANYA was involved in both BEC frauds and romance scams. Beyond his involvement in defrauding Victim Company 1 (see Section III.H.1), he discussed “ali” and “dating” transactions with IRO. For example, on May 15, 2017, ONWUASOANYA asked IRO for a bank account for “dating” payments totaling \$200,000, and IRO sent him the account information for a BOA account of IGBOKWE ending in 2660, which is one that the conspirators used for romance scam payments.

90. In addition to being a middle-man to fraudsters, he was more actively involved in BEC frauds. IRO and ONWUASOANYA discussed creating email domains, which is something that BEC fraudsters do to spoof legitimate email addresses (see n.1). They also discussed using and deploying viruses (or “v”) and using “crypters.” Based on my training and experience I know that a crypter is software that can encrypt and hide malware, making it undetectable to security programs, such as antivirus software that scans incoming emails.

2. CHUKWUOCHA

91. CHUKWUOCHA was a middle-man to BEC fraudsters and romance scammers. In addition to his involvement in defrauding M.G. and the Victim Solicitor Firm (see Section III.H.26 and III.H.23), CHUKWUOCHA also asked IGBOKWE for accounts to use in “Alibaba” and dating,” as well as “wires.” Some were for significant amounts, with CHUKWUOCHA and IGBOKWE discussing potential fraudulent transactions of “100k,” “280k,” and “400k.”

### 3. UZOKA

92. UZOKA was a middle-man to BEC fraudsters and romance scammers. In addition to his involvement in defrauding Victim Company 9 (see Section III.H.17), which itself led to a loss of \$220,337.68, UZOKA made numerous requests to IGBOKWE for bank accounts for “ali” and “dating.” Among those were requests for bank accounts to use in an “ali” transaction of “300k,” a “dating” transaction of “350k,” and an “ali” of “40k from Malaysia.”

### 4. AWAK

93. AWAK was a middle-man to romance scammers and other fraudsters. In addition to his roles in the frauds involving victim R.B. (see III.H.4) and L.B. (see III.H.16), he discussed “dating” and “client” transactions with IRO on a number of occasions. On one occasion, in July 12, 2017, shortly before the FBI executed warrants at IRO’s apartment, AWAK requested an “acct for 500k [¶] [f]rom Australia” for an “[u]rgent” transaction.

94. As noted above, AWAK arrived to the United States on August 25, 2018. Within roughly a month of his arrival, he had filed four fictitious business name statements with L.A. County, all of which were used to open a bank account at Chase that received fraudulent funds. (AWAK filed at least eight fictitious business name statements since arriving in the U.S.) Based on an interview I conducted with a Chase investigator, a victim company in Bangalore, India sent \$675,823.89 into AWAK’s Chase account ending in 0898, dba “Airborn Commercial,” dba “MissionPharma A/S,” dba “OSHC Barqi Tojik,” dba “Pharmacie Nouvelle,” between September 28, 2018 and October 1, 2018. Prior to the initiation of a recall, a portion of the funds were depleted through debit card transactions by AWAK.

### 5. EGWUMBA

95. EGWUMBA’s conversations with IRO and EROHA demonstrated his involvement in the conspiracy as a middle-man to BEC fraudsters and romance scammers. Some of the transactions were for significant amounts, such EGWUMBA’s requests to IRO for a Chase account for a “wire of 2m” (i.e., to receive a fraudulent wire of \$2 million) on June 18, 2017 and for an “Aza 4 wire – 200k” on June 26, 2017.

96. EGWUMBA and EROHA also had an extensive discussion about the percentages of fraudulently-obtained proceeds that EGWUMBA would receive depending on the type of fraud—whether “dating” or “ali”—and the type of bank account. EGWUMBA asked EROHA, “Okay Wetin be % for normal aza?” EROHA replied “Dating na 25% but if na you I go collect. Ali na 50%.”—i.e., EROHA was informing EGWUMBA that he would normally take 25 percent if the transaction was a romance scam, and 50 percent if the transaction was a BEC scheme. Later, EGWUMBA asked, as to the “ali” rate, if it was for “Ali open bene?” because the “guys complain for the amount I gave them for open bene.” In response, EROHA explained the various rates that EGWUMBA would have to pay based on the type of fraudulent scheme and account:

Ali open bene: we take 60% and U take 40% with them.  
Ali normal: we take 50% and they take 50.  
If you have middle man in ali open bene...i take 50 and give you & them take 50.  
Ali normal: if i have middle man, i take 45 and give una 55.  
Dating. I Collect 20 or 25 depends on my relationship with you.

EROHA’s messaging conversation with IRO indicates that EROHA received the information he quoted to EGWUMBA from IRO. In addition to being evidence of criminality, this illustrates the rates that IRO and EROHA would charge for receiving and laundering funds. IRO and IGBOKWE had numerous similar conversations with other coconspirators, in which they discussed and negotiated rates that they would charge.

97. In addition to being a middle-man, EGWUMBA himself appeared to be involved in hacking. EGWUMBA discussed with IRO how he had been using a “virus,” which he also appeared to reference as a “v.” Based on the conversation, it appears that EGWUMBA was unsatisfied with the performance of the virus, because he stated “[t]he v no good” and “them say make I send 200k for better v.”

## 6. ISAMADE

98. ISAMADE was a middle-man to BEC fraudsters and romance scammers. For example, on March 14 2017, ISAMADE asked IGBOKWE for a bank account into which “dating” funds totaling “59k” could be deposited, He also asked IGBOKWE for an account for

“ali” for “290 from india” (i.e., likely a BEC fraud payment of \$290,000 coming from a victim in India).

99. Additionally, IRO and ISAMADE engaged in several conversations related to fraudulent schemes, which indicate that in addition to ISAMADE getting accounts from IGBOKWE to use for romance scams and BEC, he also opened one account for IRO for BEC frauds and was involved in making deposits into accounts for IRO. For example, on March 29, 2016, IRO messaged ISAMADE about opening an account in the name of a Thai company (the “Thai Company”). IRO stated, “Can you move tomorrow?? [¶] [Thai Company] [¶] Chacha or wall of Jerusalem or us [¶] Don’t go to B.” Based on my experience with the messaging conversation and code sometimes used by the coconspirators, it appears IRO was telling ISAMADE to open the bank account at Chase, US Bank, or another bank, but not BOA.<sup>19</sup>

#### 7. ODIMARA

100. ODIMARA engaged in several conversations with IGBOKWE indicating his criminal intent and involvement in the conspiracy. For example, on April 13, 2017, ODIMARA sent the following message: “USAA BANK \$90,000 [¶] BB&T BANK \$ 30,000 to \$40,000 [¶] I need HSBC account in USA for 50k in tranches without online. And citizens bank account for 300k without online urgently. If you have any do let me know.” The next day, ODIMARA told IGBOKWE that “We should have the slip by Monday total done was \$27k plus.”

101. On April 28, 2017, ODIMARA sent a photograph of a computer screen showing a Bank of China (HK) wire of \$36,274 to a Wells Fargo bank account ending in 7276, which was opened by a coconspirator. Much of ODIMARA and IGBOKWE’s conversation over the next week related to that wire and ODIMARA questioning why it had not been confirmed as deposited in the account. For example, IGBOKWE told ODIMARA several times that nothing came into the account, and ODIMARA on May 2, 2017 sent the account information back to IGBOKWE to confirm that it was correct. Later on May 2, 2017, IGBOKWE provided apparent

---

<sup>19</sup> On April 3, 2017, IRO also asked OJIMBA to open an account in the name of the same Thai Company at “cha or us or Wells.”

online account login information for this bank account, saying, “This is the username: [REDACTED] [¶] Password:[REDACTED].” IGBOKWE provided that account information on May 5, 2017, as well.

102. IGBOKWE sent other information related to bank accounts to ODIMARA on other occasions, as well.

#### 8. UGWU

103. Based on his communications with IGBOKWE, UGWU was involved in both romance scams and BEC frauds as a middle-man. For example, UGWU repeatedly communicated with IGBOKWE about payments from an apparent romance scam victim in Illinois in December 2016 and January 2017.

104. Following one such conversation, on January 5, 2017, UGWU told IGBOKWE, “Am still gonna go on with de plan [¶] To eat the f.” IRO, IGBOKWE, and others at times discussed “eating funds”—essentially stealing fraudulently-obtained funds deposited into an account by not providing it to the fraudster who is due the funds.

105. UGWU was also a middle-man for BEC frauds. For example, on January 2, 2017, UGWU requested, “Send me acc 4 alibaba.” IGBOKWE asked, “How much [¶] And coming from whr.” UGWU let him know that it was “500k” coming from “Turkey” and that “[h]e said he needs jp morgan.”

#### 9. AGWUEGBO

106. AGWUEGBO’s conversation with IGBOKWE indicates that he was involved in numerous BEC schemes as a middle-man. AGWUEGBO began his messaging conversation with IGBOKWE on March 7, 2017 by saying, “muna give me ya digit,” referring to UKACHUKWU (i.e., “Muna”). That day, AGWUEGBO asked IGBOKWE, “boss... which azah u get,” and IGBOKWE responded “Us bank [¶] Wells Fargo [¶] BOA.” AGWUEGBO clarified, “d job i get i need wells [i.e., Wells Fargo].. na alli [i.e., “ali” or a “BEC fraud”] n e dy come fron china most tymes.” IGBOKWE responded, “Ok Ali,” confirming his understanding that AGWUEGBO was primarily interested in bank accounts for use in BEC frauds, which

AGUEGBO had said would primarily come from China. IGBOKWE then sent AGWUEGBO a US Bank account ending in 9570, in the name “A & H Sales.” (Information on IGBOKWE’s phones show that he sent that account information to two other coconspirators on March 7 and 10, 2017.)

107. On March 14, 2017, AGWUEGBO stated, “100k.. i go need open bene.. d job.. dy come from yankee . . . yankee to yankee.” IGBOKWE provided a US Bank account ending in 0362, opened in the name “Danisha Beauty Sales.” (IGBOKWE received this account information from UMEJESI on March 1, 2017. He provided it to numerous coconspirators, including UZOKA and MEGWA.)

10. CHUKWU

108. Messages between IRO and CHUKWU indicate CHUKWU’s involvement in romance scams. On February 25, 2017, CHUKWU wrote to IRO, “Bros throw me that thing” to which IRO responded by providing CHUKWU with the account information for a Wells Fargo account ending in 6969. This account was opened by EKECHUKWU, and is known by the FBI to have received romance scam proceeds.

109. On March 6, 2017, CHUKWU asked IRO, “U dey do dating payment us to us?” and IRO responded “Yes.” CHUKWU then asked IRO, “That boa dey good for 50k[,]” and IRO responded, “Send it here again [¶] Let me see.” CHUKWU then provided IRO with account information regarding a BOA account ending in 2942, apparently to confirm the details that would be included in deposit or wire instructions. IRO directed CHUKWU to “put purpose of payment” and provided the following string of letters and numbers to list: “SOH6743357.” IRO then further explained that for “dating” payments a “purpose” for the payment should be listed. (IRO at other times provided similar guidance to other coconspirators, presumably to lessen the chance of bank scrutiny on the transactions.)

11. MEGWA

110. MEGWA supplied IGBOKWE with accounts that could be used to receive fraudulently-obtained funds, and also received bank and money service account information from IGBOKWE.

111. For example, on January 25, 2017, MEGWA sent IGBOKWE two bank accounts with the business name “Danisha Beauty Sales”—one at Wells Fargo ending in 7245 and another at US Bank ending in 0362. The Wells Fargo account was one that UMEJESI later sent IGBOKWE to be used in the fraud involving Victim Company 4, an indication of MEGWA’s involvement in the same conspiracy. IGBOKWE sent both accounts to numerous coconspirators over the next several months for use in fraudulent schemes.

112. Likewise, on February 11, 2017, MEGWA sent IGBOKWE the information for three bank accounts—the US Bank account mentioned above and two Wells Fargo accounts, one account number ending in 8957 opened by a money mule with a business name resembling that of a Chinese company, and the second account number ending in 5614 in the name of the same money mule. MEGWA told IGBOKWE that the Wells Fargo accounts had been closed. After attempting to login online to the accounts (indicating his control of the accounts), MEGWA also later confirmed that the “US account is alive [¶] That wells fergo done close.” IGBOKWE then instructed MEGWA, “Make we keep aza for big f aside and keep small f aside” (that is, seemingly telling MEGWA to keep some accounts for receiving funds from large fraudulent transactions and others for receiving funds from smaller fraudulent transactions), and also instructed MEGWA to send any money he got to his “Niger aza” (i.e., Nigerian bank account).

113. IGBOKWE also sent MEGWA account information, including the Chase account ending in 7605 of Coconspirator 7, dba “M&F Enterprises,”<sup>20</sup> and accounts of a relative of MANSBANGURA at US Bank, Citibank, and Wells Fargo in February and March 2017.

---

<sup>20</sup> Based on bank records, the Chase account ending in 7605 was opened by Coconspirator 7 on December 22, 2016 with the business name “T and F Enterprises.” IGBOKWE, however, often provided the account name to co-conspirators as “M & F Enterprises.” This affidavit refers to that Chase account ending in 7605 by both names.

114. Also of note, on February 14, 2017, IGBOKWE chastised MEGWA for talking about funds on a phone line, instead saying that MEGWA should call through WhatsApp. Specifically, IGBOKWE stated, “Don’t talk about f [i.e., funds] in phone again [¶] Talk what’s up [i.e., WhatsApp] now.”

12. UKACHUKWU

115. UKACHUKWU was also involved in fraudulent schemes. On March 16, 2017, after receiving a call from UKACHUKWU, IGBOKWE sent UKACHUKWU a message containing the account information for the BOA account ending in 4859, opened by DURU, dba “PD Enterprise.” IGBOKWE sent this same account to other coconspirators for use in both BEC frauds and romance scams as well, including ISAMADE and the persons described below as Coconspirators 5 and 11.

116. UKACHUKWU responded to IGBOKWE, “Ok [¶] Wetin be the %[?]” In addition to the fact that IGBOKWE sent UKACHUKWU this account used for receiving the proceeds of fraud, UKACHUKWU’s negotiation of a rate for use of the account also is an indication of his criminal intent and involvement in the conspiracy. The call log reveals that IGBOKWE and UKACHUKWU spoke later than evening, as well.

117. On March 20, 2017, IGBOKWE asked for an “update” on the use of the account, saying, “Try make we know when they will do the payment.” UKACHUKWU responded, “He hasn’t done it yet bro . . . I just asked [¶] He just said this week.”

118. IGBOKWE also received numerous calls from UKUCHUKWU between late June 2017 and July 17, 2017. Other messages on IGBOKWE’s phones also indicate that UKACHUKWU knew and associated with other coconspirators, including DURU and AGWUEGBO.

13. OSMUND

119. OSMUND was a middle-man in a fraudulent scheme. On June 27, 2017, OSMUND told IGBOKWE, “I need aza us to us client.” (As noted earlier, “client” is a reference

to a fraud victim, often a victim of a romance scam.) In response to IGBOKWE's question "[H]ow much[?]," OSMUND said, "2,430."

120. IGBOKWE sent the Chase account ending in 7605 of Coconspirator 7, dba "M & F Enterprises." This is an account that received the proceeds of fraud schemes, including payments from elderly fraud victims B.Z. and B.P., as discussed below (see Sections III.H.8 and III.H.22, respectively).

121. OSMUND then discussed the rate that IGBOKWE would charge, saying, "I conclude with him 30 but him get 5p as contact person we na 25p...hopecits ok like that?" (In other words, OSMUND was asking IGBOKWE whether he could give 5 percent to his contact while OSMUND and IGBOKWE split the remaining 25 percent.) IGBOKWE responded, "I go call my woman," referring to MANSBANGURA. OSMUND then asked, "Ok make i give am the aza? [¶] Cos its urgent." (In other words, "Ok, can I give him the bank account, because it's urgent?") IGBOKWE responded, "OK."

14. MADEKWE

122. As discussed below, MADEKWE was IRO's money exchanger. (See paragraph 196.l) Their WhatsApp conversation included discussions of how funds were "clean[ed]," how to move money without detection, and how MADEKWE's Wells Fargo account had been shut down. However, once MADEKWE went to Nigeria in March 2017, he did not do much money exchanging for IRO. Instead, he became one of IGBOKWE's primary money exchangers.

123. The messaging conversation between IGBOKWE and MADEKWE is a roadmap to how he and IGBOKWE laundered funds. In general, their conversation illustrated that it would work as follows:

a. First, IGBOKWE would send MADEKWE a photograph of a cash deposit into a U.S. bank account used by MADEKWE. Often that would be a Chase account ending in 3891 of another person. (In addition to sometimes being pictured in IGBOKWE's conversation with MADEKWE, multiple of these receipts were found during the search at IRO's apartment.)

b. Then IGBOKWE would tell MADEKWE where to direct the funds from his Nigerian bank account. Sometimes he would ask to have the money sent to Coconspirator 18 or Coconspirator 19, who would in turn then pay a coconspirator. Other times IGBOKWE would ask MADEKWE to directly pay a coconspirator, as he did for a number of known coconspirators, or a make a payment to IGBOKWE's Nigerian bank account.

c. MADEKWE would then often send a confirmation message—sometimes a screenshot of his United Bank for Africa (“UBA”) banking application—which often listed the name of the coconspirator being paid. IGBOKWE would then sometimes send this screenshot to the coconspirator to confirm the transaction.

d. In this manner, MADEKWE exchanged and laundered nearly \$100,000 for IGBOKWE alone in two months, from May 15, 2017 through July 18, 2017, based on their messaging conversation. In addition, the Chase account ending in 3891 used by MADEKWE reflects several other deposits from accounts used and/or controlled by IGBOKWE and MANSBANGURA, adding up to close to \$15,000 more.

#### **H. Victims of the Conspiracy**

124. The conspiracy has victimized numerous individuals and companies causing pain and suffering for the victims, and millions of dollars in losses. The victims specifically discussed in this section were defrauded of nearly \$6 million attributable to the Los Angeles-based conspirators. As noted above, these victims represent only a portion of the victims who were defrauded, or attempted to be defrauded, by the conspiracy.

1. Victim Company 1—September 2014 BEC Fraud (involving IRO and ONWUASOANYA)

125. I interviewed personnel from Victim Company 1 in July and September 2017. Based on that interview, I know that Victim Company 1 is a San Diego County-based distributor of clothing items that was the victim of a BEC fraud in September 2014. Personnel from Victim Company 1 were communicating with a Chinese vendor (“Chinese Company 1”) about an order for men's shirts. Unbeknownst to personnel from either company, an unknown fraudster had

hacked one of the email systems, blocked emails, and was separately communicating with personnel from both Victim Company 1 and Chinese Company 1. On September 3, 2014, at the direction of the unknown fraudster in an email received on September 1, 2014, Victim Company 1 sent a wire of \$45,783.97 to a fraudulent HSBC Bank account ending in 6100. The fraud was not discovered until approximately two weeks later, by which time the funds were unrecoverable.

126. Yahoo instant messaging conversations between IRO (using valentino\_q2000@yahoo.com), on the one hand, and ONWUASOANYA (using samuelnnamdi@rocketmail.com) and Coconspirator 1, on the other hand, indicate that ONWUASOANYA was a middle-man for Coconspirator 1, who was involved in the fraud, while IRO assisted in the fraud by speaking to personnel from Chinese Company 1 on September 11, 2014 while pretending to be “Allen” from Victim Company 1. IRO’s and ONWUASOANYA’s involvement is further discussed in the following paragraphs.

127. On September 11, 2014, ONWUASOANYA discussed with IRO having his “contact” call IRO to discuss a scheme. ONWUASOANYA also told IRO, “+17246483504 (USA) [REDACTED] is connected to ur no.” As discussed later, that phone number was a phone number that the fraudsters sent to Chinese Company 1, purporting it to be for “Allen” from Victim Company 1. ONWUASOANYA then explained that “he”—i.e., Conspirator 1—will call your “9ja” (i.e., “Naija” or Nigerian phone number) “to explain tings [sic] for u.” ONWUASOANYA added, “company name is [Victim Company 1] USA [REDACTED] purchase manager and ur name as Allen [REDACTED] is Allen [REDACTED] then the purchase managers name is Allen the company is located in [ADDRESS REDACTED] the payment was made on 9/3/2014 total sum (\$45,783.97).” (As noted earlier, this is the exact amount that Victim Company 1 was defrauded out of a week earlier.)

128. ONWUASOANYA continued, “see wetin we send them now [REDACTED] Hi Ruth, I do hope that we understand each other on this Situation. I want you to treat this issue with utmost urgency. At the moment the shipment is being delayed because you are yet to release the goods and the refunds and we are out of stock and our customers are at our neck. Please see the need to

address this issue as soon as possible. Here is my number: +17246483504 i am available at the moment. Thank you for your cooperation. Thank you. Mr. Allen [Victim Company 1] Purchase Manager For and on behalf of [Victim Company 1] USA.” ONWUASOANYA also sent IRO some other messages that had purportedly been sent to Chinese Company 1 personnel. Based on the messages, it appeared that ONWUASOANYA, Coconspirator 1, and others may have been attempting to avoid discovery of the conspiracy.

129. Shortly after IRO began instant messaging with ONWUASOANYA on September 11, 2014, he also began conversing with Coconspirator 1. Coconspirator 1 provided similar information as ONWUASOANYA, making it evident that he was the “he”—i.e., ONWUASOANYA’s coconspirator who wanted to talk to IRO—to whom ONWUASOANYA referred. The lengthy conversation began with Coconspirator 1 saying, “MAN NO TIME TO WASTE,” and the information he provided included, “the purchase managers name is Allen . . . the company is located in [CITY REDACTED] California . . . the payment was made on 9/3/2014 total sum (\$45,783.97.” Coconspirator 1 told IRO that “Frank” was Allen’s agent in China and he would call “any moment now.” Coconspirator 1 also sent IRO the same message from “Allen” to Ruth, providing Allen’s phone number as the one that ONWUASOANYA reassigned to IRO’s phone. After Coconspirator 1 finished providing background information to IRO, he asked if IRO had any questions. IRO responded, “no [¶] reviewing everyting [sic].”

2. M.S.—August and September 2015 Fraud Scam (involving IRO and Coconspirator 2)

130. M.S., a 61-year old woman who lives in the Central District of California, fell victim to several online scams, some of which were romance-type scams through Facebook. I interviewed M.S. in September 2017, and she also provided relevant electronic evidence, including communications with fraudsters. Based on this, I know the following:

a. In May 2015, M.S. met a person on Facebook using the name “Dennis Hunt” (“Hunt”), who tried to start a relationship with her. Hunt claimed that he was living in

London and worked in real estate construction. He communicated with her through Facebook Messenger and two phone numbers with +44 telephone codes—U.K numbers.

b. At some point, Hunt asked for money for a work project. M.S. provided the money as a loan, asking Hunt to sign an IOU, which Hunt did not honor. During the course of two months, M.S. sent \$111,200 supposedly on behalf of Hunt, \$91,200 of which was deposited into IRO's Chase VOI Enterprises checking account: \$23,000 on September 3, 2015; \$46,500 on September 8, 2015; \$4,700 on September 10, 2015; and \$17,000 on September 14, 2015.

c. M.S. lost all of this money, which was primarily withdrawn from IRO's account as cash.

131. Bank records show that the VOI Enterprises checking account had a balance of \$109.59 prior to the first of the wires. They also indicate that IRO attempted to disguise the transactions as related to purchases of automobiles.

a. Following the arrival of the first wire from M.S., IRO withdrew \$14,000 on September 4, 2015, and wrote at the bottom of the withdrawal slip, "for Lexus RX330 and RX300." On September 4, 2015, IRO also wrote a check to a relative, with the memo line stating "2002 Nissan Optima."

b. On the date of the second wire, September 8, 2015, IRO withdrew \$8,000, and wrote at the bottom of the deposit slip, "for Acura MDX 2007." The withdrawal slip also indicated that IRO showed a California driver's license bearing a number that DMV records indicate was issued to him.

c. On September 10, 2015, IRO withdrew \$30,000, and wrote at the bottom of the withdrawal slip, "Mercedes 2011 and Lexis RX 350 2008." IRO also did a second withdrawal on September 10, 2015, of \$9,000.

d. On September 11, 2015, IRO wrote a check to an acquaintance for \$7,700, with the memo line stating "Camry 207 and Camry 05."

132. A series of deleted messages recovered from IRO's Samsung phone between IRO and Coconspirator 2, contain evidence of the fraud scheme involving M.S.

a. On September 3, 2015, the date of the first wire from M.S., IRO sent Coconspirator 2 the account information for the VOI Enterprises checking account, along with the instruction, "Payment for: ( INV: VOI53753 )." Based on bank records, this same payment information—"VOI53753"—was listed in the wire transfer details sent by M.S.

b. Additionally, immediately following that message, IRO told Coconspirator 2, "If your client will deposit it. No need for invoice number. But if it's a wire or any transfer. Please tell him to put the instruction I gave you. And please please please. If it's not dated [sic: "dating"] as you have told me, I will not be happy and I will return it to the sender. Because I don't do alibaba local." (This is consistent with other messages in which IRO stated he would accept money from others U.S.-based "clients" (i.e., romance scam victims) into his bank accounts, but not "alibaba" (i.e., BEC) funds from U.S.-based victims.)

c. On September 14, 2015, the date of the last wire from M.S., IRO sent Coconspirator 2 a message saying, "Invoice number: VOI00462 R MODEL 89." Based on bank records, that same notation appeared in M.S.'s wire, which said, "Invoice No. Voi 00462 R Model 89."

i. The additional wires sent from M.S. had similar notations. On September 3, 2015, the wire notation said "Other Invoice No. Voi53753." And, on September 8, 2015, the wire notation said "Invoice No. Voi 50374 Mack."

3. Victim Company 2—February 2016 BEC Fraud (involving IRO)

133. On February 12, 2016, Victim Company 2, located in Texas, was fraudulently induced to send a wire for \$186,686 from its account at UBA to IRO's Chase VOI Enterprises checking account. Those funds, although initially frozen, were subsequently unfrozen and laundered by IRO through his Wells Fargo Irva Auto Sales account, and other accounts.

134. I interviewed the president of Victim Company 2 in May 2016, during which he discussed the fraud and provided relevant emails, based on which I know the following:

a. On February 4, 2016, shortly after placing an order for oil extraction equipment from a company located in the Central District of California (“California Company 1”), Victim Company 2 received bank account information from California Company 1 where it was to deposit a partial payment for the order. Within several hours of receiving that bank information, however, Victim Company 2 received new wiring instructions. For the next several days, Victim Company 2 employees communicated with whom they believed were California Company 1 employees, but were in fact fraudsters who appeared to have hacked California Company 1’s legitimate email accounts and were also using fraudulent email accounts created at Mail.com, Google, and Hotmail. (Victim Company 2 undertook an analysis of email header information, which showed that fraudulent emails from legitimate California Company 1 email accounts were sent from Nigerian IP addresses, as were some of the emails from the fraudulent email accounts.)

b. On February 12, 2016, the unknown fraudsters told Victim Company 2 that California Company 1 would accept 50 percent of the full payment, and provided account information for the VOI Enterprises checking account. Victim Company 2 wired \$186,686 from its UBA account to that account on February 12, 2016.

c. Victim Company 2 ultimately recovered \$55,593.18 of the \$186,686, but that was only after having to hire an attorney and spending at least \$50,000 on legal fees engaging with Chase.

135. Bank records show the following:

a. The wire for \$186,686 (less \$35.00 for a wire fee) arrived in IRO’s VOI Enterprises checking account on February 12, 2016. At the time, the balance of the account was approximately \$30.00. (On February 12, 2016, an additional \$2,000 was deposited.)

b. On the same date, \$188,600 was transferred to IRO’s Chase savings account ending in 0820, in the name “VOI Enterprises” (the “VOI Enterprises savings account”) and then later that day, \$161,700 was transferred back to the VOI Enterprises checking account.

(Based on information obtained from Chase, the account was closed on February 25, 2016 after an internal investigation determined fraudulent activity had taken place.)

c. On February 16, 2016, \$132,950 was wired to the Wells Fargo Irva Auto Sales account, with the reference note: “Invoice: Mack Rd Model 2010 X.” At the time, that account had a balance of \$143.49. Also on February 16, 2016, IRO wired \$28,670 to the CalCom Federal Credit Union (“Calcom”) account ending in 3017 of Coconspirator 3, with the reference note: “Menhien Auction On Wednesday.”

d. From the Irva Auto Sales account, the \$132,950 was further laundered through additional wire transfers as well as a cash withdrawal. Specifically, on February 16, 2016, \$50,000 was wired to the BOA account ending in 1824 of “Bernards International”; on the same date, IRO made a cash withdrawal of \$50,000; and on February 18, 2016, IRO wired \$30,500 to the Chase bank account ending in 1279 of Coconspirator 4.

4. R.B.—March and April 2016 Romance Scam (involving IRO and AWAK)

136. I interviewed R.B. in February 2019, based on which I know the following:

a. R.B. is a 48 year-old woman who lived in Panama City Beach, Florida. Shortly after her first husband passed away, she met a person on Facebook with whom she started an online romantic relationship. He told her he was a doctor in the U.S. military, stationed in Libya and was a widower like her. He said he had a five-year-old daughter and he had lost his parents when the Twin Towers fell in the 9/11 terrorist attacks.

b. R.B. recalled sending money to help the fraudulent doctor and his purported child. R.B. felt that she was victimized during a very vulnerable time in her life and considered killing herself when she learned of the fraud after being contacted by Comerica Bank (“Comerica”).

137. Bank records indicate the following:

a. R.B. sent three wires to Los Angeles-area bank accounts from her Wells Fargo account in Panama City Beach, Florida: a wire for \$18,000 on March 31, 2016, to the

Comerica account ending in 2663 of IRVA Auto Sales & Equip Broker LLC (the “Comerica IRVA account”), located in Carson, California; a wire for \$39,000 to that same account on April 4, 2016; and a wire for \$30,000 to a Wells Fargo account ending in 7410, on April 7, 2016.

b. Comerica records indicate that the ending balance on the Comerica IRVA account on March 31, 2016 was \$18,623.66, and thus the account balance was \$623.66 at the time the \$18,000 wire was received. After the wires arrived in the account, there were several cash withdrawals from Nashville, Tennessee (where IRO admitted to the FBI he travels at times) and some other small debits. Some of the funds—\$55,024.19—were frozen by Comerica and then on April 14, 2016 were returned to Wells Fargo.

138. Several emails in enterprisesiro@gmail.com, obtained pursuant to an above-referenced searched warrant, indicate that IRO and other coconspirators—Coconspirator 5 and AWAK—were involved in defrauding R.B. and laundering the funds. Coconspirator 5 was a middle-man to the unknown fraudster communicating with R.B., and sent IRO several photographs of the wire transfers made by R.B. AWAK assisted IRO by making a fraudulent invoice to R.B. to make it appear that IRO had engaged in a legitimate transaction.

a. On March 31, 2016, Coconspirator 5 sent IRO an email saying “PAYMENT RECEIPT 18,000.00,” and attached a photograph of a wire transfer request from R.B. for \$18,000. The wire transfer request listed R.B.’s name, Florida driver’s license number, address, phone number, and Wells Fargo bank account number.

b. On April 4, 2016, Coconspirator 5 sent IRO an email titled “slip,” which email said “PAYMENT RECEIPT \$39,000.00” and attached a photograph of a wire transfer request.

c. On April 12, 2016, Coconspirator 5 forwarded an email saying “PAYMENT RECEIPT \$30,000.00,” and attached a photograph of a wire transfer request from R.B. for \$30,000 to the Wells Fargo account ending in 7410. In the email, Coconspirator 5 stated, “Nwanne see another \$30,000 slip after he did urs of 39k. This is a part payment of that 62k and this men re expecting balance today.”

d. On April 13, 2016, IRO forwarded the last email to ccs03h@gmail.com, which was listed as using the name “HANOI BATTERY JSC,” saying, “The slip is for 11k payment and the picture is for the 39 payment. They both have to do with shipping company. So please do it something relating to equipment.” The email attached the photograph of the March 31, 2016 wire transfer request as well as a new photograph of a “domestic advice” containing wire transfer details for the \$39,000 wire sent on April 4, 2016 to the Comerica IRVA account. As discussed in Section III.E.12, the email address ccs03h@gmail.com was used by AWAK.

e. The next day, AWAK’s email address ccs03h@gmail.com—which this time displayed the name “Kwee Tin Law”—responded, simply saying “Attached” and attaching a PDF file. The PDF contained a purported invoice to R.B. from “IRVA Auto Sales Equipment Broker LLC,” listing an address of 412 Gina Dr., Carson, California (IRO’s former residence). The fraudulent invoice falsely purported to be related to two different invoices sent on February 11, 2016 and January 29, 2016, and the total amount listed on the invoice was \$39,000, corresponding to the second wire sent by R.B.

5. F.K.—May and July 2016 Romance Scam Victim (involving IGBOKWE and MANSBANGURA)

139. F.K. is a Japanese romance scam victim, who lost more than \$200,000 during the course of a 10-month romance scam. She was fraudulently-induced to send funds to individuals in Turkey, the United Kingdom, and the U.S., including to two bank accounts used and/or controlled by IGBOKWE and MANSBANGURA—specifically, accounts in the name of MANSBANGURA’s relatives, Coconspirator 7 and Coconspirator 8.<sup>21</sup> F.K. was also fraudulently induced to make a trip to Los Angeles, California in October 2016, in order to assist the coconspirators in unfreezing one of those wires. Upon F.K.’s arrival, MANSBANGURA, impersonating Coconspirator 7, met with F.K. and drove her to a bank to unfreeze the wire.

---

<sup>21</sup> In order to obscure the identities of relatives of the charged defendants who are themselves uncharged coconspirators, this affidavit in places redacts identifying information and references.

140. I and other agents interviewed F.K. in November 2018, with the assistance of translators. In addition to being interviewed, F.K. also provided copies of additional communications with the fraudster with whom she was communicating and photographs, including some taken when she came to Los Angeles in October 2016. Based on these, I know the following:

a. In March 2016, F.K. began communicating through InterPals—an international social network intended to essentially be a pen pal network for the digital age—with a person using the name Terry Garcia (“Garcia”), who claimed to be a U.S. Army captain stationed in Syria. F.K. and Garcia began communicating by email and he began making romantic overtures to her. Although F.K. was not looking for a relationship, at some point she viewed herself in a romantic relationship with Garcia. They communicated daily, or once every two days, by email, with Garcia using a Yahoo email address. F.K. and Garcia never spoke by phone, because he said that he was not allowed to speak on the phone from Syria. F.K. and Garcia only communicated in English, and F.K.’s English is poor. She translated most of his emails, and those that she sent to Garcia, using Google Translate.

b. Approximately a month after beginning to communicate with Garcia, he told F.K. that he had found a bag of diamonds while he was in Syria. Shortly afterward, F.K. was contacted by email by someone using the name Collins Coster (“Coster”). Coster claimed to be a diplomat working with the Red Cross. He said that Garcia had been injured in Syria but that Garcia had given Coster a box, which he referred to as a “consignment,” to send to F.K.. Although Coster did not ever mention the contents of the box, Garcia separately emailed F.K. letting her know that he was sending the diamonds through Coster and that he could trust Coster.

c. After ultimately agreeing to accept the consignment, F.K. was contacted by a person using the name Owen Blair (“Blair”) who claimed to work for a company that would be shipping the “consignment.” Blair informed F.K. that she would need to pay for a customs “non-inspection tag,” which she was told would cost £1420 or \$2000. F.K. says that she also received emails from Garcia asking her to make the payment, so she made payment on April 11,

2016 via Western Union to an account in Turkey. Shortly after that, she received emails saying that she would need to pay a “final accreditation fee” of \$6,200 for the “non-inspection tag.” She paid that amount as well, also to a Western Union account in Turkey.

d. After that, F.K. was contacted by a person using the name Diplomat Romaine Kaufman (“Kaufman”), who claimed to be physically bringing the “consignment” from the U.K., through customs in Japan. Kaufman, who used a Gmail account, told F.K. that she would have to pay a “diplomatic consignment tax” of \$28,750 to get the box through customs. F.K. again paid, this time to a bank account in Turkey.

e. The fraudster(s) kept coming back to F.K. using various personas, asking for additional money through different fraudulent representations. (At one point, the fraudster(s) even told F.K. that Kaufman was stuck in customs for more than a month because F.K. did not make a payment, and threatened F.K. with arrest by the U.K. authorities if she did not continue to pay.) F.K. estimates that she made 35 to 40 payments over the ten months that she had a relationship with Garcia. During that time, the fraudster(s) emailed her as many as ten to 15 times each day, and Garcia was asking her to make the payments, so she kept paying to accounts in Turkey, the U.K., and the U.S. In total, she lost more than ¥ 23,000,000, which is more than \$200,000. Of that, F.K. borrowed more than half from others, including friends, her older sister, her ex-husband, and a bank.

f. F.K. was and is extremely depressed and angry about these losses, and is on the verge of bankruptcy. She began crying when discussing the way that these losses have affected her.

141. Bank records indicate that two of the wires sent by F.K. went to accounts in Los Angeles. The first was a wire of \$6,824.00 (less \$10.00 for the wire fee) on May 30, 2016, to a Chase account ending in 1577, opened by Coconspirator 8. F.K. sent a second wire of \$33,128.26, on July 13, 2016, to a Chase bank account ending in 0655, in the name of Coconspirator 7.

142. F.K. further stated that after she made that payment of \$33,128.26, she was contacted by the fraudster(s) and told through a series of emails that the bank would not release or return the funds, and eventually that a Russian bank manager in Los Angeles had embezzled the funds. The fraudster(s) eventually suggested that she travel to Los Angeles to assist in convincing the bank to repay the funds. F.K. agreed to travel to Los Angeles, and paid for her flight and hotel herself.

143. On the evening of October 12, 2016, F.K. arrived in Los Angeles. Records from the DHS show that F.K. was wearing a blue jacket and a backpack with red straps when she arrived. (As discussed later, F.K. was wearing these same items in a photo sent by MANSBANGURA to IGBOKWE on October 13, 2016.)

144. F.K. further provided the following information during her interview.

a. F.K. stated that the day after she arrived, she met a woman purporting to be Coconspirator 7. She did not email or text the woman directly. Instead, Owen Blair would email her letting her know where and when to meet this woman. She said the woman took her to a Chase bank branch in Los Angeles to attempt to get the funds back, but that she was unable to understand much of what was happening because the conversation was in English.

b. When shown a photograph of Coconspirator 7 during the FBI interview, F.K. said that that was not the woman she met, because the photo of Coconspirator 7 showed a woman who was older than the woman she met. F.K. was also shown several images of MANSBANGURA, and she picked out one of the images as closely resembling the woman who picked her up from her hotel in Los Angeles. F.K. also had a clear recollection of the three children the woman had with her at one point, and, when shown a photo of MANSBANGURA with her three children, F.K. said she had a clear recollection that they were the children she met.

145. Evidence on IGBOKWE's Samsung indicates his and MANSBANGURA's involvement in defrauding F.K.

a. On October 13, 2016, the day after F.K. arrived in the U.S., IGBOKWE exchanged messages with Coconspirator 6, writing “Gv me her number so my woman will call her.” Coconspirator 6 responded, “Chheck bbm,” a reference to BlackBerry Messenger.

b. Later that day, MANSBANGURA sent IGBOKWE a message saying, “This is her.” The message attached a blurry photograph of F.K., wearing the same blue jacket and backpack discussed above. (F.K. positively identified the photograph as herself.) It is unclear where the photograph was taken, but it appears that it was covertly taken because F.K. was not aware that MANSBANGURA took her photograph. The message was followed by another message saying, “I just drop her off[.] I’m not doing this again.” MANSBANGURA then re-sent the same image.

c. In messages between January and March 2017, Coconspirator 6 asked for updates about the money received from F.K. On March 24, 2017, Coconspirator 6 asked about the “russia man” who “pull[ed] the money,” apparently referencing the explanation F.K. was given for why the funds were not available. Coconspirator 6 later said, “This bnk can not eat this moni . . . the moni most have been . . . Snt to someone.” He then provided IGBOKWE a photograph of the wire transfer from F.K. of \$33,128.26, which was a photograph that F.K. recognized in her FBI interview as one she took.

d. On March 27, 2017, IGBOKWE sent the wire transfer photograph to MANSBANGURA, and said “This is the slip for the 33k . chase bank have not issue the check till now.” MANSBANGURA responded, “Ok. I told u that I did Not WANT to deal with [Coconspirator 6] anymore. Cause after everything that happen [¶] I told u that when that ASIAN Lady came to the bank.” After further protestations from MANSBANGURA, IGBOKWE responded, in part, “Call them I need this money,” and MANSBANGURA agreed to do that.

6. J.G.—October 2016 Check Fraud Scheme (involving IGBOKWE and MANSBANGURA)

146. J.G. is an attorney from Nevada, who was the victim of a fraudulent check scheme in October 2016. In total, he lost approximately \$90,730, including \$30,000 wired on

October 26, 2016 to a US Bank account ending in 2669 belonging to Coconspirator 7, dba “M&F Enterprise.”

147. I interviewed J.G. in December 2017, and he also provided relevant documents. Based on that information, I know the following:

a. On October 13, 2016, J.G was contacted via email by a potential client using the name “Frank Moss” (“Moss”). Moss claimed to have a construction company in Omaha, Nebraska and asked J.G to assist him with the purchase of equipment costing \$120,000. To purchase the equipment, Moss needed J.G to make a \$30,000 deposit, a second payment of \$78,000, and a final payment for the remaining balance upon delivery of the equipment. Moss told J.G he did not want to send the funds directly to the seller and wanted a law office to send the funds until the completion of the purchase. Moss would notify J.G once the equipment was inspected and direct him on where to send the funds.

b. The first check J.G received from Moss was for approximately \$30,750. When J.G deposited the funds into his business bank account at Heritage Bank of Nevada, the bank put a hold on the check until they could verify the funds, because the check appeared to come from a Canadian Bank. At the time, there were checks coming into J.G’s bank account for over \$100,000 for unrelated business matters related to his law firm. Since J.G had funds available in the account, he moved forward with conducting the wire transfer for Moss. Per Moss’ direction, on October 26, 2016, J.G. wired \$30,000 to the US Bank account ending in 2669 in the name “M&F Enterprise.”

148. Bank records show that at the time of J.G’s wire, the US Bank account ending in 2669 had a balance of approximately -\$404.24. After the wire was deposited in the account, it was withdrawn through a series of cash withdrawals, checks, and debit card purchases, including the following checks: \$5,500 to MANSBANGURA on October 27, 2016; \$7,580.00 to Coconspirator 8 on October 27, 2016; \$8,845.00 to Coconspirator 8 on October 28, 2016; and \$7,500 to MANSBANGURA on October 31, 2016.

149. In addition to the fact that Coconspirator 7 was MANSBANGURA's relative, evidence on IGBOKWE's phones indicates that IGBOKWE and MANSBANGURA controlled the US Bank account ending in 2669 in the name "M&F Enterprise," and that MANSBANGURA used it at IGBOKWE's direction.

a. For example, data in IGBOKWE's iPhone 6S indicates that, on January 16, 2017, IGBOKWE sent MANSBANGURA a message related to another scheme that a coconspirator appeared to have sent to a fraud victim containing that bank account information.

b. Other messages on IGBOKWE's Samsung indicate that he sent the US Bank account ending in 2669 to multiple coconspirators between December 10, 2016 and January 2, 2017. For example, on December 10, 2016, IGBOKWE sent a coconspirator a message containing the account information in response to his request for a "US aza" for "mugu . . . small money 2600"—meaning, a U.S. bank account for a small payment of \$2,600 from a fraud victim.

7. Victim Company 3—December 2016 BEC Fraud (involving IGBOKWE and MANSBANGURA)

150. Victim Company 3, which is located in Oklahoma, was the victim of a BEC fraud in which it sent a wire for \$18,457.13 on December 19, 2016 from its Chase bank account to the US Bank account ending in 2982 of Coconspirator 8. Evidence discussed below indicates that IGBOKWE and MANSBANGURA used and controlled that account.

151. SA Miguel Luna interviewed an employee of Victim Company 3 in January 2018, and she provided relevant documents, including copies of emails with the unknown fraudster(s). Based on my conversation with SA Luna, his report of the interview, and documents provided, I know the following:

a. Victim Company 3, a small company that primarily provided landscaping services, had been attempting to purchase a piece of equipment from another company. On December 16, 2016, a contract employee of that other company sent the Victim Company 3 employee wiring instructions to make the payment for \$18,457.13 to a bank account ending in

8086 in Los Angeles. The next day, a fraudster purporting to be an employee of the equipment supplier sent new wiring instructions listing the US Bank account ending in 2982.

152. US Bank records show that the wire from Victim Company 3's Chase bank account entered the US Bank account ending in 2982 on December 19, 2016. The balance of the account was approximately -\$408.51 at the time the wire arrived in the account. Subsequently, there were two cash withdrawals of \$300 and \$500 from ATMs on December 20, 2016, and \$8,500 was withdrawn from the teller at a bank branch on the same day. On December 27, 2016, US Bank sent the remaining balance of the account—\$7,545—back to Chase following Victim Company 3's wire recall.

153. The recall of the funds from the US Bank account coincided with a lengthy conversation between MANSBANGURA and IGBOKWE about which of their accounts were still "strong" and which were "under review." During that conversation, MANSBANGURA told IGBOKWE, "FYI chase close [Coconspirator 7] account [¶] So pls do not use." She also told him, "[Coconspirator 8] us bank is under account review [¶] FYI [¶] So for now use [Coconspirator 7] us bank, [Coconspirator 8] well Fargo, [Coconspirator 8] cities bank (\$50k or less\$)." On the same day using a different phone number, MANSBANGURA also sent IGBOKWE messages saying, "Pls do not used [Coconspirator 8] us bank [¶] For any transaction [¶] If u put money there [¶] It will get stuck [¶] Never come out . . . There is a Restriction on d account."

154. Messages on IGBOKWE's phones indicate that he also provided the US Bank account ending in 2982 to other coconspirators who were middle-men to fraudsters, or themselves romance scammers, on several occasions between November 21, 2016 and March 1, 2017.

8. B.Z.—March 2017 Elder Fraud Victim (involving IRO, IGBOKWE, and MANSBANGURA)

155. B.Z. is an 86-year old man with dementia and Alzheimer's who was victimized in a variety of fraud schemes. Among those was a wire for \$11,900 to a Chase account ending in 7605 on March 16, 2017, opened by Coconspirator 7 dba "T and F Enterprises."

156. In November 2017, I interviewed B.Z. and his son, N.Z., separately, and learned the following:

a. During his interview, B.Z. appeared delusional and believed his payments were legitimate investments. For example, B.Z. believed he was communicating with former Federal Reserve Chairman Ben Bernake and current U.S. Treasury Secretary Steven Mnuchin, and he expected to receive \$107 million for his investment. He did not recall the payment to the Chase account ending in 7605 but believed it could have been related to his business deal with Ben Bernake.

b. N.Z. expressed concern for his father's mental and financial wellbeing, noting that B.Z. had lost tens of thousands of dollars to fraudsters due to his dementia and Alzheimer's. For example, N.Z. stated that after B.Z.'s wife died in November 2013, he started using online dating websites and met a 37-year old Ghanaian woman to whom he paid approximately \$100,000 for the purchase of an apartment complex. After the woman purportedly was kidnapped and shot at the airport as she was bringing a gold bar to him, B.Z.'s family had to talk him out of going to Ghana to meet her.

157. Bank records confirm the wire transfer from B.Z.'s Chemical Bank account to the Chase account ending in 7605 of Coconspirator 7. After the funds were deposited into the account, they were largely withdrawn through cash withdrawals and small debit card purchases, including numerous purchases at Rebtel Luxembourg, a prepaid phone card provider (which evidence indicates MANSBANGURA used). Additionally, on March 27, 2017, a \$4,000 check was paid to Santo Tomas, LLC for "Rent." Evidence (including evidence obtained by Wells Fargo during their investigation of the later-discussed fraud of Victim Company 5) indicates that

this was MANSBANGURA's rent payment, as MANSBANGURA lived at 4525 Santo Tomas Drive, in Los Angeles, California.

158. Evidence from IGBOKWE's Samsung indicates that Coconspirator 9 was the fraudster or middle-man to the fraudster, and that IGBOKWE coordinated with Coconspirator 9 regarding the incoming wire and subsequent laundering. MANSBANGURA assisted IGBOKWE in receiving and laundering the funds, while IRO assisted in getting payment to Nigeria.

a. On February 24, 2017, IGBOKWE provided Coconspirator 9 with the account information for the Chase account ending in 7605. On March 14, 2017, Coconspirator 9 told IGBOKWE that he wanted to use the account, and on March 16, 2017 told IGBOKWE that "11850" would be wired to the account. Later that day, Coconspirator 9 sent IGBOKWE a photograph of a computer screen showing a wire application and agreement from B.Z.'s Chemical Bank account to the Chase account ending in 7605.

b. For the next two weeks, IGBOKWE and Coconspirator 9 discussed getting the funds out of the account and providing payment to Coconspirator 9 in naira, with IGBOKWE providing occasional updates. For example, on March 22, 2017, IGBOKWE sent Coconspirator 9 a screenshot of a Chase banking application showing that the payment of \$11,900 was pending in the account. Later that day, IGBOKWE sent Coconspirator 9 screenshots of his messaging conversation with MANSBANGURA, in which she described issues getting the money out of the bank account. In the conversation with MANSBANGURA, IGBOKWE stated, "This guy is chika's friend and my friend too [¶] This is his first time of bringing business to me."

c. On March 24, 2017, IGBOKWE told Coconspirator 9 that the money was "out" and they then discussed IGBOKWE transferring funds to Coconspirator 9's Nigerian bank account. On April 6, 2017, IGBOKWE provided that Nigerian bank account information to IRO—telling him "Please 1m now" (referring to 1 million naira). IRO then provided it to

Coconspirator 10, a relative of IRO living in Nigeria whom he instructed to complete the payment.<sup>22</sup>

9. Victim Company 4—March 2017 BEC Fraud (involving IGBOKWE, UMEJESI, and OJIMBA)

159. Victim Company 4, a Colombian company that imports grains, was the victim of a BEC fraud on March 29, 2017. Victim Company 4 believed it was making a payment of \$29,679.17 to a company based in Michigan (the “Michigan Company”) that sold dry food products. Victim Company 4 personnel believed they were communicating with Michigan Company personnel, but they were in fact communicating with a fraudster who had hacked the Michigan Company’s email account and was forwarding the communications to another email address. The fraudster was then communicating with Victim Company 4 and the Michigan Company using spoofed email accounts (see n.1 for discussion about spoofing accounts).

160. SA Luna and I, respectively, interviewed personnel from Victim Company 4 and the Michigan Company. We received relevant documents from each of them related to the fraud. Based on this information, I know that on March 21, 2017, a fraudster posing as a Michigan Company employee sent Victim Company 4 an email requesting payment of \$29,679.17 to a Wells Fargo bank account ending in 7245, under the name of the Michigan Company, in Whittier, California. Bank records indicate that that account was, in fact, opened by Coconspirator 25, a money mule, dba “Danisha Beauty Sales,” on January 5, 2017. (Evidence indicates that Coconspirator 25 was coordinating with UMEJESI.) Victim Company 4 paid the wire on March 29, 2017.

161. Bank records indicate that the balance in the Wells Fargo account ending in 7245 of Coconspirator 25, dba “Danisha Beauty Sales” was \$3.60, and that on the same day the wire arrived in the account the account was used to make a purchase of \$1,419.73 at a Best Buy in Hawthorne, California and a \$300 cash withdrawal. On March 31, 2017 an additional wire

---

<sup>22</sup> Before IGBOKWE provided the Nigerian bank account information to IRO, there was an message from +12134258827, another number used by IGBOKWE, to IRO on the same morning containing the account information.

arrived in the account—\$27,464.89, from what appears to be a South American tour company (a likely BEC victim)—making the total in the bank account approximately \$55,411.93. On that same day, \$200 was withdrawn as cash, and two checks were issued: the first to UMEJESI for \$11,160, and the second to “Ojimba Collins” (i.e., OJIMBA) for \$16,520. (As discussed later in this section, photographs that UMEJESI sent to IGBOKWE show that these checks were deposited into two different Chase accounts.) Account records indicate that \$4,000 was withdrawn in cash on April 1, 2017, and then Wells Fargo withdrew the remaining \$23,531 in the account on April 20, 2017.

162. Evidence in the phones indicates that IGBOKWE coordinated with UMEJESI to receive and launder the funds fraudulently-obtained from Victim Company 4, while OJIMBA also had a role in the laundering.

a. On March 27, 2017, in a conversation on IGBOKWE’s iPhone 7 Plus, UMEJESI sent IGBOKWE the account information for the Wells Fargo account ending in 7245, saying, “Prefer make u use this one because the money wey dey enter too much.” On March 29, 2017, IGBOKWE sent UMEJESI a screenshot of a wire transfer confirmation from Victim Company 4 for \$29,679.17.

b. On March 29, 2017, after IGBOKWE sent the screenshot of the wire receipt to UMEJESI, UMEJESI appeared to send it to IRO. While only a thumbnail of the image was available from IRO’s Samsung, the small image appears consistent with the image IGBOKWE sent, and the context of UMEJESI’s conversation with IRO suggested it was the same image. IRO expressed confusion at seeing the receipt, asking “Who gave you this slip [¶] Tell me his name.” In response, UMEJESI said it was “Kudon,” which I have observed is a nickname used by IGBOKWE. UMEJESI said, “Because I gave him this ulo ako [i.e., bank account] 4months ago and I’m surprised him sending me this.” IRO responded, “I’m surprised . . . Let me call my contact because I have already told him it came in.” The next day, IRO said, “Mine is 29175 and 26.” From this conversation, it appears that UMEJESI was not expecting

funds from IGBOKWE to enter the account, but was instead expecting IRO to send funds fraudulently-obtained from a different victim to the account.<sup>23</sup>

c. On March 30, 2017, UMEJESI sent IGBOKWE messages saying, “Almost close to Bank . . . I been dey wait for the girl to dress up,” indicating that he was going to the bank with Coconspirator 25. He later sent IGBOKWE apparent username and password information of her for online access to the Wells Fargo bank account ending in 7245. A minute later, he sent a screenshot of a Wells Fargo banking application for the account ending in 7245, showing a balance of \$27,947.04. UMEJESI also sent Coconspirator 25’s name, and sent IGBOKWE two photographs of deposit slips into Chase accounts. The first was a deposit of \$11,160 into a Chase account ending in 7290, while the second was a deposit of a check addressed to “Ojimba Collins” into a Chase account ending in 1767. (Both of these deposits correlate to the checks written to UMEJESI and OJIMBA, shown in the bank records for this account.)

d. On April 1, 2017, IGBOKWE sent UMEJESI messages calculating the cut they would receive for their laundering services, saying, “Our money is 11,840[.] there own money is 17,760 [¶] 29,600% [sic]\*40 = 11,840.”

10. Victim Company 5—April and June 2017 Attempted Bank Account Takeover (involving IRO, IGBOKWE, and MANSBANGURA)

163. I interviewed the CEO and President of Victim Company 5, the Vice President and General Counsel of Victim Company 5, and a Senior Investigator from Wells Fargo about the fraudulent scheme that attempted to victimize Victim Company 5. Based on those interviews, and the documents they provided, I know the following:

---

<sup>23</sup> UMEJESI provided the Wells Fargo account ending in 7245 to both IRO and IGBOKWE, and IGBOKWE provided it to a number of coconspirators to use. Based on information in IGBOKWE’s Samsung, he provided the account to five coconspirators between January 18 and March 16, 2017, including to Coconspirator 5. IRO provided it to a coconspirator on March 17 and 21, 2017, after UMEJESI provided it to IRO on March 17, 2017. There is no record of when UMEJESI provided the account to IGBOKWE beside on March 27, 2017, but based on the fraud involving Victim Company 4 and UMEJESI’s statement to IRO it appears that it was before January 18, 2017, when IGBOKWE provided it to Coconspirator 5. MEGWA also sent this account information to IGBOKWE on January 25, 2017, indicating a connection between him and UMEJESI.

a. On April 4, 2017, Wells Fargo received a request, dated March 29, 2017, purporting to be from Victim Company 5 to close Victim Company 5's account at Wells Fargo and transfer the remaining balance to a fraudulent account at Chase ending in 5027 in the name of Victim Company 5. The package included a purportedly notarized letter and forged signature of the CEO of Victim Company 5. Bank records show that the balance of Victim Company 5's Wells Fargo account was approximately \$17,300,844.58 at the time. At approximately that time, a fraudster called Wells Fargo asking about the closure of the Victim Company 5 account.

b. On June 5, 2017, Wells Fargo received a second fraudulent request, via U.S. Mail, dated June 1, 2017, to close the legitimate account of Victim Company 5. (Based on U.S. Mail tracking information, the package was mailed from Burbank, California.) The second request also directed payment to the fraudulent account at Chase ending in 5027 in the name of Victim Company 5. Bank records show that the balance of Victim Company 5's legitimate Wells Fargo account was approximately \$12,760,922.93 around that time.

164. Bank records show that the fraudulent Chase account ending in 5027 was opened by Coconspirator 7, with a business name similar to that of Victim Company 5.

165. Evidence on the phones seized indicates the involvement of IRO, IGBOKWE, and MANSBANGURA in the scheme to defraud Victim Company 5 of its money in the possession of Wells Fargo.

a. A message (which had been deleted) sent to IGBOKWE's iPhone 7 Plus on February 17, 2017, by IRO stated "Give your wife this name to take [Coconspirator 7] so they can open it today. [Victim Company 5]."

b. After receiving the message from IRO, IGBOKWE copied and sent the same message to MANSBANGURA from his iPhone 7 Plus on February 17, 2017.

c. On February 21, 2017, IGBOKWE sent IRO a message saying "Send me the name" and IRO responded with the name of Victim Company 5. IGBOKWE then replied "Hv send it." The same day, IGBOKWE again sent the name of Victim Company 5 to MANSBANGURA.

d. L.A. County records show that Coconspirator 7 filed a fictitious business name statement in a name similar to that of Victim Company 5 on February 22, 2017. Bank records show that Coconspirator 7 then opened a fraudulent Chase account ending in 5027 on February 22, 2017.

e. About a month later, on March 20, 2017, IGBOKWE sent the account information for the fraudulent Chase account ending in 5027 to IRO.

f. The following day, IRO sent the account information to two coconspirators for use in “dating” transactions. And, on March 22, 2017, he sent the account information to another coconspirator who requested an “open bene” account. On March 27, 2017, IRO also sent the account information to OGUNGBE in response to a request for an “aza for 3m\$ . . . from Philippines today.”

*g. Both of the attempted account takeovers were unsuccessful because the bank never initiated the wires.*

11. A.V.—April and May 2017 Elder Fraud Victim (involving IGBOKWE and MANSBANGURA)  
166. In March 2019, I interviewed victim A.V. and an attorney appointed as the guardian of property for A.V. and her husband. Based on those interviews, documents provided by the attorney, and bank records, I know the following:

a. A.V., an 87-year old woman whose property is now under the guardianship of a county Department of Health and Human Services, lost \$555,013.26 to fraud schemes in less than a year, and by her own account lost at least \$75,000 more prior to that. Her payments to the fraudsters included two wires of \$8,035 to the Wells Fargo account ending in 1147 of Coconspirator 12, a relative of IGBOKWE, and two wires totaling \$6,060 to the Chase account ending in 5027 of Coconspirator 7. Specifically, the wires to the Wells Fargo account were dated April 10 and 11, 2017; the first wire to the Chase account was for \$1,700 on April 27, 2017; and the other wire to the Chase account was for \$3,360 on May 1, 2017. All of those payments came from A.V.’s Capital One bank account.

b. It was apparent from the interview of A.V. that she was confused and possibly suffering from dementia or some other form of mental decline. A.V. said during the

interview that she did not have any financial data available and had been in the process of shredding it, but that she recalled making the two wires from her Capital One account to the Chase account of Coconspirator 7. She said that she made the payments for a first cousin who had gotten married and moved to Thailand. A.V. also stated that a lawyer had been assigned to take care of her finances.

c. In addition to providing documents relating to A.V.'s bank accounts and guardianship, her attorney confirmed that both A.V. and her husband suffered from dementia-related illnesses. The attorney believed that A.V. had lost roughly \$600,000 to \$700,000 to fraud, primarily to online scams, and the attorney further observed that A.V. was extremely vulnerable to financial scams.

167. Between April 11 and June 2, 2017, IGBOKWE and Coconspirator 11 exchanged numerous messages about A.V. The messages indicated that A.V. was a victim of a fraudulent scheme, and discussed payments into bank accounts controlled by IGBOKWE and MANSBANGURA—specifically, the Chase account ending in 5027 of Coconspirator 7; and the Wells Fargo account ending in 1147, opened by IGBOKWE's relative, Coconspirator 12. The exchanges between Coconspirator 11 and IGBOKWE included a PDF and photographs of multiple wires sent by A.V.

a. For example, on April 11, 2017, Coconspirator 11 provided IGBOKWE with a PDF of an outgoing wire funds transfer from the Capital One bank account of A.V., ending in 4290, to the bank account of IGBOKWE's relative, Coconspirator 12, ending in 1147. The wire transfer of \$8,035 took place on April 11, 2017.

b. On April 17, 2017, IGBOKWE provided Coconspirator 11 with account information for a BOA account ending in 3037, opened in the name of Coconspirator 12. Coconspirator 11 responded, "Giv another without Nija [i.e., Nigerian] name." IGBOKWE then sent another account—the Chase account ending in 5027, opened by Coconspirator 7, in the name of Victim Company 5. Coconspirator 11 responded, "Can this be used f Ali?" IGBOKWE responded, "No." Coconspirator then 11 inquired "Just client[?]," to which IGBOKWE replied

“If u need aza for Ali let me know. [¶] Yes[.]” (As noted earlier, “ali” was code for “BEC,” while “client” referred to an individual fraud victim, such as a romance scam victim.)

c. Also of note, on May 8, 2017, IGBOKWE sent Coconspirator 11 screenshots of a messaging conversation with MANSBANGURA discussing the “\$3360” and “1800,” in which MANSBANGURA starting by saying, “Fyi the money was NOT CLEAR ON the first.” In that conversation, MANSBANGURA asked IGBOKWE not to “use [Coconspirator 7] BUSINESS account for any transactions from Capital one anymore.” After IGBOKWE asked what happened, she continued, “Chase said that they will force (meaning = RETURNED) the money back to sender. Ounce it posted. Chase put a hard [¶] Hold on it because they want to make sure it NOT A FRAUD money.” MANSBANGURA then went on to discuss how Chase said that Capital One transactions have caused “lots of issues with them,” so she told IGBOKWE, “No more CAPITAL one TRANSACTIONS.” (Note: This paragraph reflects the capitalization used by MANSBANGURA.)

d. Additionally, on June 2, 2017, Coconspirator 11 sent IGBOKWE a voicemail from A.V. for “Mr. Davis,” where A.V. was reporting to “Mr. Davis” about her conversation with her Chase banker about why some of the money that she sent did not go through, and telling “Mr. Davis” that “Mr. Randall” should have the money. Later that day, IGBOKWE sent Coconspirator 11 an audio recording from MANSBANGURA of her own call to Chase where she asked about the \$3,360 that was deposited to the account which she had previously asked to be sent back to the remitter.<sup>24</sup> (Thus, MANSBANGURA was pretending to be Coconspirator 7 during this call, as the account was opened by Coconspirator 7 and bank records do not indicate that MANSBANGURA was listed as an authorized user of the account.)

---

<sup>24</sup> Although both MANSBANGURA and the Chase employee referred to the transaction as occurring on “March 1,” it appears that they were both referring to the wire of \$3,360 from A.V. on May 1, 2017, because they discussed how the transaction was for \$3,360, and IGBOKWE’s conversations with Coconspirator 11 about transactions do not appear to have begun until April 2017. Thus, it appears the reason IGBOKWE forwarded that message to Coconspirator 11 was that it pertained to A.V.

12. Victims Je.F. and Jo.F.—April 2017 Escrow Fraud (involving IRO and EKECHUKWU)

168. I interviewed victim Je.F. and an employee of an escrow company in February 2018, and reviewed documents provided by them. Based on that, I know the following:

a. In April 2017, Je.F. and Jo.F. (collectively, the “F Family”), who lived in Illinois, were purchasing land in Texas. Unbeknownst to the F Family and the escrow company, their email traffic was being intercepted by an unknown fraudster(s). It is unclear where the compromise occurred, but it is clear that the unknown fraudster(s) was intercepting emails between the parties and then sending copies of the emails from fraudulent email accounts, so that the fraudster(s) could provide the F Family with fraudulent wire transfer information. The fraudster(s) communicated with F Family using a mail.com address designed to imitate an escrow company employee’s real email account, while also communicating with the escrow company employee using a mail.com email account that closely mimicked Je.F.’s real Gmail email account.

b. On April 9, 2017, a fraudster sent Je.F. instructions to wire payment to the Chase account ending in 6217, which was opened by a money mule in Los Angeles, in coordination with EKECHUKWU, at the request of IRO. (CATHEY earlier assisted in opening a similarly-named account in Georgia for IRO in early-April 2017, which account information IRO subsequently sent to multiple coconspirators.)

c. On April 17, 2017, Je.F. ordered a wire transfer of \$135,800.72 to the Chase account ending in 6217. Je.F discovered the fraud the next evening, after the title agent called to say she had not received the wire and then resent the closing documents (including the wire instructions) to a different email account of Je.F. The next day, Jo.F. requested a wire recall through the F Family’s bank.

169. Evidence on the phones indicates that IRO was interacting with Coconspirator 13 and Coconspirator 14, while EKECHUKWU coordinated with the money mule.

a. On April 18, 2017, EKECHUKWU asked IRO “anything coming in the warehouse[?]” (As noted above, “warehouse” is one of the ways some of the coconspirators sometimes referred to a bank or bank account.) After some back and forth, IRO provided EKECHUKWU with the account information for the Chase account ending in 6217, saying, “Check this. Something is inside,” on April 19, 2017.

b. On April 19, 2017, EKECHUKWU and IRO discussed checking the account, with EKECHUKWU telling IRO that “He said he will check when he get off work that money alerts.” EKECHUKWU then provided the name of the money mule and his phone number, which is the same phone number listed on bank records for the account, and said, “Trying to be rude and smart.” Later that day, IRO stated, “This your guy is something else [¶] Smh [¶] Money enter....now he’s telling me he wants to send it back . . . 135800.” Later that day and also on April 20, 2017, IRO and EKECHUKWU further discussed how the money mule was being uncooperative, with IRO saying, “I don’t know what to tell the owners” (i.e., the fraudsters responsible for the F Family fraud).

c. Evidence on IRO’s Samsung phone further indicates that Coconspirator 13 and Coconspirator 14 were involved in defrauding the F Family.

13. Victim Company 6—April 2017 BEC Fraud (involving IRO and CATHEY)

170. In February 2018, I interviewed personnel from Victim Company 6. Based on that and documents provided by them, I know the following:

a. Victim Company 6, based in Wisconsin, manufactured products for commercial use and was purchasing products from a company based in China (“Chinese Company 2”). During April 2017, Victim Company 6 had a \$2.5 million project with Chinese Company 2, and intended to make a payment of \$900,000 as part of that deal. Unbeknownst to either party, Chinese Company 2’s email system had been hacked, and fraudsters were blocking Chinese Company 2’s emails and communicating independently with each party. The fraudsters

appear to have used Chinese Company 2's legitimate email address and accounts with similar domain names to communicate with Victim Company 6.

b. On April 12, 2017, the Accounts Payable Specialist for Victim Company 6 received wire instructions from Chinese Company 2's legitimate email address, but which directed Victim Company 6 to make a payment to a PNC Bank account ending in 7988 opened by Coconspirator 16, dba "Chinese Company 2," in Georgia. On April 18, 2017, Victim Company 6 completed a wire of \$900,000 to the fraudulent PNC Bank account, and sent a wire confirmation page to Chinese Company 2, as was the standard practice. The fraud was discovered soon thereafter, and the funds were ultimately returned to Victim Company 6.

171. Evidence on the phones indicates that Coconspirator 15 was the middle-man for the hackers communicating with Victim Company 6 and Chinese Company 2. IRO was Coconspirator 15's primary point of contact with the conspiracy, and CATHEY worked with Coconspirator 16 to open the fraudulent account. IRO and UMEJESI also discussed the fraud. Evidence further indicates that IKOGHO was going to be involved in the laundering, if the funds were successfully withdrawn.

a. On April 10, 2017, Coconspirator 15 sent messages to IRO saying, "900k usd [¶] Very urgent [¶] [Chinese Company 2] [¶] If e go dey possible in next 24hours." IRO agreed to open the bank account.

b. A few minutes later, IRO sent messages to UMEJESI saying, "[Chinese Company 2] [¶] Do this today. . . ." But then about ten minutes later IRO said, "Never mind," and sent messages to CATHEY saying, "[Chinese Company 2] [¶] Do this today or tomorrow. It's usa going to china." CATHEY responded, "Hey bro I'm on it."

c. On April 12, 2017, CATHEY sent IRO a message containing the account information for the account at PNC Bank ending in 7988, opened in a name similar to that of Chinese Company 2.

d. On April 13, 2017, IRO told CATHEY, "[Chinese Company 2] has confirmed and payment is tomorrow as we wake up," and later that day repeated, "The [Chinese

Company 2] confirmed too. Payment today.” IRO also sent CATHEY a screenshot of an email from a Victim Company 6 employee to Chinese Company 2 confirming that there would be “payment of \$900,000 wire on Monday.”

e. On April 17, 2017, Coconspirator 15 told IRO he had received the “invoice.” IRO then told CATHEY, “900 is happening tomorrow . . . in the one you opened,” and sent CATHEY another screenshot of an email from the Victim Company 6 employee to personnel of Chinese Company 2. CATHEY asked, “do you have details on the 900 so I can call,” and IRO sent him a screenshot of the email from the Victim Company 6 employee confirming the payment would arrive Monday. IRO added, “[Victim Company 6] [¶] Country..usa [¶] State WI.”

f. On April 18, 2017, following the wire transfer of \$900,000 by Victim Company 6, IRO sent CATHEY a screenshot of the wire confirmation page from Victim Company 6, saying “Done [¶] Hahahaha.” CATHEY responded, in part, “Awesome!!!!!! [¶] Hell yes!!,” and confirmed that he would call the bank “right now” at IRO’s request.

g. On April 19, 2017, IRO and CATHEY discussed information about Victim Company 6 and Chinese Company 2’s line of business. IRO asked, “Everything good?” CATHEY responded, “Yessiree everything is getting handled.” During that conversation, CATHEY told IRO that he flew to Atlanta the previous night “[i]n order to get this transfer done right.” Based on PNC bank records, the account was opened by Coconspirator 16 using an address in Morrow, Georgia, near Atlanta.

h. Thereafter, IRO and CATHEY had a lengthy conversation in which CATHEY relayed to IRO that the bank was “calling company to verify” and asked, “Is it going to be ok[?]” IRO responded, “Yes [¶] Is fine [¶] Nothing is wrong on our side [¶] Damn small banks [¶] Everything is well. Don’t be scared.” Later in the conversation, IRO asked, “Please I hope your person dressed good,” and CATHEY responded, “Yes in slacks with dress shirt [¶] And tie.” CATHEY added later, “From now on after this only boa and chase with DMV id [¶] And I’m doing everything personally [¶] No more using people [¶] To stressful.”

i. On April 20, 2017, CATHEY said, “Bad news bro there sending the money back. But if u need me to open at chase I can asap.” IRO responded, “Damnn [¶] This is such a bad news [¶] Smh [¶] Please bro [¶] Get to this as soon as you get to la. Please[. ]” IRO later stated, “Bro. They have received the 900 back [¶] They asking for the new one to resend it.”

j. Later that evening, Coconspirator 15 asked IRO, “Abeg u done open the Aza,” roughly meaning “Please have you opened the bank account?” IRO let Coconspirator 15 know that they were trying to open one.

k. On April 21, 2017, CATHEY sent IRO an audio message in which he discussed not missing the “opportunity on the 900” and how he “gave [his] guy the instructions.” IRO responded with an audio message also discussing the transaction. IRO also passed CATHEY’s audio message to Coconspirator 15.

l. On April 24, 2017, IRO told CATHEY that the “That dude finally messed it up. The job cast. The 900.” (As noted, the word “cast” was used to indicate that fraud had been detected and/or that the bank account had been frozen.) They went on to discuss and commiserate, with CATHEY adding, “This is totally my fault I will make it up . . . It’s getting done as we speak.” IRO responded, “It’s okay blooda [¶] No problem [¶] Send me the slip when you are done.” Later that day, CATHEY sent IRO account information for a Chase account opened in Los Angeles. IRO responded, in part, “Will keep it in file.”

i. The account that CATHEY opened was the Chase account ending in 5899, which was opened with the business name of Chinese Company 2. That account that was used in the fraud involving the Victim Law Firm (see Section III.H.18).

14. Victim Company 7 and Victim Company 8—April 2017 BEC Fraud (involving IRO)

172. I interviewed the owner of Victim Company 7 in April 2018 and SA Luna interviewed the owner of Victim Company 8 in May 2018. Based on those interviews and documents provided by the owner of Victim Company 7, I know the following:

a. Victim Company 7, based in Charlotte, North Carolina, was a victim of a BEC scheme in April 2017. Victim Company 7 was attempting to pay its manufacturer, Victim Company 8, for an order, but instead was induced on April 21, 2017 to direct a wire transfer of \$23,789 to the Chase account ending in 7866 of Coconspirator 26, which was used and controlled by IRO. Evidence indicates that Victim Company 8's email was hacked. Victim Company 7 lost all the money, but received a shipment from Victim Company 8. After the fraud was discovered, Victim Company 7 refused to pay Victim Company 8 for the product, leaving Victim Company 8 to shoulder the loss.

b. Victim Company 8 separately lost approximately \$24,000 in another BEC fraud around the same time.

c. The owner of Victim Company 8 almost went bankrupt as a result of the intrusion and payments. In total, he lost approximately \$47,000, and experienced emotional trauma and difficulty sleeping as a result of the stress he experienced.

173. Bank records indicate that at the time the funds from Victim Company 7 entered the Chase account ending in 7866 of Coconspirator 26, the balance in the account was \$129.07. After the wire from Victim Company 7 arrived, \$2,700 was transferred the same day, April 21, 2017, to the Chase savings account ending in 9927 of Coconspirator 26. On April 24, 2017, \$18,598 was wired to the SunTrust account of "B&B Motors of Tampa Bay Inc." with the note "This payment is for car purchase of Mr. Brown's; Payment For Mr Brown's Car Buy," and an additional \$500 was withdrawn as cash at an ATM near IRO's apartment. On April 25, 2017, most of the remaining funds were sent in a \$1,450 wire to a US Bank account.

174. IRO's Samsung contained evidence indicating his use and control of the Chase account ending in 7688 of Coconspirator 26

a. IRO sent the account information for the account to ten coconspirators between April 5 and 16, 2017. In multiple conversations, he emphasized that the account should be used for "dating," or that if it was not then the coconspirator using the account should expect

not to receive any of the money deposited into the account (implying that IRO himself would keep the funds).

b. Other evidence indicates that IRO used Coconspirator 26's name and identification. On May 22, 2017, IRO sent AWAK photographs of a letter from Chase indicating that it was closing another account in Coconspirator 26's name, the savings account ending in 9927. He also sent AWAK photos of a bank statement for the account ending in 7688 (showing the transaction from Victim Company 7, among others) and a photo of a cashier's check, dated May 10, 2017, addressed to Coconspirator 26 for \$3,611.83 (which IRO indicated was the balance of the account that was closed). The address listed on both letters and the check was that of IRO's apartment.

175. Coconspirator 26 is a real person. Based on bank records, Coconspirator 26's Nigerian passport number was used to open the Chase account ending in 7866 on March 29, 2017. The same passport number was used to open a BOA account ending in 0305 in Coconspirator 26's name, on approximately June 28, 2017. Records for both bank accounts listed IRO's apartment as the address on file.<sup>25</sup> The Chase and BOA accounts were both provided by IRO to coconspirators.

15. D.J.—May 2017 Romance Scam Victim (involving IGBOKWE, MANSBANGURA, and DURU)

176. D.J., who lives in Minnesota, is a 64-year-old divorcee who was the victim of a romance scam. In total, she lost approximately \$45,000 to the scam. Among the fraudulent transactions was one bank money order for \$25,600 that she deposited on May 5, 2017 in Marshall, Minnesota to the Wells Fargo account ending in 4899 of DURU, dba "PD Enterprise."

177. I interviewed D.J. in September 2018. Based on the interview, documents she provided, and bank records, I know the following:

---

<sup>25</sup> Immigration records indicate that Coconspirator 26 arrived in the U.S. at LAX on March 8, 2017, left the U.S. from LAX on April 5, 2017, came back to the U.S. via LAX on June 5, 2017, and then left again on June 29, 2017, the day after the BOA account was created.

a. In April 2017, D.J. met a person using the name “Anthony Haugen Featherstone” (“Featherstone”) on eHarmony. They started an online romantic relationship, communicating by telephone and email. Featherstone had told D.J. that he worked for an architectural company but that he was going on a long work trip. While purportedly on his trip, he asked D.J. to sign into his bank account at “Chartered Standard Bank” to do a transfer for him, and provided D.J. his login information. When she logged in, she saw that he had lots of money in his account. But, after that, Featherstone told her that the bank had cut off his access because she had logged into his account. He then started asking D.J. for financial assistance while he was purportedly overseas.

b. D.J. sent money purportedly for Featherstone to a woman in El Paso, Texas, via Walmart money transfers. (She realized afterwards that that woman was also a victim of a scam.) D.J. was also induced to send several wires, totaling approximately \$22,400 to two accounts—one to an Indonesian bank and another purportedly destined for Indonesia for a project Featherstone claimed to be working on.

c. Finally, at Featherstone’s bidding, D.J. also borrowed approximately \$25,000 from her credit union against her truck (which was already paid off), and then purchased a money order of \$25,600 from her bank, United Southwest Bank, to PD Enterprise. She then deposited the money order at a Wells Fargo branch in Marshall, Minnesota on May 5, 2017, into the Wells Fargo account ending in 4899 of DURU, dba “PD Enterprise.”

d. At some point—after it appears from the evidence in the phones described below that the funds were frozen—Featherstone asked D.J. to report the transaction as fraud to ensure the money came back to her account. Bank records and records provided by D.J. show that the funds were re-credited to her bank account on May 19, 2017.

e. After speaking to her bank at my request, D.J. further stated that her bank informed her the funds were ultimately sent to a Wells Fargo Bank account in Tempe, Arizona.

178. Evidence on IGBOKWE’s Samsung and iPhone 7 indicates that Coconspirator 5 was a middle-man to the fraudster who victimized D.J., while DURU was the witting money

mule for the transaction. MANSBANGURA assisted DURU in registering “PD Enterprises” as a business with L.A. County, at IGBOKWE’s request.

a. Messages between IGBOKWE and DURU show that on January 19, 2017, DURU sent IGBOKWE his name and address, and the following: Company name: PD Enterprise Or Vibra Enterprise. [¶] What do you think about the company names?” IGBOKWE responded, “Is cool,” and then sent that information to MANSBANGURA.

b. On January 20, 2017, in the evening, MANSBANGURA sent IGBOKWE photographs of a confirmation number for an order with L.A. County and a screenshot from a phone showing an application for a fictitious business name statement in the name “PD Enterprise,” being submitted on behalf of “Duru Princewill.” IGBOKWE then forward those to DURU, who responded by correcting his name, stating, “Princewill Duru A.”

c. On April 7, 2017, IGBOKWE told DURU “try open wells [i.e., Wells Fargo account] every body needs it.” On April 11, 2017, DURU told IGBOKWE that he was at Wells Fargo and mentioned different accounts he could open. IGBOKWE responded, “Try open one there that can carry 200k up [¶] Or 500.”

d. Later that day, DURU sent IGBOKWE account information for the Wells Fargo account ending in 4899 in the name “PD Enterprises.” IGBOKWE sent the account to multiple coconspirators, including Coconspirator 5, to whom he sent it on April 24, 2017.

e. On May 3, 2017, Coconspirator 5 asked IGBOKWE to “Re confirm Wells Fargo” for “Dating 25k,” and sent IGBOKWE the account information for the Wells Fargo account ending in 4899, in the name PD Enterprise, which IGBOKWE had previously sent to him. IGBOKWE responded, “Make i give BOA [¶] This one is for ali,” but Coconspirator 5 responded, “The[y] like Wells Fargo.” IGBOKWE then said, “Serious ok” but provided the Wells Fargo account ending in 1147 of Coconspirator 12, saying, “Another one too for dating.”

f. On May 5, 2017 Coconspirator 5 sent IGBOKWE a photograph of a check deposit receipt showing \$25,600 was deposited into the Wells Fargo account ending in 4899, and then followed with the message, “25,600.” Coconspirator 5 and IGBOKWE then discussed the

exchange rate that IGBOKWE would provide, with IGBOKWE saying he would “call [his] exchanger.” This conversation continued into May 6, 2017, with Coconspirator 5 providing a Nigerian bank account information where he told IGBOKWE to deposit “7,272,000 naira.” (₦7,272,000 would have been approximately 75 percent of the \$25,600, reflecting that IGBOKWE and DURU were receiving approximately 25 percent for their roles.)

g. IGBOKWE sent the photograph of the receipt to DURU, on May 5, 2017, and asked if the money was pending in the account. DURU indicated it had not. On May 6, 2017, DURU asked, “The work na local? [¶] Because it shows that the fund was deposited in Minnesota, Minneapolis.” IGBOKWE responded, “Yes is deposit,” and explained, “Dating can come from anywhere.” DURU then asked, “Hope it’s safe though?,” and IGBOKWE replied, “Yes very safe.”

h. On May 7, 2017, Coconspirator 5 asked IGBOKWE when the money could be withdrawn from the account, asking, “25k can’t be pull at ones [sic: “once”]?” IGBOKWE responded, “No” and asked if he could call Coconspirator 5. On May 8, 2017, he told Coconspirator 5, “He will cash out today bro.”

i. On May 8, 2017, IGBOKWE told DURU, “U go bring cash out today,” and DURU responded, “Yea sure.” Later that day, DURU sent IGBOKWE the photograph of the deposit receipt that IGBOKWE had initially sent to him.

j. On May 9, 2017, DURU asked IGBOKWE for the name and basic information about the “client” for when he discussed the transaction with the bank. DURU later discussed how the bank told him that there was a “block” on the account, and that he was trying to “unblock it.” IGBOKWE responded, “Just hold on they will unlock it.”

k. After a series of calls between IGBOKWE and DURU on May 9 through 11, 2017, DURU explained that he would have to open a new BOA account, and sent account information for a BOA account ending in 8102 in the name “P Will Enterprises.” IGBOKWE let Coconspirator 5 know that DURU was “trying 2 change his business name,” and then later explained, “Will have change it to P will Enterprise.”

l. DURU later said to IGBOKWE, “Nwanne, after this one. I go dey collect normal Aza 20% for dating and 40% for Ali or any other work. I no go dey take all these risk to get only 10%. I’m not trying to be greedy at all, I’m just being very reasonable make I know say the risk is compensated to a level. I hope you understand where I’m coming from make we no misunderstand each other.” IGBOKWE responded, “Lol.” (In addition to indicating that this was not DURU’s only experience receiving and laundering fraudulent proceeds, this conversation also reflects that IGBOKWE was planning on keeping approximately 15 percent of the total amount, given that he and DURU were splitting approximately 25 percent, as noted above.)

m. On May 15, 2017, DURU sent IGBOKWE multiple messages explaining his conversations with Wells Fargo about getting the fraud hold lifted. Among those, DURU stated, “He advised me to call the fraud and loss prevention department for them to explain the situation to me because he can’t disclose it to me. If you can contact your guy and tell him to contact his client to talk to the bank to release the money, that would be helpful I guess. These whole thing is stressing me out and I’m spending money I’m not getting back. [¶] For him to tell me not to come to the bank without calling him first, I feel something must be really wrong. And I don’t want to take that chance. For now I’ll only communicate with them on the phone. [¶] Another thing is. I don’t know how they got my present address because I used my previous address for all the paper work when I was opening the account [¶] And he said getting the money in the account is not guaranteed depending on their investigation and findings. This is exactly what I’ve been avoiding [¶] Nwanne. This people dey ask me too many personal questions about the client, the check and what the money is meant for. And my relationship with the person and how long I’ve known her. And many questions o. All I’ve been getting is hold on. They transfer me from one person to the other. Now I’m on hold again.”

16. L.B.—May 2017 Romance Scam Victim (involving IRO, IGBOKWE, and AWAK)

179. L.B., who lives in Alabama, is a romance scam victim who made a payment of \$3,000 to IGBOKWE’s BOA account ending in 2660 on May 9, 2017. L.B. was 73 years old at the time of the fraud and lost more than \$46,700 in the scam. I interviewed L.B. in September 2017. Based on that interview, I know the following:

a. L.B. was a retired real estate agent. She met a person using the name “Brian Smith” (“Smith”) on Facebook in February 2017. Smith told her that he found her through mutual friends, and that he was project manager on an oil rig off the coast of Marina Del Rey, California. L.B. considered herself to be in a relationship with Smith, and considered herself to still be in that relationship at the time that I interviewed her. As a result, L.B. was initially somewhat disbelieving that she had been defrauded, but eventually called me back, saying she felt that Smith had manipulated her in every way he could.

b. At some point, Smith started asking L.B. for money to help finish a business project. L.B. believed she had lost more than \$46,700 to Smith in total. She recalled two transactions from her Wells Fargo bank account and two from a Regents Bank account.

180. Bank records indicate that one of the transfers—a payment of \$3,000 on May 9, 2017—went to IGBOKWE’s BOA account ending in 2660. There was approximately \$4,078.59 in the account at the time of the wire, and, during the following month, almost all of that money was spent down through retail purchases, cash withdrawals, and IGBOKWE’s lawful permanent resident (i.e., green card) application (\$1,225 on June 7, 2017). (U.S. Citizenship and Immigration Services has confirmed the payment.)

181. Evidence in the phones indicates that IRO, IGBOKWE, and AWAK were involved in victimizing L.B.

a. On May 3, 2017, after discussing another “dating” transaction, IRO told AWAK, “But make I give you house for the 3k,” i.e., that he would provide a bank account for an incoming payment of \$3,000. IRO then provided information related to a BOA account

ending in 2660 in the name “Christo Gunus C.”<sup>26</sup> In response, AWAK said, “Yes I go use this house.”

b. On May 4, 2017, AWAK told IRO, “For the 3k see the update,” and sent an image (which was not available on IRO’s phone). IRO responded, “Please tell them not to deposit any checks ageb [¶] No checks [¶] Please,” and AWAK replied, “yea no be check she go deposit. Later that day, AWAK sent another image. Although that image was not available on IRO’s phone, it appears based on the file name that IRO later sent the same image to IGBOKWE. The image, which was recovered from IGBOKWE’s iPhone 6S, was a photograph of a wire transfer request from L.B.’s Wells Fargo account to IGBOKWE’s BOA account ending in 2660. However, the name listed for the receiving account was simply “christo gunus,” similar to what IRO had provided it to AWAK, not IGBOKWE’s full name.

c. On May 7, 2017, IRO and AWAK discussed why it was that IRO had not sent a screenshot confirming that the transaction entered IGBOKWE’s account.

d. On May 9, 2017, AWAK complained to IRO about his customer service, saying, “Bro I no understand you [¶] You say you check account, money no dey you could have simply took a screenshot and send to me [¶] I no understand if screenshot na based on the amount [¶] You forget say who bring 3k job today can also bring 1m job [¶] Please do the needful. Check today again if nothing send me screenshot so the boy can know where to start tracing.” (emphasis added).

e. IRO and IGBOKWE then discussed IGBOKWE’s bank account, with IRO asking, “Anything show?” After IGBOKWE confirmed that nothing had appeared in the account, IRO said, “Please can you send me the screen let me show them abeg.” IGBOKWE then sent those screenshots to AWAK. IRO and AWAK discussed whether the name associated with the account was input incorrectly, and IRO provided the full account information to AWAK

---

<sup>26</sup> BOA records indicate that the account ending in 2660 was opened in the name “Christogunus C. Igbokwe,” rather than the name listed above. Additionally, the name “Christogunus C. Igbokwe” inverts IGBOKWE’s first and middle names.

again and also clarified that the full name associated with the account was “Christogunus C Igbokwe,” a variation of IGBOKWE’s name

f. Later that day, AWAK told IRO that L.B. was at the bank trying to make the transfer: “She dey bank right now [¶] The bank don resend with the new name [¶] So you should receive this time.”

g. On May 13, 2017, AWAK and IRO discussed how IRO would pay AWAK. IRO ultimately asked his relative, Coconspirator 10, who was in Nigeria, to pay 742,500 naira to AWAK’s bank account.

17. Victim Company 9—April 2017 BEC Fraud (involving IRO, IGBOKWE, IKOGHO, UMEJESI, OGUNGBE, and UZOKA)

182. Victim Company 9 is a large food and beverage distributor in a Caribbean nation. In April and May 2017, employees of Victim Company 9 communicated with an employee of a supplier based in Barbados (“Caribbean Company 1”). Unbeknownst to Victim Company 9, the Caribbean Company 1 employee’s email had been hacked, and Victim Company 9 exchanged numerous emails with the fraudster, ultimately sending a wire of \$220,337.68 to an account at BOA ending in 1004, which was opened by a money mule (“Coconspirator 17”), using the business name “Kuft SA.” Victim Company 9 did not recover any portion of that wire.

183. I interviewed the CEO of the parent company of Victim Company 9 in August 2017. Based on that interview and documents he provided, including relevant emails and an internal audit report, I know the following:

a. In April and May 2017, personnel from Victim Company 9 exchanged emails with a Caribbean Company 1 employee about a payment of \$220,462.68 for a series of orders. It was only discovered long after the fact—on May 18, 2017—that the Caribbean Company 1 employee was on vacation for a portion of the time and that her email had been hacked and blocked. The hacker had continued to send emails to Victim Company 9 from the Caribbean Company 1 employee’s email account, apparently blocking her from receiving them

or seeing emails sent by the hacker. Based on what Caribbean Company 1 told Victim Company 9, the last legitimate email from the Caribbean Company 1 employee was sent on April 24, 2017.

b. Victim Company 9 employees exchanged numerous emails with the fake Caribbean Company 1 employee between April 25 and May 18, 2017. On April 25, 2017, the fraudster provided account information for a BOA account ending in 7812, in New York. After Victim Company 9 made the payment but did not list the company name consistent with the name on the account, the Caribbean Company 1 employee told Victim Company 9 that the payment would be put on hold.

c. On April 28, 2017, the fraudster provided instructions for payment to a different BOA account ending in 1004, in the name of "Kuft Sales." This account was opened in Northridge, California by Coconspirator 17, using the business name "Kuft SA." Victim Company 9 provided the new bank account information to its bank on May 3, 2017, and the wire transfer was initiated on May 10, 2017.

184. Bank records indicate that the wire for \$220,462.68 (less \$40.00 in wire fees) was received into the Kuft SA bank account on May 10, 2017. At the time, the account had a balance of approximately \$1,183.51. On May 10, 2017, a check for \$10,000 was deposited into the Chase account of a coconspirator with the notation "Buy Goods." On May 11, 2017, \$60,000 was transferred through a teller transfer to the BOA account ending in 5283 dba "Griffin's Plumbing and Construction Inc.," which, as discussed later, was opened by a money mule but used by IKOGHO. On May 12, 2017, \$75,000 was transferred to the BOA account ending in 9405, dba "Irena Works," which as discussed later, was done in coordination with OGUNGBE. On May 15, 2017, cashier's checks of \$21,000 and \$9,500 were purchased in the names of UMJESI and IGBOKWE. Also on May 15, 2015, \$30,000 more was transferred via teller transfer to the BOA account ending in 9405, dba "Irena Works."

185. Evidence in the phones shows that IRO, IGBOKWE, UMEJESI, OGUNGBE, and UZOKA were involved in victimizing Victim Company 9 and laundering the proceeds.

a. First, evidence indicates that the “Kuft Sales” BOA account ending in 1004 was used and/or controlled by UMEJESI, who sent the account information to IGBOKWE for use on numerous occasions. Specifically, on March 24, March 29, and April 13, 2017, UMEJESI sent IGBOKWE the account information. On April 3, 2017, IGBOKWE told UMEJESI, “Kuft sales I use it for 98k coming from CN China.” On April 22, 2017, IGBOKWE sent UMEJESI the Kuft Sales bank account information and told him, “Using it 4 100 k.” On May 3, 2017, in response to IGBOKWE’s request for “account for 10k” for “Ali,” UMEJESI again sent the “Kuft Sales” account information.

b. On April 24, 2017, IGBOKWE sent UZOKA the “Kuft Sales” BOA account. On April 28, 2017, UZOKA asked, “this olu still good[?],” and IGBOKWE responded “👍.”

c. On May 3, 2017, UZOKA sent IGBOKWE a message containing an email from a Victim Company 9 employee to the Caribbean Company 1 employee, which appeared to be from the Caribbean Company 1 employee’s hacked email account. (At other points, UZOKA provided other screenshots of emails between the two.) UZOKA later let IGBOKWE know “this one is 220k” and sent him a wire transfer details confirmation for an earlier wire from Victim Company 9 to the other account discussed above—the BOA account ending in 7812, in New York. UZOKA explained that “the account they used spoil so now they have call the money and resending it here.” IGBOKWE sent the Kuft Sales bank account information again, and UZOKA responded, “yap na this one i use . . . this kuft.”

d. On May 10, 2017, UMEJESI sent a screenshot of a banking application showing that the Kuft SA bank account had a balance of \$221,738.86, which IGBOKWE sent to UZOKA. UZOKA responded by sending a screenshot of “Wire Instructions Details” that the fake Caribbean Company 1 employee provided to Victim Company 9, followed by a second image of a wire transfer details page from Victim Company 9 detailing a payment of \$220,462.68 on or about May 11, 2017 to the “Kuft Sales” BOA account. IGBOKWE later sent this to UMEJESI.

e. Also on May 11, 2017, UMEJESI asked IGBOKWE, “Oga send me the information of the account to do the transfer.” IGBOKWE responded, “Hold on. [¶] Am waiting for Val to send it to me,” referring to IRO. Later that morning, IRO sent IGBOKWE the BOA account ending in 5283 dba “Griffin’s Plumbing and Construction Inc.” IRO also sent a message saying, “Tell him...to tell the banker he want to make a payment. If the banker ask him, what kind of payment. Him should tell them send money to a company by teller transfer.” IRO also sent IGBOKWE the account information for the BOA account ending in 9405 dba “Irena Works,” which IGBOKWE forwarded to UMEJESI with the instruction “Val say u should use this one.”

f. IRO had received the account information for the BOA account ending in 5283 from IKOGHO earlier that day. Prior to that, on May 10 and 11, 2017, IRO discussed with IKOGHO that he was going to be receiving a wire for “200k,” and IRO then had a lengthy negotiation with IKOGHO about the exchange rate that IKOGHO would provide.

g. Also on May 11, 2017, UMEJESI sent IGBOKWE a photograph of a deposit slip showing transfer of \$60,000 from the Kuft Sales BOA account to the BOA account ending in 5283 dba Griffin’s Plumbing and Construction. IGBOKWE then sent this photo to IRO.

h. On May 12, 2017, UZOKA instructed IGBOKWE, “Tell him not to do round number [¶] If he want to do 70k he can do 74k 652 [¶] Because [ ]round no is not good on transaction.” IGBOKWE responded, “I know.”

i. Later on May 12, 2017, UMEJESI sent IGBOKWE a photograph of a deposit slip showing a transfer of \$75,500 from the Kuft Sales BOA account to the BOA account ending in 9405 dba “Irena Works.” IGBOKWE then sent this photo to IRO.

j. On May 13, 2017 and several other dates, UZOKA provided account information for Diamond Bank, a Nigerian bank—namely, “ezirim uzoma diamond bank [ACCOUNT NUMBER REDACTED]”—which at other points he referred to as “my Diamond.”

He also provided other Nigerian bank accounts to IGBOKWE where he requested funds be transferred.

k. On May 13, 2017, IGBOKWE told IRO to make payments from “2 different ones” (likely two different fraudulent schemes) into the Nigerian bank account of Coconspirator 18, IGBOKWE’s Nigerian wife.<sup>27</sup> In total, IGBOKWE gave IRO two separate payment instructions of ₦21,300,000 and ₦26,802,500, for a total of ₦48,102,500, which depending on the exchange rate provided would be approximately \$128,000 to \$141,000.

l. Later that day, IRO passed to IKOGHO (who used the “Griffin’s Plumbing and Construction” account) the instruction to pay ₦21,300,000 to Coconspirator 18. IKOGHO responded to IRO shortly afterward passing along a texted bank transfer receipt for “15,300,000.00,” and added “Balance 6,180,000,” indicating that was how much IKOGHO still had to transfer. Shortly after that, Coconspirator 18 told IGBOKWE, “I just got 15 million,300 thousand.” On May 15, IKOGHO confirmed to IRO payment of the remaining “6,000,000.00,” and Coconspirator 18 later told IGBOKWE, “I just got 6million.”

m. On May 16, 2017, IRO told OGUNGBE (who used the “Irena Works” BOA account) to pay ₦26,802,500 to the Nigerian bank account of a relative of IGBOKWE, Coconspirator 19, at First Bank. When OGUNGBE told IRO that he needed it to be a Diamond Bank account, IRO instead provided the account of his relative, Coconspirator 10. On May 17, 2017, IRO then asked Coconspirator 10 to “Pay 26,652,500” to the Fidelity Bank (Nigeria) account of Coconspirator 18, but after a series of phone calls asked Coconspirator 10 to pay “17,500.000” (₦17,500,000) to the bank account that UZOKA provided and ₦9,152,500 to Coconspirator 18 (IGBOKWE’s Nigerian wife). IRO also shared with IGBOKWE on May 19, 2017 that he requested these transfers. *Ogunjbe is not a licensed money transmitter.*

n. On several dates, IGBOKWE asked Coconspirator 18 to make transfers to the “Ezirim Uzoma” Nigerian bank account: ₦7,750,000 on May 15, 2017; ₦8,000,000 on May

---

<sup>27</sup> Messages on IGBOKWE’s phone indicate that MANSBANGURA eventually found out about Coconspirator 18.

19, 2017; and ₦3,150,000 on May 23, 2017. After the final transfer, UZOKA confirmed that he received the funds, saying, “saw money in my account . . . . I saw 3.1m.”

o. On May 14, 2017, UZOKA asked, “Did they make it on the cashes cheque [sic],” apparently referring to a plan to withdraw funds through cashier’s checks. IGBOKWE responded, “They said tomorrow,” which would have been May 15, 2017, the same date that cashier’s checks totaling \$30,500 were issued to UMEJESI and IGBOKWE. UZOKA also asked that IGBOKWE let him know when funds were “credit tomorrow,” and IGBOKWE responded, “I will move it immediately.”

p. Later on May 14, 2017, and into May 15, 2017, UMEJESI and IGBOKWE discussed the amounts that had been transferred from the “Kuft Sales” BOA account, and the amount remaining. This included discussion of the cashier’s checks, with IGBOKWE asking for a cashier’s check for \$9,500 addressed to him. On May 15, UMEJESI also sent IGBOKWE a photograph of a deposit slip showing a transfer of \$30,000 from the “Kuft Sales” BOA account to the “Irena Works” BOA account. IGBOKWE then sent this photo to IRO.

q. On May 16, 2017, UMEJESI sent IGBOKWE a photograph of a cashier’s check for \$9,500 addressed to IGBOKWE. Later, UMEJESI said, “I don get your cashier check,” (roughly meaning, “I have your cashier’s check”) and IGBOKWE provided him with the address for IRO’s apartment, presumably as the place to drop off the check.

18. Victim Law Firm May 2017 BEC Fraud (involving IRO, IGBOKWE, and CATHEY)

186. On May 11, 2017, Victim Law Firm was fraudulently induced to send a wire of \$83,140.98, which were the proceeds of a client’s real estate transaction, to the Chase bank ending in 5899 opened in the name of Chinese Company 2, which CATHEY had caused to be opened at the request of IRO. (As discussed in paragraph 171.i.i, the bank account had been opened by CATHEY in furtherance of the fraud involving Victim Company 6.) After the fraud was discovered and wire recall initiated, the funds, minus \$1,800 were returned to the Victim

Law Firm. Separately, on May 12, 2017, IRO and CATHEY realized that the victim was a U.S. law firm, and, on or about May 13, 2017, attempted to send the money back because they were concerned about scrutiny on the transaction.

187. I interviewed the owner of the Victim Law Firm in January 2018. Based on that interview, and documents he provided, I know the following:

a. The Victim Law Firm is located in North Carolina. In May 2017, a Victim Law Firm client completed a sale of property, with the Victim Law Firm assisting in the transaction. At the time the client came in to sign the closing documents, she was not prepared to provide wire instructions, so she said she would email wire transaction details to the Victim Law Firm. On May 11, 2017, a Victim Law Firm paralegal received an email from a Gmail account purportedly of the client providing instructions to wire the payment to the Chase bank account ending in 5899 opened in the name of Chinese Company 2. Although it is unclear whose email had been hacked, it is now apparent that this was not the client's email address; rather, it was a fraudster providing the transaction details.

b. The funds—\$83,140.98—were wired on or about May 11, 2017. Between May 11 and 15, 2017, the person using the fraudulent client email account sent several emails asking for confirmation of the wire transfer, in response to which the Victim Law Firm emailed a wire confirmation page.

c. On or about May 16, 2017, the real client called and asked about the funds. After discovering the fraud, the Victim Law Firm initiated a wire recall through SunTrust Bank and reported it to the authorities.

188. Evidence in the phones indicates that IRO, IGBOKWE, Coconspirator 20, and CATHEY were involved in victimizing the Victim Law Firm. In addition, IRO also discussed this transaction with OGUNGBE and EROHA—specifically, his reasons for attempting to return the funds.

a. On May 2, 2017, IRO provided IGBOKWE with the account information for the Chase account ending in 5899 in the name of Chinese Company 2. On May 4, 2017,

IGBOKWE asked IRO, “Should I use this aza us to us Ali [¶] 400[?]” IRO later responded, “Yes go ahead.”

b. IGBOKWE then sent Coconspirator 20 account information for two Los Angeles bank accounts—that Chase account ending in 5899 in the name of Chinese Company 2; and a US Bank account ending in 0362 dba “Danisha Beauty Sales,” which he also indicated went by the name “DB Sales.” In response, Coconspirator 20 indicated that he would use both accounts, and that it was for an “ali” (i.e., BEC fraud) of “400,430.”

c. On May 11, 2017, Coconspirator 20 sent a message to IGBOKWE saying the name of Chinese Company 2. Later that day, Coconspirator 20 called IGBOKWE. Shortly after that, IRO sent messages to CATHEY saying, “Please check the [Chinese Company 2] [¶] 200k was made today [¶] Check id it’s in there yet.” A few hours later, IRO asked CATHEY, “Check the [Chinese Company 2] again please [¶] Another 80plus is coming in.” CATHEY responded saying, “Ok I’ll check now,” and then shortly afterward said, “83k came.” IRO responded, “Cool [¶] 200 is coming.”

d. Later that day, IRO sent IGBOKWE a text saying “83k.” On May 12, 2017, IRO sent IGBOKWE a message saying “send that slip,” and IGBOKWE then provided a copy of the wire confirmation page, a PDF, confirming payment from Victim Law Firm, which IRO then sent to CATHEY.

e. Later on May 12, 2017, IRO and CATHEY had a lengthy conversation about the source of the funds. During the conversation, CATHEY expressed surprise and alarm that the “83 [wa]s domestic” (i.e., from a victim in the U.S.). IRO was apologetic to CATHEY and said repeatedly that he thought he could use the account for “local” wires (e.g., “Smh. Damn. [¶] Honestly, I thought you told me I can use that for local because the acc we opened it for was paying to local. Maybe I automatically thought it can be used for local.”). It appeared from the conversation that IRO and CATHEY were concerned because of their fear that CATHEY’s identity would be discovered.

f. On May 13, 2017, IRO wrote to CATHEY about the Victim Law Firm transaction: “I was just looking at the slip last night [¶] Bro yiu know I love you so much and I won’t let you get in trouble. Was looking at the slip and saw it came from something law firm . . . .” CATHEY responded, “Ohhhh yea that scared me.” IRO then said, “So this definitely might come back at us . . . Don’t let them send it back their self. Tell them to send it back . . . . Because if you let them send it back their self..it will mess the acc up [¶] But if you return it with your hand it will make the acc strong.” IRO then went on to give CATHEY further advice about how to convince the bank to take the funds back. CATHEY said he would try to return the funds, but later sent a voice note (essentially, an audio voice file) to IRO discussing how he was unable to return the funds unless he went into the bank branch.

g. Later on May 13, 2017, IRO sent IGBOKWE a screenshot from what appears to be a mobile banking application showing the wire from the Victim Law Firm and another wire from a likely BEC victim in Indonesia for \$22,013.88. IRO then sent another screenshot showing the account balance of \$105,195.86.<sup>28</sup>

h. There were other relevant messages, including screenshots sent by IRO and IGBOKWE to each other, from IRO to CATHEY, and from IGBOKWE to Coconspirator 20 regarding other conversations with the participants in this fraud. There were also conversations between IGBOKWE and Coconspirator 20 in which Coconspirator 20 repeatedly asked about whether the transaction was successful.

i. Finally, IRO had conversations with both OGUNGBE and EROHA about the wire from the Victim Law Firm, in each instance discussing how he sent the payment back after discovering that it was from a law firm.

---

<sup>28</sup> These files came from CATHEY; although IRO’s messaging conversation with CATHEY did not contain the images, the names of the files that CATHEY sent to IRO were the same as the names of the files that IRO sent to IGBOKWE.

19. D.V.—May 2017 Romance Scam (involving IGBOKWE and MANSBANGURA)

189. D.V., a 63-year old woman from Arizona, was victim to a romance scam in which she lost close to \$5,000, including two payments of \$500 to the Western Union account of Coconspirator 7 on May 13 and 15, 2017. I interviewed D.V. in December 2017, and she provided receipts related to the Western Union payments, as well as payment to another money service account controlled by a different person. Based on that information, I know the following:

a. In approximately January 2017, D.V. met a person using the name “Alan Good” (“Good”) on Facebook. Good claimed to be 47 years old and a sniper in the military. D.V. believed herself to be in a relationship with Good, who claimed that he wanted to leave the military so that he could come marry her.

b. At some point, Good asked D.V. for money to get out of having to complete his military service. D.V. believed she had sent Good close to \$5,000 in total, including a few payments through money services and money she had spent on credit cards. Good provided receipts for two payments through Western Union to Coconspirator 7, both for \$500, on May 13 and 15, 2017. (Records from Western Union also confirm those transactions.)

c. At the time of the scam, D.V. was approximately 61 years old and described herself as being victimized while she was “vulnerable” due to her longtime boyfriend passing away as well as some other family issues.

190. Evidence on the phones indicates that IGBOKWE was in contact with an unknown fraudster, and coordinated with MANSBANGURA regarding receipt of the funds from D.V.

a. On May 14, 2017, IGBOKWE sent MANSBANGURA a message saying, “Sender’s Details: [¶] Name: [D.V.] [¶] Address: [ADDRESS REDACTED] AZ [ZIP CODE REDACTED] . . . [Coconspirator 7].” When MANSBANGURA asked, “How much[?],” IGBOKWE responded, “500”, to which MANSBANGURA replied, “The money gram have my

[RELATIVE – REDACTED] name on it.” IGBOKWE later sent the same account information with an additional line saying “[RELATIVE – REDACTED],” instead of the name of Coconspirator 7.” IGBOKWE then also sent MANSBANGURA information about another apparent romance scam victim sending money through a money service.

b. On May 15, 2017, IGBOKWE sent MANSBANGURA a message saying, “Sender’s Details: [¶] Name: [D.V.] [¶] Address: [ADDRESS REDACTED] AZ [ZIP CODE REDACTED] . . . [RELATIVE – REDACTED] [¶] 500\$ [¶] Western union.” MANSBANGURA acknowledged the message.

191. Western Union records confirm the transactions by D.V. on May 13 and 15, 2017, to Coconspirator 7’s Western Union account, and that the funds were withdrawn on May 15, 2017.

20. Victim Company 10—May 2017 BEC Fraud (involving IRO, IGBOKWE, CATHEY, and Coconspirator 20)

192. I interviewed the Assistant General Manager of Victim Company 10 in July 2018, and, in January 2018, interviewed the Chief Financial Officer (“CFO”) of a Pennsylvania company with which Victim Company 10 was doing business (the “Pennsylvania Company”), and received documents from both persons. Based on that information, I know the following:

a. Victim Company 10 is a small Chinese company that sells components for railroad parts, while the Pennsylvania Company was selling components to Victim Company 10.

b. Victim Company 10 and the Pennsylvania Company agreed to a contract of more than \$700,000, in which the Pennsylvania Company would supply Victim Company 10 with parts for a railway project. Unbeknownst to both companies, the email account of a Victim Company 10 employee had been hacked, and a fraudster(s) began intercepting communications from Pennsylvania Company employees and set up a fraudulent email account through which the fraudster(s) communicated with Victim Company 10.

c. Specifically, a fraudster using the hacked email account of a Victim Company 10 employee was intercepting and blocking legitimate email traffic from the

Pennsylvania Company. The fraudster(s) created email accounts impersonating at least three Pennsylvania Company employees—the head of sales, the general manager, and the Chief Operating Officer (“COO”)—that they used to communicate with the Victim Company 10 employee. This impersonation included the creation of numerous fake contractual documents, which included falsification of a pre-payment amount (to inflate it) and the signatures of the three Pennsylvania Company employees. The fraudster(s) also created email addresses at Chinese email providers that they used to communicate with Pennsylvania Company personnel during the fraud scheme and after the scheme was discovered.

d. The fraudster(s) intercepted wire transfer information provided by the Pennsylvania Company, and sent wire instructions for a fraudulent Chase bank account ending in 7262, opened on May 15, 2017 in Inglewood, California, by a money mule, in the name of the Pennsylvania Company.

e. On May 17, 2017, Victim Company 10 wired \$301,201.20 to that account. Ultimately, after reporting the fraudulent transfer to the FBI at the Pennsylvania Company’s urging, China Merchants Bank and Chase were able to recover the funds and return them to Victim Company 10.

193. Evidence on the phones indicates that Coconspirator 20 was the middle-man for the fraudster(s) communicating with Victim Company 10. Similar to the fraud involving the Victim Law Firm, IGBOKWE was Coconspirator 20’s primary point of contact with the conspiracy, while IRO provided instructions to CATHEY, who worked with money mules.

a. On May 11, 2017, Coconspirator 20 sent messages asking IGBOKWE to open a bank account in the name of the Pennsylvania Company at a bank other than First National Bank, where Coconspirator 20 said the Pennsylvania Company had a legitimate bank account and indicated the funds were coming “Frm China to Usa.”

b. On May 11, 2017, IGBOKWE sent IRO a screenshot of his conversation with Coconspirator 20 about opening an account in the name of the Pennsylvania Company and said, “My friends call me if I can open this is business name [¶] Coming from China.” In

response to IRO's question "When do they need it[?]," IGBOKWE responded "Today [¶] Or tomorrow."

c. On May 12, 2017, IGBOKWE sent the name of the Pennsylvania Company to IRO again. Two minutes later, IRO sent a message to CATHEY saying, "Bro. Just got this order right now. Can you make it happen today?? If possible," and passed along the name of the Pennsylvania Company. CATHEY responded, "Ofcourse let me try asap."

d. On May 14, 2017, Coconspirator 20 emailed IGBOKWE about the "[Pennsylvania Company] account name," asking "It will be gud if we can get it today cos China people don write us and they are waiting." On May 15, 2017, at approximately 6:30 a.m., IGBOKWE then sent a screenshot of Coconspirator 20's messages to IRO, and asked for "any update from [IRO's] guys." IRO stated, "Yes they are getting everything today sir [¶] That's why I'm up."

e. On May 15, 2017, IRO sent messages to CATHEY stating, "Please remember this name today [¶] Company nane [sic]: [Pennsylvania Company] [¶] Please open it today." Later on May 15, 2017, CATHEY provided the account information to IRO for the Chase account ending in 7262, opened in the name of the Pennsylvania Company, in Inglewood, California. IRO provided the information to IGBOKWE, who, in turn, provided it to Coconspirator 20.<sup>29</sup>

f. On May 16, 2017, Coconspirator 20 asked IGBOKWE for "the evidence"—i.e., the wire transfer confirmation—for the deposit. In response, IGBOKWE sent a screenshot of his conversation with IRO, wherein he passed along Coconspirator 20's message to IRO. Coconspirator 20 later sent IGBOKWE what appeared to be a copy of an email sent by Victim Company 10 to the fraudster posing as the Pennsylvania Company.

---

<sup>29</sup> Based on my review of L.A. County records, on May 15, 2017, the money mule filed a fictitious business name statement matching the name of the Pennsylvania Company and adding "Beauty Supply" to the ending of the business name. On the same day, the money mule opened Chase bank account ending in 7262 in the Pennsylvania Company's name and dropped "Beauty Supply" from the account name.

g. On May 17, 2017, IGBOKWE sent IRO a screenshot showing the wire confirmation page for the wire from Victim Company 10 to the fraudulent Chase account ending in 7262. IRO then sent a message to CATHEY stating “Please I need you to go pay in money thru the atm to that acc. Put in like 1 or 2 or 5k [¶] Please do it this morning [¶] They paid to [the Pennsylvania Company],” and sent CATHEY the wire confirmation page. Later on May 17, 2017, IRO asked CATHEY to “service” the fraudulent bank account opened in the name of the Pennsylvania Company, among others that CATHEY had opened at IRO’s request, and then asked CATHEY to check the account.

h. On May 19, 2017, IRO asked CATHEY, “The [Pennsylvania Company]. I hope you servicing it too ya?? [¶] And everything is good. Ya?” CATHEY responded explaining that the bank had “refused to give a temp card” but that “the card should come in the mail today.”

194. Later on May 19, IRO and CATHEY exchanged messages about the payment to the fraudulent account. Among them, CATHEY said, “The sender is requesting the money back smh”; IRO said, “Damnnn [¶] No no no. This can’t happen.” CATHEY stated “Damn they found out huh?,” and IRO responded “I’m trying to find out.” After it became clear that the bank had frozen the funds, CATHEY asked, “Ok should I make another [Pennsylvania Company] account[?]” They then engaged in the following back-and-forth:

<b><u>SENDER</u></b>	<b><u>MESSAGE</u></b>
IRO	Damn
IRO	Smh
IRO	Okay
IRO	No problem
CATHEY	They recalled?
IRO	I just don’t know what to do or say
CATHEY	Did I do something wrong?
IRO	Not yet. Just trying to figure out
IRO	No no no no bro
IRO	Everything you did was perfect
IRO	It’s not your fault
IRO	I blame them for not holding the job well
IRO	They don’t know how to work well
CATHEY	Damn damn

IRO	My other contact would have held it better
CATHEY	We live to fight another day
IRO	👍 Yes forsure

21. Victim Company 11—June 2017 BEC Fraud (involving IRO, IKOGHO, UMEJESI, CATHEY, and EROHA)

195. In June 2018, FBI personnel interviewed representatives of Victim Company 11, which is based in Lebanon. Based on the report of the interview and documents provided by Victim Company 11, and bank records, I know the following:

a. Victim Company 11 is a company based in Lebanon that imports and distributes medical devices. In June 2017, Victim Company 11 was attempting to make a payment of \$297,617.11 to a major U.S. supplier of medical equipment (“U.S. Company 1”). Unbeknownst to Victim Company 11 employees, at some point they began communicating with hackers who were using email addresses at fraudulent domains that had been created to mimic the email domain of U.S. Company 1. Meanwhile, employees of U.S. Company 1 were communicating with a fraudster who also was using a fraudulent domain designed to look similar to the email domain of Victim Company 11.

b. On June 13, 2017, Victim Company 11 wired \$297,617.11 to a BOA account ending in 4180, which had been opened by a money mule. But BOA had closed the account in the meantime, so the transfer was not successful. The fraudsters therefore provided a new Wells Fargo bank account to be used, in the name of U.S. Company 1, which was opened by a different money mule. Victim Company 11 sent a second wire around June 16, 2017, and, based on review of bank records, a sum of \$297,563.11 arrived in the Wells Fargo account ending in 7984 on June 21, 2017. At some point after Victim Company 11 sent the second wire to the Wells Fargo account ending in 7984, Wells Fargo froze the funds and contacted U.S. Company 1, which then contacted Victim Company 11.

c. As discussed below, EROHA then opened BOA bank account ending in 3563 at IRO’s request, with a business name that was a variation of the name of U.S. Company 1. As of a week later, Victim Company 11 was still communicating with a fraudulent U.S.

Company 1 email account, but Victim Company 11 did not transfer funds to that BOA account ending in 3563.

196. Evidence on the phones indicates that Coconspirator 21 was the fraudster communicating with Victim Company 11 and U.S. Company 1, or a middle-man to the fraudster. IRO was Coconspirator 21's primary point of contact with the conspiracy, and he coordinated registering of business names and opening of bank accounts with IKOGHO, UMEJESI, CATHEY, and EROHA.

a. On May 25, 2017, Coconspirator 21 asked IRO to open a bank account in the name of U.S. Company 1, saying that he expected a payment of "300k" in the next week. IRO asked to remove the "Inc." from the name that Coconspirator 21 proposed. (IRO on other occasions removed the "Inc." from company names in whose names he was opening bank accounts because he said it took too long to register the business with L.A. County if "Inc." was in the name.)

b. A few minutes later, IRO asked CATHEY to open a bank account in the name of U.S. Company 1, telling him it was "[v]ery important and payment is soon." On May 26, 2017, CATHEY provided the BOA account ending in 4180 in the name of U.S. Company 1. Bank records and other evidence on the phones indicate that the account was opened by a money mule, on May 26, 2017, and that the money mule also filed a fictitious business name statement in the name of U.S. Company 1 with L.A. County on the same day. IRO provided the bank account information to Coconspirator 21 on May 26, 2017.

c. On May 31, 2017, Coconspirator 21 told IRO that he was "Expecting 300k for [U.S. Company 1]" in "Mid June," and he also sent IRO an email from a Victim Company 11 employee to personnel at U.S. Company 1.

d. On June 13, 2017, Coconspirator 21 told IRO, "Dem paid 297k USD today," and sent the text of an email from Victim Company 11 remarking how this was the first time that U.S. Company 1 had asked for a copy of the wire confirmation. Coconspirator 21 also

said that the money came from Lebanon and because “Ds ppl na very big company [i.e., “These people are a very big company”] . . . [u]sually dey don’t send slip.”

e. On June 13, 2017, CATHEY told IRO, “Bad news [U.S. Company 1] is going to bounce back. They [i.e., the bank] didn’t believe me so they closed account without me knowing because it was taking some time.” IRO responded, “Whatttt [¶] Oh God [¶] This is bad news [¶] Damnn.” IRO and CATHEY discussed what to do, and IRO eventually asked, “Please get it reopened so when it bounces back. I give it back to them.” Later that day, IRO said to CATHEY, “Another bad news. They paid another 459 to [U.S. Company 1] today [¶] When you opened the acc. I told you to service them because payments are coming in soon. I had my reasons.” After CATHEY apologized, IRO again asked him to reopen an account in the name of U.S. Company 1.

f. When, on June 14, 2017, IRO did not hear from CATHEY about opening a new account in the name of U.S. Company 1, he asked UMEJESI to open an account in that name, saying “Make sure you open it tomorrow. Not with boa. Open it with chase or wells.”

g. On June 15, 2017, IRO and UMEJESI again discussed opening the account, with UMEJESI telling IRO he was at the “county” (i.e., the L.A. County Registrar/Recorder’s Office), and then later reported, “We dey bank” (i.e., “We’re at the bank.”) UMEJESI later provided the information for a Wells Fargo account ending in 7985 in the name of U.S. Company 1. Based on bank records, this account was opened by a different money mule on June 15, 2017, and she also registered the company name with L.A. County on the same date. IRO also provided instructions about how to service the account, saying “We need to put more money” than the \$100 that UMEJESI and the money mule had deposited. Later on June 15, 2017, IRO warned UMEJESI not to discuss their activities, saying, “Bro. No tell anyone our business [¶] Just keep it to yourself.”

h. Also on June 15, 2017, IRO had a conversation with Coconspirator 21, in which he discussed having to open a new bank account. Although CATHEY and UMEJESI were the ones interacting with the bank, IRO told Coconspirator 21 that the bank manager told

him “that the acc was placed on hold since last week. Because they called me to provide more documents and information about my business but I didn’t pick up. So that they have decided to close the acc and not do business with me again.” IRO added, “So I quickly went and opened another aza,” and then he passed along the account information for a Wells Fargo account ending in 7984, which he said Coconspirator 21 should provide to Victim Company 11 and ask them to resend the money. IRO explained, “the boa don spoil” (i.e., the BOA account was frozen/closed) because “I think the real [U.S Company 1] has acc with them . . . . It has been a very stressful day.”

i. On June 19, 2017, IRO told UMEJESI to deposit \$1,000 into the Wells Fargo account ending in 7984 opened in the name of U.S. Company 1, because “Money is coming in there today or tomorrow.”

j. On June 20, 2017, IRO told UMEJESI that the funds had arrived, saying, “The slip just came . . . 3hk” (i.e., “\$300,000”). Later that day, IRO sent a screenshot of the wire transfer details (which Victim Company 11 separately provided to the FBI following its interview), saying, “I just saw the slip now. It says the value date is 21st.” While the image that Coconspirator 21 sent to IRO that day was not saved in the conversation on IRO’s phone, Coconspirator 21 said essentially the same information that IRO passed to UMEJESI: “D value date says 21 June 2017.”

k. On June 22, 2017, IRO approached MADEKWE about assisting in laundering the funds. He told MADEKWE, “3hk dey,” and asked “Are you interested?” MADEKWE initially misunderstood IRO as asking about “3k,” so IRO clarified, “No. I said 3hk [¶] 3 hundred k.” IRO discussed wanting to remove “[a]tleast 50” by a “Cash depo,” and to “do the rest for chinco,” i.e., sending the rest of the funds to China. MADEKWE asked if IRO could do a “c c,” i.e., cashier’s check, but IRO said, “Not in first move [¶] First move d always dey very critical.” They then went on to discuss the exchange rate MADEKWE would provide. The next day, however, MADEKWE reported to IRO, “Bro dey shut my account yesterday night,” seemingly referencing the Wells Fargo account discussed in paragraph 80.a.

l. On June 23, 2017, a Friday, with MADEKWE not available to launder the funds, IRO told UMEJESI to “Pay in \$84,755” to a different Wells Fargo account in the name of R.L. IRO received that account information from IKOGHO earlier that day.

m. On June 23, 2017, IRO and MADEKWE again discussed the possibility of MADEKWE laundering funds, with MADEKWE expressing interest in laundering approximately \$70,000. However, IRO told MADEKWE that he was “already on the move,” suggesting that he had already started laundering the funds.

n. On June 24, 2017, IRO told Coconspirator 21 that he had opened a new account using the name of U.S. Company 1, but using “In.” at the end rather than “Inc.” He added that he could not call it “[U.S. Company 1]” because that was “already in use. It can’t be registered 2times. [¶] So that’s why I put IN.” (Earlier, IRO had separately explained to Coconspirator 21 that it was “[n]ot gonna work” to include “Inc.” in the name.)

o. On June 25, 2017, IRO provided Coconspirator 21 with the information for the new BOA account ending in 3563, in the name of U.S. Company 1. Based on bank records, that account was opened by EROHA on June 23, 2017, and he registered the business name with L.A. County on the same date, listing the address as IRO’s former residence in Carson, California.

p. On June 25, 2017, UMEJESI sent EROHA the screenshot of the wire transfer confirmation from Victim Company 11, saying, “This is Aribaba [i.e., Alibaba] invoice.”

q. On June 26, 2017, IKOGHO sent IRO the information for a Wells Fargo bank account in Georgia. After IKOGHO sent it, IRO asked, “And yiu control it ya? [¶] Because I don’t want situation like this again [¶] Your boy answer don put my acc on hold. The wells. How can he say he doesn’t know about the money [¶] That he doesn’t know what it’s for.” In other words, it appears IRO was chastising IKOGHO for an earlier incident in which a money mule told the bank that he did not know about the source or purpose of incoming BEC funds. (Based on discussion below, it appears that occurred on June 24, 2017.) IKOGHO reassured IRO, “He said he told then he receive lots of funds and let him check which of the funds.”

r. On June 26, 2017, IRO gave UMEJESI instructions to go with his “girl” into the bank branch and try to transfer the money to the Wells Fargo account in Georgia that IKOGHO had provided, and to tell the bank that there had been a “mistake” about which account the money was transferred to. IRO also gave UMEJESI instructions about how to dress, telling him “Please you guys must dress well [¶] Please [¶] Dress well. Suit if you can [¶] Talk confidently.”

s. On June 26, 2017, IRO reported to Coconspirator 21, “There’s a problem,” and explained that while the funds came in on Friday the “receiver go do mistake” and attempted to transfer \$84,000 on Saturday (a reference to his instruction to UMEJESI to transfer \$84,755 on June 23, 2017). IRO reported that the bank that received the wire “suspected his acc and held it. Returned the money to our acc. [¶] Now...they have put our own on hold. [¶] Told us they will close it.” IRO also sent Coconspirator 21 screenshots of the Wells Fargo account ending in 7984 reflecting the deposit of funds from Victim Company 11 and the subsequent withdrawal of \$84,755. IRO added, “This is totally my fault. Na d stupid new exchanger I go use cause,” seemingly a reference to IKOGHO. Iro explained that his “main exchanger” (a reference to MADEKWE) had gone to Nigeria and this “dude [i.e., IKOGHO] messed me up mehnnnnn.”

t. On July 6, 2017, UMEJESI and IRO again discussed Victim Company 11, with UMEJESI saying, “Oga, is urgent [¶] Can you call me[?]” After IRO called, IRO sent him a message saying, “The country is. Lebanon. [¶] Company is. [Victim Company 11].”

u. On July 12, 2017, Coconspirator 21 told IRO, “[U.S. Company 1] just update all their customers [¶] That there is no change of account.” IRO responded, “Damnn [¶] So we lost it. Ya?”

22. B.P.—June & July 2017 Elder Fraud (involving IGBOKWE and MANSBANGURA)

197. B.P. is an 81-year old woman from Hawaii who was defrauded of approximately \$750,000. Her payments to the fraudsters included \$4,800 in three wires to the Chase account

ending in 7605 of Coconspirator 7, dba “T and F Enterprises.” Specifically, bank records indicate that she made the following wires from her First Hawaiian Bank account in Honolulu, Hawaii: \$750 on June 23, 2017; \$1,500 on June 27, 2017; and \$2,550 on July 13, 2017.

198. I interviewed B.P. in March 2019, after previously interacting with her by email. Based on those interactions, I know the following:

a. B.P. stated that she met a man on Facebook approximately four years ago who worked on an oil rig in Belgium. She had a platonic relationship with him but he asked her help in couriering a box of cash to the United States. B.P. believed that she was making payments toward receiving that box of cash.

b. It was apparent from the interview that B.P. was actively in the process of being defrauded, and was in denial. She refused to give me the man’s name without first asking the man about having received a call from the FBI.

c. B.P. did, however, confirm that she made the three wire transfers to the Chase account ending in 7605 of Coconspirator 7, dba “T and F Enterprises,” which she confirmed in an email she believed they were for “courier fees, tax stamps & customs fees.”

d. B.P. also stated that her husband, J.P., believed that she was being defrauded, but then she abruptly ended the interview.

199. A few minutes later, J.P. called me and shared the following information:

a. J.P., who is also elderly, overheard my conversation with B.P. from an adjacent room, and added that the story B.P. shared with me was one he had never heard. He had, however, heard about 15 different stories about different approaches by online “friends” to B.P.

b. J.P. stated that they had been married for more than 50 years, but the last three had been very difficult because she had been repeatedly defrauded by individuals who she met online who she was convinced were real, who enlisted her for help in obtaining “gold,” a “box of cash,” and other items of value.

c. J.P. said that B.P. became very angry when he confronted her about these online “friends.” Although she had sold businesses she owned for more than a million dollars, he believed that she had lost approximately \$750,000 to online fraudsters and that she had spent her savings including annuities of \$300,000 and additional money from IRAs. B.P. was now deeply in debt, including \$130,000 in short-term debt, such as credit card expenses. J.P. added that he had tried to get her debts under control but could not stop her from giving her money away and that he was afraid of losing her.

200. Evidence on the phones indicates that Coconspirator 22 was the middle-man to the fraudsters controlling B.P. Coconspirator 22 communicated with IGBOKWE about defrauding B.P., and MANSBANGURA assisted IGBOKWE with receiving and laundering the funds.

a. Coconspirator 22’s messaging conversation with IGBOKWE made clear that B.P. was a fraud victim. For instance, Coconspirator 22 referred to her as a “mugu . . . from America.”

b. On June 20, 2016, IGBOKWE provided Coconspirator 22 his BOA account ending in 2660, and also the Chase account ending in 7605 of Coconspirator 7, dba “M&F Enterprises.”

c. On June 23, 2017, Coconspirator 22 told IGBOKWE that his “guy” said that the “mugu” had made a payment, and Coconspirator 22 then provided the Nigerian bank account of his “guy,” where IGBOKWE should send the money.

d. Each of the transactions—the wires of \$750 on June 23, 2017, \$1,500 on June 27, 2017, and \$2,550 on July 13, 2017 into the Chase account—were discussed in great detail by Coconspirator 22 and IGBOKWE, including Coconspirator 22 sending photographs of wire transfer orders and deposit slips, and also discussing the specific amounts deposited in the accounts.

e. They also discussed laundering the funds, including sending funds to Nigeria. For example, on June 26, 2017, IGBOKWE stated, “Am sending it 2 9ja [Nigeria].”

He confirmed that he had Coconspirator 22's bank account information and information for the account of Coconspirator 22's "guy," and Coconspirator 22 told IGBOKWE to send 10 percent to Coconspirator 22 and the rest of to his "guy."

f. On June 27, 2017, IGBOKWE instructed Coconspirator 19, who was in Nigeria, to make payments to Coconspirator 22 and the Nigerian bank account referenced above. IGBOKWE instructed Coconspirator 19 to make payments to both accounts on July 5, 2017, as well.

g. MANSBANGURA assisted in receiving and laundering the funds. IGBOKWE's messages to Coconspirator 22 on June 28 and 29, 2017 indicate that MANSBANGURA was checking the Chase bank account for incoming funds. On June 28, IGBOKWE said that he could not check the bank account because his "woman" was at the hospital. When Coconspirator 22 asked, "which of ur woman [¶] the one there or the one in niaja [sic]," IGBOKWE responded, "America." On June 29, 2017, IGBOKWE sent Coconspirator 22 a video that MANSBANGURA had sent to him of her navigating through the bank account using a banking application, showing that the transaction about which Coconspirator 22 was asking was not yet pending in the account.

23. Victim Solicitor Firm—June 2017 BEC Fraud (involving IRO, IGBOKWE, CATHEY, IKOGHO, and CHUKWUOCHA)

201. Victim Solicitor Firm is a U.K. solicitor firm, which frequently assists with property sales. On June 22, 2017, the Victim Solicitor Firm was fraudulently induced to send a wire of \$199,060 to a Chase account ending in 7633, which had been opened by a money mule in the name of a Middle Eastern company ("M.E. Company 1").

202. One of the owners of the Victim Solicitor Firm was interviewed by law enforcement in the U.K. in September 2018, during which he also provided relevant documents. Based on this, I know the following:

a. In June 2017, the Victim Solicitor Firm was working for a client company in Wales (the “Welsh Company”), arranging a bridging loan of approximately \$200,000 to an American company (“U.S. Company 2”).

b. On June 22, 2017, the Victim Solicitor Firm received an email purporting to be from the finance director of the Welsh Company, using a Yahoo email address designed to look like it was coming from the Welsh Company. The email requested that the Victim Solicitor Firm send the planned wire transfer to a Chase account ending in 7633, using the name of U.S. Company 2. In reality, the bank account was opened by a money mule with the business name of M.E. Company 1, which she had also recorded with L.A. County.

c. The Victim Solicitor Firm made the payment on June 22, 2017, and then, after receiving another email from the same account requesting confirmation of the transfer, subsequently emailed a wire transaction detail report. (That transaction detail report was ultimately sent by Coconspirator 20 to IGBOKWE, who then forwarded it to IRO.)

d. The fraud was not discovered until July 11, 2017, when the Victim Solicitor Firm received a call from the owner of U.S. Company 2, asking why the payment had not arrived. The Victim Solicitor Firm immediately contacted Lloyds Bank, which was able to provide a partial reimbursement of £114,423.45 (\$147,160.00). The Victim Solicitor Firm also hired an IT company, which identified that the Victim Solicitor Firm’s email system had been hacked and a number of emails to and from the Victim Solicitor Firm had been intercepted and blocked. From reviewing the emails, the Victim Solicitor Firm discovered a fraud involving another of his clients at approximately the same time, which led to a loss of £10,616.94.

203. Bank records show that after the funds were credited to the Chase account ending in 7633 in the name of M.E. Company 1, a transfer for \$43,750 was made to the Chase account ending in 6781 of a money mule dba “Friar SA” on June 23, 2017. An additional \$9,150 was withdrawn by cashier’s check addressed to another person on June 24, 2017. The remaining funds (\$147,160.00) were frozen and reversed by the bank on June 28, 2017 when the bank

determined that the beneficiary name on the wire transfer (U.S. Company 2) did not match the account name (M.E. Company 1).

204. Evidence on the phones indicates that, similar to the frauds against the Victim Law Firm and Victim Company 10, Coconspirator 20 was the middle-man for the fraudster(s), IGBOKWE was Coconspirator 20's primary point of contact with the conspiracy, and IRO provided instructions to CATHEY, who worked with money mules. IKOGHO laundered the funds after they arrived in the Los Angeles account, in coordination with a money mule(s) working at his direction.

a. On June 20, 2017, Coconspirator 20 sent a message to IGBOKWE saying, "I need USA account for 200k from UK (Alibaba)." Coconspirator 20 and IGBOKWE then went on to discuss potential accounts into which the funds would be deposited (including a BOA account ending in 7032, opened by a money mule in the name "Miami Perfume Junction"<sup>30</sup>; a Wells Fargo account ending in 5309, opened by a money mule in the name "Michael Park Motorcycle Club"; and a BOA account ending in 1004, opened by a money mule in the name "Kuft Sales"), but Coconspirator 20 rejected them as having business names that were "Not good" "[f]or Ali." After discussing what IGBOKWE's cut would be, Coconspirator 20 sent the name of U.S. Company 2.

b. Shortly afterward, IGBOKWE asked IRO to open the account, saying "[U.S. Company 2] Can we open this name 200k coming from U.K. [¶] If possible today they will pay it tomorrow." IGBOKWE later repeated his request.

c. Also on June 20, 2017, Coconspirator 20 asked IGBOKWE, "What's the progress . . . Am still waiting and waiting." IGBOKWE responded, "Still waiting for the guy," and sent Coconspirator 20 a portion of a conversation between IRO and CATHEY discussing opening the account.

---

<sup>30</sup> IRO's messaging conversation with OJIMBA revealed that this "Miami Perfume Junction" account and several others were opened by a money mule who worked with OJIMBA, at the direction of OJIMBA and UMEJESI.

d. IRO told IGBOKWE if he needed “LLC” in the bank account name that it “will take 2weeks,” which IGBOKWE relayed to Coconspirator 20 on June 21, 2017.

Coconspirator 20 responded, “Remove llc bro,” and further told IGBOKWE that he needed the account in the name of U.S Company 2 “today.”

e. Later on June 21, 2017, IRO provided the bank account information for the M.E. Company 1 account to IGBOKWE.<sup>31</sup> Shortly afterward, on June 21, 2017, IGBOKWE provided Coconspirator 20 the following account information:

Bank: chase  
[U.S. Company 2]  
Name: [M.E. Company 1]  
Acc: [REDACTED]7633  
Rout: 322271627  
Address: 6201 Bristol Parkway  
Culver City, ca 90230

f. When Coconspirator 20 asked, “What’s [M.E. Company 1?],” IGBOKWE responded “Remove it,” and then provided the same information to Coconspirator 20 minus that name.

g. On June 22, 2017, Coconspirator 20 confirmed with IGBOKWE the account details, saying, “Below is how the account was given for 200k from UK.” Later that day, CATHEY informed IRO, “Hey bro the 199 came in. We getting 40 or 50%[?] So I can tell me ppl how much I’m paying them.” After some discussion, IRO confirmed for CATHEY, “You guys get 40k.” IRO also told CATHEY to expect additional payments and to service the account so that it would be easy to get funds out: “The payment they made is 20% deposit. They

---

<sup>31</sup> The M.E. Company 1 account was opened at the request of two persons. The history of how the account was opened is noteworthy because it illustrates the structure of money laundering operations, with multiple middle-men for Nigerian hackers reaching out to multiple persons about laundering funds.

CATHEY coordinated opening the account for IRO on June 20, 2017, after IRO and IGBOKWE received separate requests to open an account in the name of M.E. Company 1. Specifically, on June 19, 2017, a coconspirator sent IRO a message saying the name of M.E. Company 1 and then telling IRO, “My guys need aza. 400k usd.” IRO sent the name of M.E. Company 1 (without the “LLC”) to CATHEY that day. On that same date, later in the day, CHUKWUOCHA sent IGBOKWE messages saying the name of M.E. Company 1, and stating “My guys need acct 400k” in “USA.”

are supposed to make another by the end of next week. So let's keep the acc good. And please. You know how we do. You need to start making use of it [¶] Gas....food electronic [¶] No hair product...no shoes....no cloths.”

h. On June 23, 2017, Coconspirator 20 sent IGBOKWE screenshots of emails between the Victim Solicitor Firm and a fraudster purporting to be the finance director of the Welsh Company—including an email later provided by the Victim Solicitor Firm to U.K. law enforcement—indicating that Coconspirator 20 or a co-conspirator of Coconspirator 20 was controlling the email account.

i. On June 23, 2017, IRO gave instructions to CATHEY to “Pay \$43,750” to a Wells Fargo account ending in 6781, in the name “Friar SA.” IRO received this bank account information from IKOGHO earlier that day, and from IRO’s conversation with IKOGHO later that day IKOGHO appeared to be controlling the Friar SA bank account. Later in the day, IRO asked IKOGHO to “Confirm c”—i.e., confirm the transaction into the Chase account, and that the transaction would be for \$43,750. IKOGHO confirmed that this transaction and another transaction related to the fraud involving Victim Company 11. On June 23, 24, and 26, 2017, IRO and IKOGHO engaged numerous telephone calls.

j. Later on June 23, 2017, Coconspirator 20 sent IGBOKWE the wire transaction detail report, which is the same document that the Victim Solicitor Firm provided to U.K. law enforcement. IGBOKWE forwarded it to IRO, who in turn sent it to CATHEY. Coconspirator 20 and IGBOKWE also had a lengthy discussion spanning June 23–25, 2017, about how quickly funds could be removed from the account, with Coconspirator 20 complaining, “Just that 40k out off 199k is small for a start.” Ultimately, after hearing that more of the funds were not available, Coconspirator 20 suggested that the person IGBOKWE was working with had stolen the money because there was “no evidence that it’s only 40k that has been removed.”

k. On July 25, 2017, IRO and CATHEY discussed the Victim Solicitor Firm funds, with IRO telling CATHEY, “It went thru but the fool went to remove it yesterday and

they put his acc on hold. Told him they will return it to our account tomorrow.” After discussing it further, CATHEY told IRO, “Ok bro I’ll take care of it no worries.” (This episode was discussed in relation to the fraud involving Victim Company 11.)

l. On June 26, 2017, however, CATHEY wrote to IRO, “Bad news bro. Jerry [i.e., IKOGHO] wasn’t lying they found out. There closing the account.” CATHEY and IRO exchanged a number of messages and audio messages to each other, most of which IRO passed on to IGBOKWE, as well.

m. IRO sent IGBOKWE messages saying, “They returned the 43k back and put our thing on hold. That they suspected the acc we send money to. So they returned it back today and put our acc on hold. [¶] The only thing g that came out is 8k.” In the series of messages that ensued, IRO sent IGBOKWE an audio message from CATHEY discussing the “43,000 that was trying to be returned” and how it “Looked like fraud from jerry [i.e., IKOGHO] end so they did a review... they fucked everything up.” After sending IGBOKWE several other audio files exchanged between IRO and CATHEY, IRO added, “Jerry messed me up [¶] How can money enter his acc on Friday and he went to remove it on Sat morning . . . And funny enough.....they put my wells onhold too.” Later IRO said, “They returned the 84k to my wells [¶] And 43 to the chase,” which is a reference to the Victim Company 11 fraud, in addition to the Victim Solicitor Firm fraud.

n. IRO sent IGBOKWE additional voice audio files from CATHEY and himself regarding the M.E. Company 1 account, and also screenshots of his messaging conversation with CATHEY wherein CATHEY provided a money mule’s birthdate, social security number, and name, as well as providing the bank account information for the M.E. Company 1 account.

o. Also on June 26, 2017, after a series of calls with IKOGHO, IRO also exchanged a number of messages with him. During the conversation, IRO and IKOGHO pointed the finger at each other, with IKOGHO saying, “If it’s [i.e., the funds] been cleaned it’s not suppose to just mess up like that,” and IRO responding, “I tell you it has been cleaned . . . . Na

your end cause everything.” IRO said that the “Wells” and “C” (i.e., Wells Fargo and Chase) “[b]oth just burst today.” IRO also provided IKOGHO with the money mule’s account information, and, the next day, told IKOGHO that the funds came from “[Victim Solicitor Firm] [¶] From: uk [¶] Chase.” They then again exchanged several calls.

p. There were numerous other additional messages between the coconspirators about this transaction.

24. Victim Company 12—June 2017 (involving IRO and CATHEY)

205. Victim Company 12, a distributor of steel pipes based in Texas, was the intended victim of a BEC fraud in June 2017, relating to a payment of \$2,502,585.30 to a South Korean company (the “Korean Company”) that supplied products used in oil and gas extraction.

206. I interviewed the CFO of Victim Company 12 in August 2018. Based on that interview and documents provided by the company, I know the following:

a. On May 22, 2017, an employee of the Korean Company sent an email attaching an invoice for a 25 percent deposit for Victim Company 12’s planned purchase from the Korean Company. The deposit was to be approximately \$631,185. The next day, May 23, 2017, a fraudster sent the same document with the same legitimate bank information of the Korean Company, but from a fraudulent email account that used a fraudulent email domain that was a slight misspelling of the Korean Company’s name. (In starting by intercepting but not otherwise interfering with the communications about a legitimate transaction, the hacker may have been attempting to get Victim Company 12 to communicate with him without raising its suspicions, in the hope that he could intercept the later, larger wire of \$2,502,585.)

b. The planned wire of \$2,502,585.30 was intended to be the outstanding 75 percent owed to the Korean Company. At some point before the transaction, however, Victim Company 12 discovered the fraud when its employees noticed the misspelling in the fraudulent email domain compared to the Korean Company’s legitimate email domain. Based on conversations with the Korean Company, Victim Company 12 personnel understood that the Korean Company’s email system had been hacked. Thus, on June 28, 2018, when the

fraudster(s) sent fraudulent bank information for the planned payment of \$2,502,585.30—a Chase account ending in 6679 opened by a money mule in the name of the Korean Company—Victim Company 12 did not make the transfer. (Based on records from the L.A. County Recorder, a business in the name of the Korean Company was registered on May 30, 2017.)

207. Evidence on the phones indicates that IRO coordinated with Coconspirator 21 regarding the fraud, and that Coconspirator 21 was a middle-man for the fraudster. Additionally, IRO coordinated with CATHEY regarding the creation and preparation of the fraudulent bank account.

a. On May 25, 2017, Coconspirator 21 sent IRO a message saying the name of the Korean Company. Coconspirator 21 went on to tell IRO, “They have remitted 25% to d real ppl yesterday [¶] 25% was 681k Usd [¶] So d balance is against Bl [¶] Balance is 2.7M [¶] D earlier we have d aza d better[.]” Coconspirator 21 further stated that the next payment should be coming in “[t]wo weeks.” IRO responded, “I will work on the aza do it will be ready and strong on or before Monday.”

b. IRO then sent CATHEY a message asking him to open an account in the name of the Korean Company, in addition to an account in the name of U.S. Company 1, both of which he said were “[v]ery important.” The next day, IRO said, “[Korean Company] is due in 2weeks for 2.7m. We can open that one next week Monday or Tuesday.” CATHEY responded, “OK I am on it double time.” IRO also told CATHEY, “These are sure deals [¶] He’s the owner of the last year we did.”

c. On May 30, 2017, IRO and CATHEY discussed the transaction, and CATHEY sent IRO account information for the account opened by a money mule. IRO passed that information to Coconspirator 21, in addition to further discussing the transaction.

d. At several points in June, IRO checked in with Coconspirator 21, who told him that the money was still expected. IRO appeared to discuss with both Coconspirator 21 and CATHEY another transaction of “1.4” coming into the Korean Company account from a company in Colorado, but on June 3, 2017 told CATHEY, “The [Korean Company] that paid

1.4. The reason it didn't come in they also found out and cancelled it. . . . But we still have hope of 2.7 from [Korean Company] [¶] But that is in 2weeks." It appears that this might have been another bank account, though, because on June 28, 2018, CATHEY stated, "Ok cool. I made 3 [Korean Company] accounts I'm just confirming the right one." IRO then confirmed for CATHEY that "we using the chase," and re-sent the account information for that account.

e. On June 28, 2017, Coconspirator 21 told IRO that the "D documents don come" (meaning, "the documents have come") and further discussed the transaction.

f. Later on June 28, CATHEY told IRO, "I'm just waiting for my cousin to wake up . . . I've been blowing up his phone I know he's sleep [¶] He just confirmed that the account is good [¶] So Ima service it and call [¶] Do you have any details I can call with." IRO responded, "I think the money is coming from here." Later that day and on June 29, 2017, IRO and CATHEY discussed servicing the bank accounts.

g. On June 30, 2017, IRO requested information about the companies involved in the transaction, and Coconspirator 21 told him that the money would be coming from Victim Company 12 and that the Korean Company was from Korea. IRO passed some of that information to CATHEY. IRO and CATHEY continued to discuss the account and a potential transaction in the account into July 2017.

25. D.A.—June 2017 (involving IGBOKWE and MANSBANGURA)

208. D.A., a 64-year old man, was defrauded of at least \$500 in a debit card scam in June 2017, in which D.A. was told that he would receive a debit card containing funds if he first made a down payment. D.A. made the \$500 wire from the account of his company, located in Kansas (the "Kansas Company").

209. D.A. was interviewed in February 2018, and provided an email related to the payment. D.A. indicated that from June 6 through 16, 2017, he received several emails from a person using the name "George Wilson" related to the scam. On June 15, 2017, D.A. was instructed to make a payment to the Chase account ending in 5027 of Coconspirator 7 dba

“Victim Company 5.” D.A. made a payment of \$500 on June 16, 2017, and referenced in a communication to the fraudster that he had previously made other payments.

210. Evidence on the phones indicates that Coconspirator 23 was either the fraudster using the name George Wilson or a middle-man to the fraudster. IGBOKWE was Coconspirator 23’s point of contact with the conspiracy, and MANSBANGURA assisted in laundering the fraudulent proceeds.

a. On June 16, 2017, Coconspirator 23 sent IGBOKWE attachments named “[Kansas Company] Wire Confirmation.pdf” and “[Kansas Company] Wire Confirmation-1.pdf,” which contained an identical copy of a “Fedwire Payment” page, indicating that the Kansas Company had made a wire of \$500 from its Capital City Bank account to the Chase account ending in 5027. The PDF listed D.A.’s name and address, as well as his social security number.

b. On June 16, 2017, after receiving the PDF from Coconspirator 23, IGBOKWE forwarded it to MANSBANGURA, saying “Check if the 500.” MANSBANGURA responded, “The \$500 is not there,” and then MANSBANGURA and IGBOKWE had a 2 minute and 10 second conversation.

c. On June 17, 2017, Coconspirator 23 said, “Hope u got it,” and IGBOKWE responded, “Nothing yet [¶] Beside his bank is a big problem here.”

211. Bank records confirm the wire was deposited and posted to the Chase account ending in 5027 from an account of D.A.’s company at Capital City Bank, on June 16, 2017.

26. M.G.—July 2017 through May 2018 Romance Scam Victim (involving IRO, IGBOKWE, AJAEZE, EROHA, and CHUKWUOCHA)

212. M.G., who lives in Mexico, is a romance scam victim who made six payments, totaling \$40,700, to accounts opened by EROHA and AJAEZE, among others. M.G. was interviewed by SA Luna in October 2018, and provided relevant documents. Based on the report of her interview and the documents she provided, I know the following:

a. M.G., who is an attorney, began an online relationship with a person using the name “David Cole” (“Cole”) in March 2017. She initially was contacted by Cole through a dating website, and they quickly moved their conversations to Viber, a messaging application. Cole told M.G. that he was a widower with a five-year-old daughter, and was a chemical engineer at an oil refinery in New Jersey. Although M.G. attempted to talk to Cole by phone or video-chat, Cole always came up with reasons that he could not talk to her. Nevertheless, M.G. considered herself to be in a romantic relationship with Cole and exchanged messages with him through Viber almost every day until she was contacted by the FBI.

b. At some point, Cole told M.G. that he had been involved in a lawsuit and had to pay a judgment. He said he had paid \$60,000 and needed to pay an additional \$20,000. Cole sent M.G. the proof of payment and asked whether he could borrow the rest from her. While M.G. was initially hesitant, she eventually agreed to loan him money. On July 6, 2017, M.G. used her HSBC account to wire \$11,000 to a BOA account opened by EROHA in the name of U.S. Company 1, which Cole told M.G. was the company to which he owed money.

c. Over the course of the next ten months, M.G. made five additional payments, each to a Los Angeles bank account. Among those were the following payments:

- i. Approximately \$5,000 on July 17, 2017 to EROHA’s BOA account ending in 3563 opened in the name of U.S. Company 1;
- ii. Approximately \$5,500 on December 15, 2017 to a BOA account ending in 3349 opened by AJAEZE, which listed its address as IRO’s apartment;
- iii. Approximately \$2,000 on December 22, 2017 to AJAEZE’s BOA account ending in 3349; and
- iv. Approximately \$11,000 on May 2, 2018 to a US Bank account ending in 2910 in AJAEZE’s name.

213. Bank records further indicate that funds deposited through the wires to EROHA’s BOA account ending in 3563 were withdrawn as cash withdrawals, retail purchases, and wires.

Notably, on July 10 and 11, 2017, wires of \$6,000 and \$2,800 were paid to the Wells Fargo account ending in 5736 of CHUKWUOCHA.

214. Additionally, as discussed in the next section, following the \$5,000 wire to EROHA's BOA account ending in 3563 from M.G. on July 17, 2017, \$5,000 was withdrawn as cash. The messaging conversation between IGBOKWE and CHUKWUOCHA reflects that \$4,150 was then deposited in cash to CHUKWUOCHA's Wells Fargo account ending in 5736 on July 18, 2017. Bank records confirm this cash deposit to CHUKWUOCHA's Wells Fargo account, which was opened in his name on March 31, 2017.

215. Evidence in the phones indicates that CHUKWUOCHA was a middle-man to the unknown fraudster interacting with M.G., while IGBOKWE was CHUKWUOCHA's point of contact with the conspiracy. EROHA and AJAEZE received fraudulent funds into their bank accounts, and IRO provided advice to EROHA about receiving the funds. EROHA, IGBOKWE, and CHUKWUOCHA were also involved in laundering the funds (in addition to bank records which indicate that AJAEZE received fraudulent funds into his bank account).

a. On July 3, 2017, CHUKWUOCHA asked IGBOKWE for an "aza for dating" for "11k" coming from "Mexico." After they discussed IGBOKWE's cut, IGBOKWE sent the account information for EROHA's BOA account ending in 3563 opened in the name of U.S. Company 1, with the additional instruction to CHUKWUOCHA: "Please give them this purpose of payment. [¶] Payment for Hill43636." That account information and latter instruction was given by IRO to EROHA earlier on July 3, 2017, who then provided that same information and instruction to IGBOKWE when sending him the account information.

b. On July 6, 2017, CHUKWUOCHA sent IGBOKWE a message saying, "the client don pay the 11k" (i.e., the romance scam victim paid \$11,000), and later sent IGBOKWE a photograph of a computer screen showing a wire order, saying, "[T]his is the slip." (M.G. provided the same photograph to the FBI.)

c. On July 7, 2017, CHUKWUOCHA also pasted an apparent message from M.G., saying, "Hello baby already make the deposit to name [U.S. Company 1] Account [ending

in] 3563. Swiftcodigo BOFAUS3N. For eleven thousand dollars. I hope I have done the right thing, and I also hope that you will really give it back to me.” Later that day, CHUKWUOCHA sent his name, city, and persona; bank account information to IGBOKWE. IGBOKWE then sent that information to EROHA, who asked him to get the “Get routin[g] number from chi boy” (referring to CHUKWUOCHA’s nickname).

d. Later on July 7, 2017, IGBOKWE sent CHUKWUOCHA a photograph of a wire request from EROHA’s BOA account to CHUKWUOCHA’s Wells Fargo account, in the amount of \$6,000. This amount corresponds with the wire that went through on July 10, 2017, discussed above. On July 11, 2017, IGBOKWE sent CHUKWUOCHA a photograph of a wire request from EROHA’s BOA account to CHUKWUOCHA’s Wells Fargo account, in the amount of \$2,800, which corresponds to the wire reflected in bank records on that date.

e. On July 15, 2017, CHUKWUOCHA said to IGBOKWE, “I wan give that Mexico your aza.” On July 17, 2017, CHUKWUOCHA said, “Nwanne na 5k she pay [¶] She will pay the rest on Wednesday,” and then sent a photograph of a computer screen showing the wire order from M.G.’s account. (M.G. gave the FBI a version of this photograph, as well.)

f. Later that day, IGBOKWE let EROHA know that a “5k” payment for “dating” would come “[f]rom the same person.” He then provided EROHA with CHUKWUOCHA’s name and Wells Fargo bank account number.

g. On July 18, 2017, the day before the FBI executed search warrants at IRO’s apartment, IGBOKWE sent CHUKWUOCHA a photograph of a cash deposit of \$4,150 into a Wells Fargo account ending in in 5736, CHUKWUOCHA’s account. (As noted, bank records confirm a \$5,000 cash withdrawal that same day from EROHA’s bank account.) They then discussed that \$150 of that amount was for MACWILLIAM CHUKWUOCHA and that CHUKWUOCHA was paying “the guy” \$4,000, and they also discussed the exchange rate.

27. Victim Company 13—August 2017 BEC Fraud (involving IRO, CATHEY, UMEJESI, EKECHUKWU, IGBOKWE, and OGBUNGBE)

216. Victim Company 13, which is based in Dubai and sells chemicals related to oil extraction, was the victim of a BEC fraud on August 3, 2017, shortly after the government executed search warrants at IRO’s apartment. Victim Company 13 believed it was making a payment of \$382,295 to a Chinese company (“Chinese Company 3”) for supplies. It ultimately lost all of those funds.

217. An employee of Victim Company 13 was interviewed by an FBI agent. Based on that interview and documents provided, I know the following:

a. Unbeknownst to Victim Company 13 and Chinese Company 3 personnel, an unknown fraudster had hacked Victim Company 13’s email system, blocked its emails, and was communicating with both Victim Company 13 and Chinese Company 3 personnel using fraudulent email accounts at email domains created to closely resemble the legitimate email domains of Victim Company 13 and Chinese Company 3.

b. On August 2, 2017, an unknown fraudster sent Victim Company 13 personnel wiring instructions to make payments on to four invoices related to purchases of supplies—totaling \$382,295—from its bank account at Abu Dhabi Commercial Bank in Dubai to a Chase bank account ending in 5092, opened in the name of Chinese Company 3. That bank account had been opened by a money mule on July 11, 2017. Business licenses in names similar to the name of Chinese Company 3 were obtained from L.A. County on July 12 and June 20, 2017 by that money mule and another money mule.

c. On August 3, 2017, Victim Company 13 wired \$382,295 to the fraudulent Chase account opened in the name of Chinese Company 3. At the request of a fraudster, Victim Company 13 also provided a copy of the SWIFT confirmation for the wire on August 6, 2013.

d. On August 7, 2017, Chinese Company 3 discovered the fraud and informed Victim Company 13. Victim Company 13 contacted its bank to rescind the wire, but was informed that by that time the funds had been withdrawn.

218. Evidence in the phones indicates that, prior to execution of the search warrants at IRO's apartment, IRO coordinated with Coconspirator 24 regarding the fraud, and requested CATHEY, UMEJESI, and EKECHUKWU to open up bank accounts in furtherance of the fraud.

a. On July 9, 2017, Coconspirator 24 sent IRO messages saying, “[Chinese Company 3] [¶] 416460kg.” They went on to discuss the potential transaction, with Coconspirator 24 saying it would be “in 2weeks or less,” and IRO promising to “start the process tomo.”

b. On July 10, 2017, IRO asked CATHEY to open a bank account in Chinese Company 3's name, telling him that “Payment is Monnday/Tuesday.” IRO then asked him, “Can you open with chase??,” and CATHEY confirmed he could. IRO also suggested either “add[ing] it to [Indian Company 1] or FRESH FRUITS” or “do[ing] it separate.” (Indian Company 1 is an Indian equipment manufacturer. This name and the name “Fresh Fruit” are significant because accounts with both of those names received funds laundered from the Victim Company 13 fraud.)

c. Shortly after contacting CATHEY, IRO sent messages to EKECHUKWU saying, “[Chinese Company 3] [¶] If you can run it with citi...Wells...” EKECHUKWU responded, Ok wells . . . First thing in the morning, it will be done,” and, on July 12, 2017, provided IRO the information for an account ending in 4636 opened in Chinese Company 3's name at Wells Fargo in Los Angeles.

d. After contacting both CATHEY and EKECHUKWU, IRO sent messages to UMEJESI saying, “[Chinese Company 3] [¶] Open with boa or citi.”

e. On July 11, 2017, CATHEY provided the account information to IRO for the Chase account ending in 5092, opened in the name of Chinese Company 3, which IRO then relayed to Coconspirator 24.

f. On July 14, 2017, IRO sent the account information to UMEJESI, saying, “Abeg help me do it now. [¶] Tell them to put purpose of payment as. [¶] Payment for shipment. [¶] I gave you this acc to open but you could not.” Roughly an hour later, UMEJESI sent an

image to IRO, and IRO responded “Thank you sir.” While the image was not available from the conversation between IRO and UMEJESI, based on the filename IRO then sent that image to CATHEY. IRO then sent messages to CATHEY saying, “Paid in 2k [¶] Please call to confirm it.” On July 15, 2017, CATHEY said to IRO, “the money is confirmed in the account . . . The 2,000 that u put in.” IRO asked if “the card ready,” and then said, “If yes. You need to start using it. Start buying gas...food [¶] No shoes..no withdrawal... [¶] You know how we do it.”

i. Bank records confirm that \$2,000 was deposited to the Chase account ending in 5092, opened in the name of Chinese Company 3 on July 14, 2017, and that the account was used for cash withdrawals (contrary to IRO’s instructions) and purchases starting on July 19, 2017. It further appears that some of the purchases—two payments of \$27.50—were likely used to register businesses with L.A. County, based on the notation in the records.

g. On July 17, 2017, Coconspirator 24 said to IRO, “[Chinese Company 3] will happen dis week btw.” On July 18, 2018, about 12 hours before the FBI executed warrants on IRO’s apartment, Coconspirator 24 told IRO that “416460k” was coming from “Payer: [Victim Company 13] [¶] From [ADDRESS REDACTED] dubai [¶] Payee: [Chinese Company 3].” IRO sent that information, including part of his conversation with Coconspirator 24 to CATHEY, on July 18, 2017, to support an apparent call that CATHEY had with Chase regarding the account.

219. Bank account records indicate that IGBOKWE and OGUNGBE received laundered funds, as did accounts that CATHEY caused to be opened for IRO.

a. After the wire transfer on August 3, 2017, the funds were used to make a purchase at a Gucci store on August 4, 2017, and also purchase four cashier’s checks to the same individual totaling of \$34,658. On August 7, \$3,225.63 was withdrawn through a purchase at an Apple store, and \$3,000 was also withdrawn in cash.

b. In addition, starting on August 7, 2017, several additional cashier’s checks were purchased: \$47,606.40 in the name of a U.K. equipment manufacturing company, \$52,602

to Chinese Company 2, \$65,965 to Coconspirator 16 dba “Fresh Fruit,” \$35,000 to a name appearing to imitate the name of an Indian company (“Indian Company 2”), and two checks of \$35,000 in the name of Indian Company 1. Airline tickets were purchased on August 8, 2017, and on the next three days cash withdrawals were made, totaling \$8,000.

c. On August 10, 2017, an additional \$60,000 was wired to the BOA account ending in 2660 of IGBOKWE.

d. Bank records illustrate how IGBOKWE assisted in further laundering the funds. The records show that \$5,000 was withdrawn in cash over the next two weeks, starting with small withdrawals \$400, and that the rest of the money—\$54,600—was wired to OGUNGBE’s Chase account ending in 9931, dba “P and P Motors LLC,” on August 15, 2017.

i. In addition to bank records showing that the account was opened by OGUNGBE on July 27, 2016 and that it uses the name of his business, evidence on IRO’s Samsung shows OGUNGBE’s use of the account. In the conversation between IRO and OGUNGBE, on July 11, 2017, OGUNGBE provided the account information for that account including the account number and name of the account (in connection with the purchase of a 2013 Lexus RX for \$20,160), demonstrating OGUNGBE’s control of that account. (IRO then sent that account information to a relative.)

e. On August 16 and 22, 2017, the cashier’s checks written to Indian Company 1—a total of \$70,000—were deposited into the Chase account ending in 5812 opened in the name of Indian Company 1 by the same money mule who opened the Chase account ending in 5092 in the name of Chinese Company 3. The account in the name of Indian Company 1 was opened on June 6, 2017, and account information for that account was sent by CATHEY to IRO in June and July 2017, indicating that it was an account that they used and/or controlled. Most of the funds were withdrawn through cash withdrawals over a one-month period, while \$30,000 was withdrawn through a cashier’s check addressed in a name similar to that of an Ecuadorian seafood company.

28. Victim Company 14—January and February 2018 BEC Fraud (involving IRO and AJAEZE)

220. Victim Company 14 is a German company that was defrauded through a BEC scheme in which it believed it was paying for raw materials from a company in Mauritius (the “Mauritius Company”). Rather than going to the legitimate bank account of the Mauritius Company, the wires sent on January 18 and 30, 2018—\$76,688.99 (€4,350) and \$39,004.47 (€2,250), respectively—entered a Chase account ending in 0038.

221. While the payments occurred well after the FBI’s execution of search warrants at IRO’s apartment, and there is therefore no evidence on the phones regarding this specific transaction, evidence indicates AJAEZE’s and IRO’s involvement. The Chase account ending in 0038 was opened by AJAEZE in the name of the Mauritius Company, and the address for the account on file with Chase was IRO’s apartment in Carson, California. The funds were laundered through a set of retail purchases, wire transfers (related to automobiles and a tuition payment to The George Washington University), and cash withdrawals (including by IRO and AJAEZE).<sup>32</sup>

222. German authorities interviewed employees of Victim Company 14. Based on those interviews, and other records obtained by the FBI that I have reviewed, I know the following:

a. In January 2018, employees of Victim Company 14 were communicating by email with the general director of the Mauritius Company, about purchases of a raw material. At some point, an unknown fraudster who had evidently hacked the Mauritius Company’s email system began communicating with the Victim Company 14 employees using a similar email address at a different email domain. On or about January 15, 2018, the fraudster sent new wiring instructions to the Victim Company 14 employees, requesting that they make future payments to

---

<sup>32</sup> IRO’s conversation with AJAEZE also contained evidence of AJAEZE’s involvement in the conspiracy. One such conversation was described in n.6. Additionally, on July 10, 2017, IRO asked AJAEZE, “Can you just tell your wife to take you to chase to open just a checking and savings account today[?]” AJAEZE responded, “Naa [¶] She go suspect sir,” but suggested “Maybe your bro can take me” (an apparent reference to EROHA).

the Chase account ending in 0038 of AJAEZE, dba “[Mauritius Company],” which had been opened on January 12, 2018. (AJAEZE had also registered a company in the name of the Mauritius Company with L.A. County on January 12, 2018.)

b. On January 18, 2018, Victim Company 14 paid a wire of €64,350—amounting to approximately \$76,688.99—to the account. Bank records confirm the transaction and that the account balance was approximately \$6,000 at the time of the wire. They further indicate that, after the wire into the account, the funds were withdrawn over the next week. In particular, a wire of \$27,455 was paid to the Wells Fargo account of “Cadon Auto Corporation Inc.” on January 19, 2018, and a wire of \$51,865.00 was sent to a Mashreqbank PSC account of “Elite Auto Fze – UAE,” an account based in the United Arab Emirates.

c. Bank records also indicate there were cash withdrawals of \$500 each made at ATMs on January 22 and 23, 2018. Video from Chase on January 22, 2018, shows AJAEZE making a cash withdrawal from an ATM in Los Angeles, and IRO standing behind him. The video further shows AJAEZE handing at least part of the cash to IRO. Video from January 23, 2018 also shows AJAEZE making a cash withdrawal from an ATM in Carson, California, near IRO’s apartment.

d. On January 25, 2018, the fraudster sent Victim Company 14 an invoice for another payment. On January 30, 2018, Victim Company 14 paid a wire of €32,250—amounting to approximately \$39,004.47—to the Chase account ending in 0038 of AJAEZE. Bank records confirm the transaction and indicate that AZAEZE and IRO had depleted the funds in the account to \$1,940.17 at the time the wire reached the account.

e. Bank records and video show that the funds were depleted in a variety of ways. Bank records show that cash withdrawals of \$500 each were made on January 30, 2018 and February 5, 2018, and video from those dates shows AJAEZE making cash withdrawals at banks in Los Angeles and Carson, respectively.

f. Bank records also indicate that a wire of \$19,000 was made to the PNC Bank account of The George Washington University, listing a student’s name in the transaction

notes. Records from the university confirm that this payment was a tuition payment to the account of a student on February 1, 2018 for part of Spring 2018 tuition.

g. Bank records show that AJAEZE purchased a cashier's check of \$12,793 from the account on February 1, 2018. The withdrawal slip contained a teller's notation that AJAEZE provided his passport as identification, and the withdrawal slip noted the passport number and the expiration date.

h. Bank records also indicate that a cash withdrawal of \$2,000 was made from a bank branch in Carson, near IRO's apartment, on February 5, 2018.

29. Victim Company 15—February 2018 BEC Fraud (involving IRO, IKOGHO, and AJAEZE)

223. I and another FBI agent interviewed an attorney representing Victim Company 15 on March 6, 2018. Based on the interview and documents provided by the attorney, I know the following:

a. Victim Company 15, based in Indonesia, was a commodities trading company that was in email communication with a Hong Kong-based company ("Chinese Company 4") about a purchase of a commodity.

b. Victim Company 15 personnel had been communicating with a Chinese Company 4 employee, but, on February 14, 2018, an unknown fraudster used a similar email account to send fraudulent wire transfer instructions to Victim Company 15, directing its personnel to make a payment to a Chase Bank account that the fraudster claimed was in Hong Kong. It was, in reality, the Chase account ending in 0038 of AJAEZE.

224. Since the fraud on Victim Company 14, AJAEZE had added two additional business names to the account, after registering both as fictitious businesses with L.A. County—the name of a Minnesota-based fitness equipment manufacturer on February 1, 2018 and Chinese Company 4 on February 13, 2018. AJAEZE filed fictitious business name statements for both, as well. (In total, AJAEZE had nine businesses registered with L.A. County.) In addition to the

Chase account ending in 0038 listing IRO's address in the account records, the fictitious business statement for Chinese Company 4 also listed the street address of IRO's apartment as its address.

225. On February 14, 2018, just one day after AJAEZE added the name of Chinese Company 4 to the business checking account, Victim Company 15 wired \$886,950 to the Chase account ending in 0038. Chase records showed that multiple outbound wires sent the BEC victim funds out of the account shortly after Victim Company 15's funds were deposited into the account.

a. On February 15, 2018, \$84,985.00 was wired to a BOA account ending in 5903.

b. On February 16, 2018, \$189,000 was wired to a Compass Bank account ending in 3681, in the name of D&H Sales LLC, in Lynwood, CA 90262. Bank records indicate that this account was opened by IKOGHO and that the address on record was 17630 Crabapple Way, in Carson, California, which is IKOGHO's address (see paragraphs 37.a, 37.b, and 38). (Bank records also indicate numerous checks written from the account to IKOGHO, as well as having checks from and to OJIMBA after the account had apparently been frozen.)

c. Additionally, on February 16, 2018, \$8,000 was withdrawn as cash from the business checking account, and \$500 was withdrawn from an ATM in Los Angeles.

226. As noted earlier, AJAEZE used and controlled the Chase account ending in 0038, sometimes in conjunction with IRO. Additional evidence indicates that AJAEZE specifically conducted the transactions on February 16 and 17, 2018. Surveillance photographs from February 16, 2018, show AJAEZE inside a Chase bank branch located in Carson. In the photos, he was speaking with a teller and was on his cell phone. On February 17, 2018, video footage showed AJAEZE visiting a Chase ATM in Los Angeles.

227. As to the \$189,000 that was deposited in IKOGHO's Compass Bank account ending in 3681 on February 16, 2018, the balance of that account was \$163.42 at the time the wire entered the account. Compass Bank records indicate that two checks cleared from the

account on that date, one of which account records further indicate was cashed for \$8,000, and a second of which was written as a \$35,000 cashier's check.

30. Victim Company 16—February 2018 BEC Fraud (involving IRO and AJAEZE)

228. I reviewed a statement by T.H., the owner of Victim Company 16, from September 2018, which was provided by U.K. law enforcement. I also interviewed the CEO of a Washington-based company (the "Washington Company") that was engaged in a business transaction with Victim Company 16. Based on these interviews and relevant documents provided by both, I know the following:

a. Victim Company 16 is a U.K. company that buys and sells collectible vehicles. In February 2018, T.H. was in email contact with the CEO of the Washington Company and agreed to the sale of rare racecar. Victim Company 16 agreed to pay the Washington Company \$1.75 million.

b. On February 15, 2018, T.H. wired approximately \$1,750,000 from his account at National Westminster Bank PLC to the Wells Fargo bank account ending in 1849 of AJAEZE, opened in the name of a high-end Parisian jeweler, which T.H. had been provided on February 14, 2018. The email T.H. received was from an email address at a fraudulent domain that had been designed to resemble the name of the CEO of the Washington Company, and it indicated that the bank account was located in Sacramento, California. Records from Wells Fargo indicate that AJAEZE opened this account on January 22, 2018, in Carson, California, using his Nigerian passport as identification.

229. Bank records indicate that, at the time that the funds from Victim Company 16 were deposited into AJAEZE's Wells Fargo bank account ending in 1849, the balance was approximately \$809.78. On the days following the funds coming in, several debit card purchases were made using the funds. Then, on February 20, 2018, AJAEZE made three online transfers of \$200,000; \$500,000; and \$500,000 to a Wells Fargo account ending in 7748, opened by AJAEZE with a business name similar to that of the Washington Company. Records from the

L.A. County Recorder indicate that AJAEZE filed a fictitious business name statement for that name on February 13, 2018.

230. Prior to AJAEZE making the wires to the Wells Fargo account ending in 7748, T.H. and the CEO of the Washington Company discovered the fraud on February 17, 2018 and both contacted their banks to reverse the wire. On February 21, 2018, Wells Fargo froze the funds and returned the wires, including the wires that had been sent to AJAEZE's Wells Fargo account ending in 7748.

231. A Financial Crimes Consultant for Wells Fargo informed me that he attempted to speak to AJAEZE about the wires but did not reach him. He further stated that AJAEZE called the Wells Fargo call center on February 21, 2018, and call notes indicate that AJAEZE was "rude, unprofessional, and complaining" about the money being frozen, saying that it was his money.

#### IV. CONCLUSION

232. For all the reasons described above, there is probable cause to believe that the defendants have committed violations of 18 U.S.C. § 1956(h) and 18 U.S.C. § 1349.

  
\_\_\_\_\_  
KIMBERLY C. ANDERSON,  
Special Agent  
Federal Bureau of Investigation

Subscribed to and sworn before me  
this 31st day of May, 2019.

**JEAN P. ROSENBLUTH**

\_\_\_\_\_  
HONORABLE JEAN P. ROSENBLUTH  
UNITED STATES MAGISTRATE JUDGE