

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

ONWUCHEKWA NNANNA KALU

Defendant.

GRAND JURY ORIGINAL

VIOLATIONS:

18 U.S.C. § 371 (Conspiracy);
18 U.S.C. § 1343 (Wire Fraud);
18 U.S.C. § 1956 (Laundering of Monetary
Instruments);
18 U.S.C. § 2 (Aiding and Abetting,
Causing an Act to be Done)

FORFEITURE ALLEGATION:

18 U.S.C. § 981(a)(1)(C), 28 U.S.C.
§ 2461(c)

INDICTMENT

The Grand Jury for the District of Columbia charges:

Background

At all times material herein:

1. A business email compromise (“BEC”) is a scam targeting businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject or subjects compromise(s) legitimate business e-mail accounts through social engineering or computer intrusion techniques, and uses that compromise to misdirect a transfer of funds into accounts controlled by the subject(s).
2. Company A was an investment firm located in Boston, Massachusetts. Company A invests in other companies with the goal of improving human health in the areas of cardiovascular disease and stroke. Over the past twelve years, Company A has invested in 42 companies located in North America, Europe, and Israel. Employee A worked for Company A and reported to Director A-1. Director A-2 also worked for Company A.

3. Company B was a financial services company located in London, England, which processed fund transfers for a bank account held by Company A at BNY Mellon in the United States. Employee B worked for Company B and processed fund transfers for Company A at the direction of Director A-1.

4. Heart Monitor Company was located in Tel-Aviv, Israel. During July 2019, Company A planned to invest \$625,000 in Heart Monitor Company.

5. Defendant ONWUCHEKWA NNANNA KALU ("KALU") was a citizen of Nigeria who resided in Nigeria and had no known or last known residence in the United States.

COUNT ONE
(Conspiracy)

6. Paragraphs 1 through 5 of this Indictment are re-alleged.

7. The conduct alleged in this Count began and was committed outside of the jurisdiction of any particular State and district, and none of the offenders are known to have resided within any State or district. The conduct is therefore within the venue of the United States District Court for the District of Columbia, as provided by 18 U.S.C. § 3238.

8. From a time uncertain but by no later than July 9, 2019, and continuing until on or about July 19, 2019, KALU and others did knowingly conspire, combine, confederate, and agree with each other to violate:

- a. 18 U.S.C. § 1343, Wire Fraud, by, having devised and intending to devise any scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitting and causing to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, and attempting to do so; and
- b. 18 U.S.C. § 1956(a)(2)(A), Laundering of Monetary Instruments, by transporting, transmitting, and transferring, and causing to be transported, transmitted, and transferred, a monetary instrument and funds from a place

in the United States to a place outside of the United States and to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity, to wit, wire fraud, and attempting to do so.

Purpose of the Conspiracy

9. It was a purpose of the conspiracy for KALU and other conspirators to enrich themselves through a BEC scheme that targeted Company A.

Manner and Means

10. Among the manner and means by which KALU and other conspirators would and did carry out the objectives of the conspiracy were the following:

a. Unbeknownst to Employee A, all of Employee A's emails containing any of six words—capital, invoice, fund, pay, payment and wire—were forwarded to an external email account, george.morgan33333@gmail.com, which was controlled by the conspirators. The members of the conspiracy reviewed all of those emails from locations outside of the United States without authorization from Employee A.

b. The conspirators created a “spoofed” domain name for Company A (“SpoofDomain.org”) which differed from Company A's actual domain name by a single letter.

c. Using SpoofDomain.org, the conspirators created “spoofed” email accounts for Director A-1 and Director A-2 which differed from their real email addresses by only one letter.

d. The conspirators then used the spoofed email accounts to communicate with Company B and to direct Employee B at Company B in London, England, to misdirect transfers of Company A's money from its account at BNY Mellon to bank accounts outside of the United States controlled by the conspirators – rather than the intended recipients.

e. Once the members of the conspiracy had transferred the funds to financial institutions outside of the United States, the conspirators transferred some of those funds to bank accounts controlled by the conspirators at Bank of Africa in Nigeria.

Overt Acts

11. In furtherance of the conspiracy and to effect its objects and purposes, defendant KALU and other conspirators committed, and caused others to commit the following overt acts, among others:

(1) On or about July 9, 2019, a member of the conspiracy read the following email from Director A-1 to Employee B in London, England, with copies to Director A-2 and Employee A:

Hello [Employee B],

This morning [Heart Monitor Company] held a Board meeting . . . [Heart Monitor Company] has sent across the attached documentation. We have 14 days from this notice to wire funds [to Heart Monitor Company]. The amount listed in the investor schedule of \$625,000 is correct . . . [T]his should be deployed out of [Company A's account at BNY Mellon]. Please let me know if there is any other information you need to set this up.

(2) On or about July 9, 2019, a member of the conspiracy read the following email from Employee B in London, England, to Director A-1, Director A-2, and Employee A:

Thanks [Director A-1],

We will set the wire up for July 16 if that works for you. I note the bank details, the account number is different to [sic] the one we use for the first [investment] Tranche. We do not need any additional information.

(3) On or about July 9, 2019, a member of the conspiracy read the following email from Director A-1 to Employee B with copies to Director A-2 and Employee A: "Hi

[Employee B], Thank you. Yes – [Heart Monitor Company] made some changes to their banking recently so I’m not surprised it’s a new account.”

(4) On or about July 9, 2019, a member of the conspiracy read the following email from Employee B in London, England, to Director A-1, Director A-2, and Employee A: “Thanks [Director A-1]. I’ll call you at 9[:]30 tomorrow in that case. Regards, [Employee B.]”

(5) On or about July 9, 2019, a member of the conspiracy read the following email from Director A-1 to Employee B, Director A-2 and Employee A: “Perfect.”

(6) On or about July 9, 2019, a member of the conspiracy registered a spoofed domain name for Company A (“SpoofDomain.org”) which differed from Company A’s actual domain name by only one letter.

(7) On or about July 9, 2019, a member of the conspiracy created a spoofed email address for Director A-1 (“DirectorA1@SpoofDomain.org”) which differed from Director A-1’s actual email address by only one letter.

(8) On or about July 9, 2019, a member of the conspiracy created a spoofed email address for Director A-2 (“DirectorA2@SpoofDomain.org”) which differed from Director A-2’s actual email address by only one letter.

(9) On or about July 11, 2019, a member of the conspiracy created a PDF document that had the appearance of a letter from Banco Mercantile del Norte (“Banorte Bank”) in Mexico, but was fraudulent, which stated that Heart Monitor Company maintained an account at that bank (Account x-4084) under the name “Val Min S.A. de C.V” – an account controlled by the conspirators.

(10) On or about July 11, 2019, a member of the conspiracy sent the following email message from DirectorA1@SpoofDomain.org to Employee B, in London, England,

Employee A, and DirectorA2@SpooofDomain.org with a copy of the fraudulent wiring instructions to Banorte Bank attached:

Hello [Employee B],

This morning [Heart Monitor Company] held a Board meeting where the company decided and informed that they are revising Appendix 2 (Wire Instructions), as the previous account details in Appendix 2 can not [*sic*] receive funds at the moment. They have issued a signed revision as Appendix 2(i).

Appendix 2(i) with the new wire instructions hereby replaces Appendix 2.

Kindly find attached the revised documents. Please acknowledge receipt of this, and can you advise if you would be able to set up and process the wire by Monday 15th July? We await your feedback.

(11) On or about July 15, 2019, a member of the conspiracy caused Employee B, on behalf of Company A, to send \$625,000 from Company A's account at BNY Mellon to an account at Banorte Bank (Account No. x-4084) in the name of "Val Min SA de CV" – an account controlled by the conspirators.

(12) On or about July 15, 2019, having received confirmation from Employee B that a transfer from the account at BNY Mellon had been completed, a member of the conspiracy using the account DirectorA-1@SpooofDomain.org sent the following email to Employee B:

[Employee B], Thanks for the confirmation.

However we noticed you made a little error with the Account Name. Can you kindly refer to the revised Appendix 2i (find attached again), and inform your bank of the correct Account Name, so the wire can be successful.

(13) On or about July 16, 2019, after receiving an email from Employee B stating that the name on the transfer was correct and asking for confirmation that Heart Monitor Company had received the transfer, a member of the conspiracy sent an email from

DirectorA1@SpoofofDomain.org as follows: “Thanks for the information and correction. We would [*sic*] inform you as soon as [Heart Monitor Company] confirms receipt of the wire.”

(14) On or about July 16, 2019, a member of the conspiracy took a screenshot picture of a bank statement showing a deposit in the amount of \$625,000 from Company A.

(15) On or about July 16, 2019, a member of the conspiracy using the email account DirectorA1@SpoofofDomain.org informed Company B that Company A needed to make another transfer of \$625,000 for the benefit of Heart Monitor Company because the July 15 transfer would be returned:

[Heart Monitor Company] says because of the ongoing audit in Banorte Bank, the funds you wired will be returned to your [*sic*] BNY account within the next 7 days. This has put us all into pressure because we need funds to be cleared and value date on or before the 17th July.

[Heart Monitor Company] wants to provide another wire instruction to wire another \$625,000 for value date tomorrow while funds return to your [*sic*] BNY account within the next 7 days.

Kindly confirm if this can be done for value date 17th July 2019.

(16) On or about July 16, 2019, a member of the conspiracy reviewed the following email sent from Employee B to DirectorA1@SpoofofDomain.org:

Dear [Director A-1],

If you can confirm that you would like us to wire out a second payment, pending receipt of the first one back in, then we will do so. Given the time difference and short notice, we will likely not be able to wire for value 17th, but we will do whatever we can to expedite this.

(17) On or about July 16, 2019, a member of the conspiracy created a fraudulent PDF document which appeared to be from HSBC indicating that Heart Monitor Company had an account at HSBC Mexico (Account No. x-3268) under the name “Clamour Robotics S.A. de C.V” – an account controlled by the conspirators.

(18) On or about July 16, 2019, a member of the conspiracy using the email account DirectorA1@SpooofDomain.org sent the following email to Employee B which attached the fraudulent PDF document attachment with copies to Employee A and DirectorA2@SpooofDomain.org:

Hi [Employee B],

This is to confirm that you should wire out a second payment, pending receipt of the first one back. Attach [*sic*] is the wire instructions . . . Please try your best as discussed so value 17th July.

...
Sorry for all the inconveniences and thanks again for your help so we can close this out.

(19) On or about July 17, 2019, a member of the conspiracy caused Employee B with Company B, on behalf of Company A, to send \$625,000 from Company A's account at BNY Mellon to a bank account in the name "Clamour Robotics SA de CV" at HSBC Mexico – an account controlled by the conspirators.

(20) On or about July 17, 2019, a member of the conspiracy took a screenshot of a bank statement showing a deposit from Company A on that same date.

(21) On or about July 18, 2019, a member of the conspiracy caused \$250,000 to be transferred from the account at HSBC Mexico (Account No. x-3268) to and through the United States to a bank account at the United Bank for Africa in Lagos, Nigeria, in the name of "Anumudu Brothers Sons Enterprises."

(22) On or about July 19, 2019, a member of the conspiracy caused \$244,311 to be transferred from the account at HSBC Mexico (Account No. x-3268) to and through the United States to a bank account at the United Bank for Africa in Lagos, Nigeria, in the name of "Mosky Enterprises and Autos LTD."

(Conspiracy to Commit Wire Fraud and Laundering of Monetary Instruments, in violation of 18 U.S.C. § 371)

COUNTS TWO AND THREE
(Wire Fraud)

12. Paragraphs 1 through 10 of this Indictment are re-alleged.

13. On or about the following dates, KALU and his conspirators, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice:

COUNT	DATE	TRANSMISSION IN INTERSTATE AND FOREIGN COMMERCE
2	July 11, 2019	Email from DirectorA1@SpoofDomain.org with wiring instructions for bank account in the name of Val Min SA de CV at Banorte Bank in Mexico (Overt Act 10)
3	July 16, 2019	Email from DirectorA1@SpoofDomain.org with wiring instructions for a bank account in the name of Clamour Robotics SA de CV with HSBC in Mexico (Overt Act 18)

(Wire Fraud, in violation of 18 U.S.C. § 1343)

COUNTS FOUR THROUGH SEVEN
(Laundering of Monetary Instruments)

14. Paragraphs 1 through 10 of this Indictment are re-alleged.

15. On or about the following dates, KALU and his conspirators transported, transmitted, and transferred, and caused to be transported, transmitted, and transferred, a

monetary instrument and funds from a place in the United States to and through a place outside of the United States and to a place in the United States from and through a place outside of the United States with the intent to promote the carrying on of specified unlawful activity, to wit, wire fraud, and attempted to so:

COUNT	DATE	MONETARY INSTRUMENT AND FUNDS
4	July 15, 2019	Transfer of \$625,000 from Company A's account at BNY Mellon to a bank account in the name of "Val Min SA de CV" at Banorte Bank in Mexico (Overt Act 11)
5	July 17, 2019	Transfer of \$625,000 from Company A's account at BNY Mellon to a bank account in the name Clamour Robotics SA de CV at HSBC Mexico (Overt Act 19).
6	July 18, 2019	Wire transfer in the amount of \$250,000 from an account in the name of Clamour Robotics SA de CV at HSBC Mexico to and through the United States to a bank account in Nigeria (Overt Act 21)
7	July 19, 2019	Wire transfer in the amount of \$244,311 from an account in the name of Clamour Robotics SA de CV at HSBC Mexico to and through the United States to a bank account in Nigeria (Overt Act 22)

(Laundering of Monetary Instruments, in violation of 18 U.S.C. § 1956(a)(2)(A); Aiding and Abetting, and Causing an Act to be Done, in violation of 18 U.S.C. § 2)

FOREFEITURE ALLEGATION

16. Paragraphs 1 through 15 of this Indictment are re-alleged for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).


17. Upon conviction of the offenses in violation of Title 18, United States Code, Sections 371, 1343, and 1956 set forth in Counts One through Seven of this Indictment the defendant, KALU, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense(s). The property to be forfeited includes, but is not limited to, the following: Money Judgment in the amount of \$1,250,000.

18. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

(Forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))



CHANNING D. PHILLIPS
Acting United States Attorney
for the District of Columbia

A TRUE BILL

Foreperson
Date: