# IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA \*

\*

v. \* CRIMINAL NO. PWG-17-661

\*

ALDRIN FON FOMUKONG, et al.

\*

\*\*\*\*\*

## **GOVERNMENT'S MEMORANDUM IN AID OF SENTENCING**

The United States of America, by and through its undersigned counsel, hereby submits its memorandum in aid of sentencing. This memorandum is intended to provide the Court with additional background regarding the conspiracies to which the defendants in the above-captioned case have pled guilty and the respective role of each defendant in this case.

#### A. Offense Conduct

Between at least February 2016 through July 2017, members of a large-scale business email compromise ("BEC") scheme based in South Africa and operating in Maryland and elsewhere in the United States victimized at least 13 individual and business victims located throughout the United States. Over the course of the conspiracy, the defendants fraudulently attempted to obtain over \$10.9 million and actually obtained at least \$4.2 million. Specifically, members of the conspiracy, many of whom were located in South Africa, compromised individual and business email accounts, gaining access to those accounts. The members then sent false wiring instructions to the victims' email accounts from spoofed email accounts. These spoofed email accounts resembled legitimate email accounts for title companies, vendors, and other businesses and individuals from whom the victims were expecting wire instructions. The

spoofed emails, however, contained bank accounts opened by the members of the conspiracy, including the defendants, in the name of fictitious businesses. These accounts are known as "drop accounts." The members of the conspiracy registered fictitious businesses (primarily in Maryland) and then opened or managed corresponding drop accounts, frequently opening up numerous bank accounts at different financial institutions in the same business name. The drop accounts, in turn, were used to receive millions of dollars from the victims using the false wire instructions.

Once the victims' funds were in the drop accounts, the members of the conspiracy, including the defendants, thereafter quickly dispersed the funds by using wires to transfer money to other accounts, by initiating account transfers to other accounts at the same bank, by withdrawing cash, by obtaining cashier's checks, and by writing checks to other individuals and entities. Many of the cashier's checks were negotiated outside of Maryland, such as Louisiana or Texas—states to which the members of the conspiracy traveled in order to cash the checks. The members of the conspiracy engaged in these transactions in order to promote the fraud and to disguise the nature, source and control of the victims' funds.

# B. Procedural Background

Based on the conduct described above, on March 12, 2018, a federal grand jury returned a superseding indictment charging six defendants – Aldrin Fomukong, Nkeng Amin, Carlson Cho, Yanick Eyong, Ishmael Ganda, and Izou Digifa (collectively "the defendants") – with Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h) (Count Two). Two defendants – Aldrin Fomukong and Nkeng Amin – were also charged with Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349 (Count One).

On or about May 21, 2018, Fomukong pled guilty to both Conspiracy to Commit Wire Fraud and Conspiracy to Commit Money Laundering. Nkeng Amin is expected to plead guilty to Conspiracy to Commit Wire Fraud and Conspiracy to Commit Money Laundering on January 2, 2019. Eyong, Cho, and Ganda each pled guilty to Conspiracy to Commit Money Laundering on July 16, 2018, August 6, 2018, and September 12, 2018, respectively. Digifa is scheduled for trial beginning June 25, 2019.

#### C. Relative Roles of Each Defendant

Aldrin Fomukong was the leader of the conspiracy in Maryland. Specifically, Fomukong recruited individuals such as Amin, Cho, Eyong, Ganda, Digifa and several others to open fictitious businesses and corresponding drop accounts in order to receive victim funds.

Fomukong provided the drop account banking information to other members of the conspiracy, including the co-conspirators in South Africa, who would insert that information into the fictitious wire instructions sent via the spoofed email accounts. Once the members of the conspiracy identified a victim, the co-conspirators would alert Fomukong that the funds were entering the drop accounts. Fomukong would then alert the defendants that the funds were entering their sham accounts. Once the money was in the drop accounts, Fomukong worked with the other members of the conspiracy, such as Amin, Cho, Eyong, Ganda and Digifa, to quickly remove the victim funds from the drop accounts. Fomukong gave his co-conspirators specific instructions on, for example, the amount of money to withdrawal, who to make the cashier's checks to, or how to get the money wired out of the country. (Many of these instructions came from Fomukong's co-conspirators located in South Africa.)

Fomukong's profit from the fraud was staggering. Of the over \$4 million obtained from

the 13 victims, Fomukong would typically keep some of the funds, give a portion of the funds to the other members of the conspiracy located in the United States (such as Amin, Cho, Eyong, Ganda, and Digifa), and send the rest to members of the conspiracy abroad. This arrangement was lucrative: not only did Fomukong keep cash obtained from the fraud, he also used approximately \$231,800 of victim funds to purchase a 2010 Mercedes 4-door Sedan, a 2011 Porsche 4-door sedan, a 2014 Land Rover, and a 2012 Bentley Continental.

Nkeng Amin was first recruited by Fomukong to open drop accounts and launder the victim funds. For example, as further explained below, Amin obtained a \$458,500 fraudulent wire transfer from Victim E into his drop account, and quickly dissipated the funds before the victim learned they were victimized. However, Amin's role in the conspiracy expanded and Amin began recruiting other individuals to open drop accounts on his behalf. Amin would then provide the drop accounts directly to Fomukong and other members of the conspiracy so that the drop accounts could be included in the fraudulent wire instructions. Indeed, Amin recruited Eyong to register a fictitious business, open corresponding drop accounts, and launder victim funds. Amin also communicated with Fomukong and Individual 7 to assist with laundering the funds deposited into Eyong's drop account. As a result, Amin caused an actual loss to Victims E, G, and K of over \$1 million and an intended loss of over \$6.7 million. Eyong caused an actual loss to Victims G and K of approximately \$693,000, and an intended loss of over \$6.2 million.

Carlson Cho, who resided in Massachusetts, was originally recruited by Fomukong to assist Fomukong with transferring large sums of victim funds out of the country. Cho was in a position to do so because he was a Bank of America employee and thus was able to authorize large international wire transfers. As such, Cho assisted Fomukong by wiring \$393,750 to a bank

account located in Cameroon and \$350,000 to a bank account located in South Africa, both of which came from Victims C and D. In addition, Cho recruited at least one other individual to open a drop account to receive victim funds. And, after receiving a \$227,000 wire transfer from Victim L, Cho and this recruited individual (with the assistance of Fomukong) flew from Massachusetts to Texas in order to make cash withdrawals and to obtain numerous cashier's checks (which were later cashed in Texas). Furthermore, Cho eventually began communicating directly with the co-conspirators in South Africa (cutting Fomukong out of the middle), and initiated wire transfers, using his position as a Bank of America employee, to launder over \$2 million of victim funds out of the country. In total, Cho caused an intended loss to Victims C, D, L, and M of over \$3.3 million.

Ganda's and Digifa's role was similar to Eyong's role, except they were recruited by Fomukong (as opposed to Amin) to register businesses and open corresponding bank accounts. These accounts then received victim funds, which Ganda and Digifa quickly dissipated by a series of transactions. In total, Ganda caused Victim H an actual and intended loss of over \$149,000. Digifa caused Victims B, F, H, I and J an actual loss of approximately \$237,800 and an intended loss of approximately \$454,800.

#### **D.** The Fraudulent Transactions

#### Victim A

Defendants: Fomukong

Date of Wire(s): June 23, 2016 and June 24, 2016 Intended Loss: \$47,000 and \$200,000 = \$247,000

*Actual Loss:* \$247,000

On February 2, 2016, Individual 1, at the direction of Fomukong, registered the fictitious business Syndicate Remera LLC in Maryland. On February 23, 2016, Individual 1, at the

direction of Fomukong, opened Capital One x4384 in the name of Syndicate Remera LLC. In June 2016, Victim A, a business located in California, fell victim to the defendants' BEC scheme. Specifically, an accountant for Victim A began receiving correspondence regarding a wire transfer from a fraudulent email address. As a result, on June 23, 2016, Victim A sent a fraudulent wire in the amount of \$47,000 to Capital One x4348. On June 24, 2016, Victim A sent another fraudulent wire in the amount of \$200,000 to Capital One x4384.

On June 24, 2016, Fomukong caused four separate cash withdrawals for a total of approximately \$40,000. Fomukong also obtained a cashier's check in the amount of \$10,000, made out to Fomukong; a \$51,000 cashier's check that Fomukong used to purchase a 2011 Porsche, as described above; and a cashier's check in the amount of \$29,000, made out to Fomukong.

### Victim B

Defendants: Fomukong, Digifa
Date of Wire(s): January 27, 2017
Intended Loss: \$165,179.30
Actual Loss: \$165,179.30

On November 14, 2016, Digifa, at the direction of Fomukong, registered Gryphson Renolt LLC in Maryland. On November 16, 2016, Digifa opened TD Bank x1076 in the name of Gryphson Renolt LLC.

On January 27, 2017, Victim B, a business located in Connecticut, sent a \$165,179.30 wire intended for a vendor. On January 5, 2017, Victim B had received a fraudulent email with the wire instructions to TD Bank x1076. Victim B sent the funds from their bank account to TD Bank x1076 on January 27, 2017. Victim B went to pay the vendor again in February 2017, and received an email with new wire instructions: Ramanson Grindoy LLC, Capital One x4547.

(This account was opened on February 1, 2017 by another individual involved in the defendants' conspiracy.) At this time, the vendor informed Victim B that their email had been compromised.

Following the \$165,179.30 wire into TD Bank x1076, Digifa wrote two checks: a \$60,050 check to Fomukong for "car purchase" and a \$98,450 check to Albanky Productions, a business registered to Fomukong. The \$60,050 check was deposited into Fomukong's bank account. The \$98,450 check was deposited into a bank account in the name of Albanky Production LLC, which was controlled by Fomukong. Fomukong then drew a \$17,299.94 check from that account to purchase a 2010 Mercedes, as described above.

## Victim C and Victim D

Defendants: Fomukong
Date of Wire(s): March 9, 2017

*Intended Loss:* \$875,000 and \$123,620.55 = \$998,620.55

*Actual Loss:* \$350,000

On February 21, 2017, Individual 2, at the direction of Fomukong, registered Chavez Investment LLC in Maryland. On February 21, 2017, Individual 2 opened Bank of America x9655 (BOA x9655) in the name of Chavez Investment Inc. Fomukong drove Individual 2 to register both the business and open the bank account, and provided Individual 2 with approximately \$100 to do so. On March 9, 2017, Victims C and D (a married couple) initiated two separate wire transfers in the amount of \$875,000 and \$123,620.55 to BOA x9655. Victims C and D received fraudulent wire instructions from an individual purporting to be their realtor, and thus believed they were wiring the \$998,620 to purchase a home.

After the fraudulent wire, Individual 2, at the direction of Fomukong and with the assistance of Cho (who was an employee of Bank of America at the time) thereafter caused a wire transfer in the amount of \$393,750 to a bank account located in Cameroon in the name of

Fomukong's mother, and a separate wire transfer in the amount of \$350,000 to be sent to a bank account located in South Africa in the name of Business 2. In addition, Fomukong withdrew \$500 in cash.

### Victim M

Defendants: Fomukong, Amin, Cho

 Date of Wire(s):
 April 12, 2017

 Intended Loss:
 \$2,085,050

 Actual Loss:
 \$2,085,050

On April 12, 2017, Individual 8 opened Bank of America x8581 (BOA x8581) in the name of Minnever S/A. On April 12, 2017, the account received an incoming wire transfer in the amount of \$2,085,050 from Victim M, a business located in Colorado. Beginning on April 19, 2017, Amin sent Fomukong the BOA x8581 account information, as well as identification documents for Individual 8. Amin also sent Fomukong a photo showing the balance of \$2,085,050 in the account. Amin and Fomukong also discussed Fomukong receiving 30% of the victim funds.

On April 19, 2017, and April 20, 2017, after receiving the \$2,085,050 wire transfer from Victim M into BOA x8581, Cho (using his position as a Bank of America employee) initiated the following wire transactions: (1) a \$250,000 wire to a bank account in the Czech Republic; (2) a \$500,000 wire to a bank account in South Africa; (3) a \$574,955 wire to a bank account in Poland; and (4) a \$760,000 wire to a second bank account in Poland.

8

## Victim E

Defendants: Fomukong, Amin
Date of Wire(s): May 2, 2017
Intended Loss: \$458,500
Actual Loss: \$328,737

On February 7, 2017, Amin registered the fictitious business JB Studios LLC in Maryland. On February 7, 2017, Amin opened Bank of America x9244 (BOA x9244) in the name of JB Studio LLC. On April 25, 2017, Amin provided Fomukong the account information for BOA x9244. On May 2, 2017, a co-conspirator caused Victim E to wire \$458,500 into BOA x9244, controlled by Amin. Victim E had received fraudulent wire instructions from the conspirators, who purported to be Victim E's realtor.

On May 3, 2017, after receiving the \$458,500 wire transfer from Victim E into BOA x9244, Amin made a \$220,000 wire transfer to Bank of America x3599 (BOA x3599), controlled by Individual 5. On May 3, 2017, Amin obtained from BOA x9244 a \$105,000 cashier's check made out to Business 3 and a \$98,000 check made out to Individual 6. On May 3, 2017, Fomukong used the \$105,000 cashier's check to purchase from Business 3 a 2012 Bentley Continental. On May 3, 2017, Amin made three separate cash withdrawals totaling \$8,000. Amin and Fomukong also made additional purchases debited from BOA x9244.

#### Victim F

Defendants: Fomukong, Digifa
Date of Wire(s): June 7, 2017

Intended Loss: \$50,703 Actual Loss: \$50,703

On May 22, 2017, at the direction of Fomukong, Digifa registered Mercatel Investment LLC in Maryland. Digifa then opened Suntrust Bank x4431 in the name of Mercatel Investment

LLC. Fomukong provided this banking information to his co-conspirators. On June 7, 2017, Victim F, a business located in Colorado, received fraudulent wire instructions from an email account purporting to be Victim F's customer. As a result, on June 7, 2017, Victim F sent a wire in the amount of \$50,703 to Suntrust x4431. Later, Victim F learned that an outside party breached the accounting manager's email address and added a "rule" to the mailbox wherein all emails that matched certain criteria would be automatically forwarded to a conspirator's email account. Additionally, the true emails would be forwarded to an inbox where they would go unnoticed. The outside party thereafter edited intercepted emails by changing the sender's email address and bank wire instructions. After the alteration, the fraudulent email was sent to the accounting manager, resulting in the wire transfer of \$50,703.00 to Suntrust x4431. On June 9, 2017, Victim F's client contacted Victim F about the wire they were expecting, but did not receive.

Following the wire transfer, on June 8, 2017, Fomukong purchased a train ticket for Digifa to travel from Virginia to Maryland. Once in Maryland, Digifa made a withdrawal of \$44,486, comprised of a \$39,486 check made out to a sham business and the remainder in cash. The \$39,486 check was later cashed in Louisiana. In addition, Fomukong made payments to his American Express and Citicard Online credit cards for approximately \$6,000.

#### Victim L

Defendants: Fomukong, Cho
Date of Wire(s): June 15, 2017
Intended Loss: \$227,000
Actual Loss: \$203,372

On June 7, 2017, at the direction of Cho, Individual 3 opened Bank of America x7760 in the name of a sham business. On June 16, 2017, Victim L, located in California, reported he had

been the victim of a BEC fraud scheme. Victim L was attempting to purchase a home in California, and believed he had sent \$227,000 to a title company in California to complete the purchase on June 15, 2017. He had unknowingly received false wiring instructions via email which resulted in him sending a false wire transfer in the amount of \$227,000 to Bank of America x7760 (BOA x7760).

On June 16, 2017, Victim L and his wife went to a Bank of America branch in California and attempted to stop the false wire transfer. However, before the wire transfer could be stopped, Cho purchased flights from Massachusetts to Texas for himself and Individual 3 using a debit card associated with BOA x7760. On June 16, 2017, in addition to smaller transactions, Cho and Individual 3 withdrew a total of \$202,200 from BOA x7760, comprised of a \$8,000 cash withdrawal, a \$9,200 cash withdrawal, a cashier's check in the amount of \$90,000 made out to Business 4, and a second cashier's check in the amount of \$95,000 made out to Business 4, all from Bank of America branches located in Texas. The two cashier's checks were subsequently negotiated in Houston, Texas.

#### Victim G

Defendants: Fomukong, Amin, Eyong

*Date of Wire(s): June 21, 2017* 

*Intended Loss:* \$6,000,000 (\$6 million)

*Actual Loss:* \$589,812

On June 15, 2017, at the direction of Amin, Eyong registered the fictitious business CL Escrow LLC in Maryland and provided the business registration documents to Amin. On June 16, 2017, Amin provided Fomukong the business registration documents. On June 17, 2017, Eyong opened Bank of America x0042 (BOA x0042). On June 21, 2017, Fomukong provided a co-conspirator the information for BOA x0042, including the bank name, account number,

account holder address, and business name (CL Escrow). On June 21, 2017, Fomukong provided Amin with Victim G's name, "reason for wire," and "reason for cashier's check." On June 21, 2017, a co-conspirator caused Victim G to wire \$6,000,000 into BOA x0042, controlled by Eyong. Specifically, an attorney for Victim G, a business located in Massachusetts, received fraudulent wire instructions related to a real estate purchase Victim G was attempting to make.

On June 21, 2017, after receiving the \$6,000,000 wire transfer from Victim G into BOA x0042, Eyong made a \$2,350,000 wire transfer to a bank account located in South Africa in the name of Business 5. On June 22, 2017, Amin and Eyong obtained three cashier's checks from BOA x0042, each for \$95,000 in the name of Business 6. Eyong and Amin also made a \$10,000 cash withdrawal and other purchases, and Fomukong paid off numerous credit card bills.

Fomukong also purchased (using victim funds) flight tickets for himself and Eyong to travel to Texas. On June 23, 2017, Eyong obtained three additional cashier's checks from BOA x0042 while in Texas. The cashier's checks were: a \$95,000 check in the name of Individual 7, a \$95,000 check in the name of Business 6. These checks were subsequently negotiated in Texas.

### Victim H

Defendants: Fomukong, Digifa
Date of Wire(s): June 23, 2017
Intended Loss: \$104,450

Actual Loss: \$0

Defendants: Fomukong, Ganda
Date of Wire(s): June 29, 2017
Intended Loss: \$149,226
Actual Loss: \$149,226

On August 8, 2016, Ganda opened Navy Federal Credit Union x3451 ("NFCU x3451"),

Navy Federal Credit Union x8060 ("NFCU x8060"), and Navy Federal Credit Union x5615 ("NFCU x5615"), all in the name of Giclef International LLC. Ganda also maintained personal accounts at Navy Federal Credit Union, namely an account ending in 3445 ("NFCU x3445") and an account ending in 3690 ("NCFU x3690").

Victim H was a resident of Colorado and the owner of a business. An employee of the business received emails from a co-conspirator, purporting to be Victim H and authorizing payments on invoices. As a result, on June 23, 2017 and June 29, 2017, Victim H initiated two separate wire transactions, respectively: (1) a \$104,450 wire to Capital One x3758, in the name of Mercatel Investment LLC, which was opened by Digifa; and (2) a \$149,226 wire to NFCU x3451, controlled by Ganda. The first wire transfer to Digifa was not successful. The second wire transfer to Ganda was successful.

After receiving the \$149,226 wire transfer, Ganda or Fomukong made the following transactions from the NFCU x3451 account:

6/30/17	\$3,003.54 POS Withdrawal at Shoppers Food in College Park, MD
6/30/17	\$50,000 transfer to NFCU x5615
6/30/17	\$2,300 ACH transfer to Fomukong's American Express account
6/30/17	\$10,000 cash withdrawal
7/3/17	\$600 transfer to NFCU x3445 [Ganda's personal account]
7/3/17	\$2,000 transfer to NCFU x3690 [Ganda's personal account]
7/3/17	\$18,158 transfer to NFCU x8060
7/3/17	\$32,000 transfer to NFCU x5615
7/3/17	\$670 ACH transfer to Fomukong's American Express account
7/3/17	\$10,000 cash withdrawal
7/3/17	\$15,000 cash withdrawal
7/5/17	\$820.23 POS Debit Payment to Comcast
7/5/17	\$2,263.80 POS Debit Payment to Iberostar Hotels
7/5/17	\$1,750 transfer to NFCU x3445 [Ganda personal account]

After receiving into NFCU x5615 the \$50,000 and \$32,000 wire transfers from NFCU

x3451 described above, Ganda or at some other times a co-conspirator, at the direction of Fomukong, made the following transactions from the NFCU x5615 account:

6/30/17	\$10,000 cash withdrawal
6/30/17	\$4,000 transfer to NCFU x3690 [Ganda personal account]
6/30/17	\$4,000 transfer to NFCU x8060
7/3/17	\$10,000 cash withdrawal
7/3/17	\$52,400 wire transfer to Bank of America account ending in 3862

After receiving into NFCU x8060 on or about June 30, 2017, the \$4,000 wire transfer from NFCU x5615 and the \$18,158 wire transfer from NCFU x3451, Ganda or at some other times a co-conspirator, at the direction of Fomukong, made the following transactions from the NFCU x8060 account:

6/30/17	\$3,003.54 POS Withdrawal at Shoppers Food in College Park, MD
7/3/17	\$18,000 cash withdrawal

## <u>Victim I and Victim J</u>

Defendants: Fomukong, Digifa

 Date of Wire(s):
 July 3, 2017

 Intended Loss:
 \$140,134.25

 Actual Loss:
 \$21,000

On May 22, 2017, Digifa registered Mercatel Investment LLC in Maryland. Mercatel Investment LLC was registered in the state of Maryland. That same day, Digifa opened (among other bank accounts) Bank of America x9237 in the name of Mercatel Investment LLC.

Victim I and Victim J were residents of Massachusetts and attempting to make a real estate purpose. Their lawyer, however, received false wiring instructions and, as a result, on July 3, 2017, wired \$140,134.25 to Bank of America x9237. Before the accounts were frozen, Fomukong purchased a train ticket for Digifa to travel from Virginia to Maryland. Once in Maryland, on July 5, 2017, Digifa (at the direction of Fomukong, who drove Digifa to the

various bank branches and waited outside) made three cash withdrawals at three different bank branches totaling \$21,000. In addition, Digifa attempted to make a \$35,000 wire transfer.

### Victim K

Defendants: Fomukong, Amin, Eyong

 Date of Wire(s):
 July 13, 2017

 Intended Loss:
 \$292,830.10

 Actual Loss:
 \$103,425

After Eyong registered the fictitious business CL Escrow LLC in Maryland, as described above, on June 19, 2017, Eyong opened TD Bank x3845. On July 13, 2017, a co-conspirator caused Victim K to wire \$292,830.10 into TD Bank x3845, controlled by Eyong. Victim K is a resident of California who was attempting to purchase a new home.

On July 14, 2017, Fomukong provided Amin an image of wire instructions related to a wire in the amount of \$292,830.10 from Victim K to TD Bank x3845. On July 14, 2017, after receiving the wire transfer from Victim K into TD Bank x3845, Amin and Eyong made a \$5,000 cash withdrawal from a TD Bank branch in Beltsville, Maryland. On July 14, 2017, Eyong made a separate \$5,000 cash withdrawal from TD Bank x3845 from a TD Bank branch in Laurel, Maryland. On July 14, 2017, Eyong obtained a \$58,500 check made out to Business 3, which Fomukong used to purchase a 2014 Land Rover. Fomukong also made numerous cash withdrawals from TD Bank x3845, as well as debit payments.

# E. Conclusion

The government hopes that this memorandum will be helpful to the Court with respect to the sentencing of the seven defendants in this case. The government will address, in more detail, the specific facts relating to each defendant at the sentencing of that defendant.

Respectfully submitted,

Robert K. Hur United States Attorney

By: \_\_\_/s/\_\_\_ Kelly O. Hayes Assistant United States Attorney