

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division**

UNITED STATES OF AMERICA)

v.)

OLABANJI OLADOTUN EGBINOLA)

Defendant)

Case No. 3:19-mj-224



**AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION OF
OLABANJI OLADOTUN EGBINOLA**

I, Brian R. Hood, being duly sworn, state that:

1. I am a citizen of the United States of America and a resident of the Commonwealth of Virginia. I make this affidavit in support of the request of the United States of America to the United Kingdom of Great Britain and Northern Ireland for the extradition of Olabanji Oladotun Egbinola, a dual citizen of the United Kingdom and Nigeria.

2. I graduated from the Georgetown University Law Center in 1994. From 1999 to the present, I have been employed by the United States Department of Justice as an Assistant United States Attorney for the Eastern District of Virginia. My duties are to prosecute persons charged with criminal violations of the laws of the United States. During my practice as an Assistant United States Attorney, I have become knowledgeable about the criminal laws and procedures of the United States.

3. In the course of my duties, I have become familiar with the charges and evidence in the case of United States v. Egbinola, Criminal No. 3:19-mj-224, filed in the United States District Court for the Eastern District of Virginia.

4. The charges in Egbinola follow an investigation by the Federal Bureau of Investigation (“FBI”), which revealed that from on or about September 26, 2018, through on or about December 26, 2018, Olabanji Oladotun Egbinola, a dual Nigerian-UK citizen, conspired with others to defraud Virginia Commonwealth University of \$469,819.49 and to launder the proceeds of fraud.

SUMMARY OF THE FACTS OF THE CASE

5. Business email compromise (“BEC”) fraud schemes come in a variety of forms, but all have in common the perpetrators’ use of emails and social engineering to impersonate a party in a business transaction. When the impersonation is successful, the perpetrators convince victims to send money to bank accounts that the perpetrators control. Victims of BEC schemes typically include state and local government agencies, universities and businesses.

6. Virginia Commonwealth University (“VCU”) is a public university located in Richmond, Virginia, and within the jurisdiction of the United States District Court for the Eastern District of Virginia. On September 26, 2018, an individual using the name “Rachel Moore” contacted an employee in VCU’s procurement department using the email address accounts@kjellstromleegroup.com. As detailed further below, the domain name associated with accounts@kjellstromleegroup.com is purposefully very similar to the actual email domain name for Kjellstrom and Lee, Inc., which is a large construction company located in Richmond, Virginia, and which has completed construction projects for multiple universities including

VCU. “Rachel Moore” advised the procurement department employee that the bank account on file for receiving payments was currently being audited and inquired if the next payment could be sent to another bank account. From October 4, 2018, through December 10, 2018, “Rachel Moore” repeatedly emailed back and forth with the VCU employee, using a variety of social engineering techniques that convinced the VCU employee that the sender worked for the accounting department at Kjellstrom and Lee. “Rachel Moore” persuaded the VCU employee that Kjellstrom and Lee had signed up to receive payments in the form of ACH transactions¹ to an account with the Bank of Hope located in Los Angeles, California.

7. On December 20, 2018, VCU initiated a payment via ACH wire transfer for \$469,819.49 from their bank account to a particular Bank of Hope account as requested in the ACH setup form provided by “Rachel Moore.” On January 3, 2019, VCU was contacted by their bank, which raised concerns that the December 20, 2018 wire transfer was fraudulent. VCU contacted Kjellstrom and Lee and learned the construction company did not have an employee named “Rachel Moore,” nor had any employee taken action to establish ACH wiring procedures to receive payments from VCU.

8. The December 20, 2018 wire from VCU appeared in the Bank of Hope account the next day, December 21, 2018. At the time the VCU wire posted, the account was overdrawn and had a balance of -\$246.64. Over the next three days, from December 21 to December 24, 2018, the authorized signer(s) for this account initiated four wire transfers and wrote 38 checks

¹ In banking, ACH stands for Automated Clearing House, which is a network that coordinates electronic payments and automated money transfers. ACH is a way to move money between banks without using paper checks, wire transfers, credit card networks, or cash.

totaling \$452,736.90, or approximately 96% of the \$469,819.49 received from VCU. These payments involved 25 different payees, many of whom appeared to be clothing and textile companies located in Los Angeles, California. Of the 38 checks written on the Bank of Hope account, 22 checks were for amounts between \$7,000 and \$9,840, which is indicative of efforts to circumvent currency-reporting requirements for transactions over \$10,000. The majority of the wire transfer by VCU could not be recovered and was a loss for the university.

9. Bank records obtained from Bank of Hope for the account that received the wire transfer from VCU showed that the account was opened by a subject, identified herein as “S.C.,” in the name of EDHD, Inc. Those records further showed that EDHD, Inc. was incorporated by a second subject, identified herein as “H.C.,” who is the father of S.C.

10. FBI agents interviewed S.C. and H.C. on February 25 and March 1, 2019, respectively, in Los Angeles, California. Investigators learned that S.C. opened the account at H.C.’s direction. During his interview with investigators, H.C. acknowledged receiving the \$469,819.44 wire. According to H.C., sometime in January 2019 “two white men” walked into his company at EDHD Inc., located at 825 E. 29th Street, Los Angeles, California, and asked to go into business with him. H.C. claimed that he had never met those men before, and did not recall their names, phone numbers or any other contact information. H.C. said that he gave his Bank of Hope account information to these individuals in the form of a voided check, and believed they were investors who wanted to invest in his company. Shortly thereafter, the \$469,819.44 wire transfer was deposited into his account. H.C. said he had several outstanding debts and therefore did not ask questions about the source of the funds. H.C. admitted during his interview that he had used an ink stamp with S.C.’s signature to endorse the checks, and that

he had directed his son S.C. to make the four wire transfers out of the account immediately after receiving the incoming \$469,819.44 wire transfer.

11. A review of publicly available information, as well as records obtained pursuant to legal process, determined that the “kjellstromleegroup.com” domain associated with the fraudulent emails to VCU was registered by NameCheap, Inc. (“NameCheap”), which is an accredited Internet domain name registrar. NameCheap also provided email services for the kjellstromleegroup.com domain. Records provided by NameCheap revealed that kjellstromleegroup.com was registered by someone using the NameCheap username “bridgetclark” on September 26, 2018, which was the same day that VCU received the first fraudulent email message from “Rachel Moore” using email address accounts@kjellstromleegroup.com.

12. NameCheap’s records show that the “bridgetclark” account was opened on March 13, 2017. These records further show that the NameCheap user “bridgetclark” had registered more than 60 domains incorporating deceptively subtle variations on the true Internet domain names belonging to legitimate construction companies.

13. Records obtained from NameCheap indicate that the subject(s) using the “bridgetclark” account used technological means to conceal their true location(s). Many of the IP addresses used to login to the “bridgetclark” account resolved to US-based networking providers that rent virtual private servers (VPS), provide virtual private network (VPN) services, and resell their IP address space to other VPN providers. By design, VPNs and VPSs provide encryption and privacy that enable users to transmit data securely across open networks without revealing their true location or the contents of those communications. Many also accept

payment in various forms of cryptocurrency, such as Bitcoin, which further obscures the identity of the account holder. In fact, the “bridgetclark” NameCheap account was paid for using Bitcoin.

14. Numerous other IP addresses used to log into the “bridgetclark” account resolved to Internet service providers in the United Kingdom, including many cellular data companies. Prepaid cellular data plans are difficult to trace due to the multitude of ways the service can be paid for without having to use identifying payment methods such as credit cards in true name. Due to network engineering considerations, many cellular providers route multiple customers’ data through a single IP address at any given time, which significantly complicates the ability of investigators to pinpoint the correct device that is associated with a specific Internet communication. Many cellular providers maintain logs for relatively short periods, making it difficult to obtain the assistance of foreign law enforcement in time to contact the carrier and obtain identifying subscriber records.

15. Based on this evidence of technological obfuscation, along with the unknown identity and location of the perpetrator using accounts@kjellstromleegroup.com, on February 12, 2019, the Honorable David J. Novak, United States Magistrate Judge for the United States District Court for Eastern District of Virginia, issued a search warrant for electronic data.

16. On February 13, 2019, an FBI special agent sent an email containing an attached document to accounts@kjellstromleegroup.com from an account that appeared to be associated with VCU. FBI investigators determined that someone accessed the email account and opened the attached document from an Internet account with IP address 86.191.189.88. Public source information indicated that British Telecomm (“BT”) owned this IP address.

IDENTIFYING EGBINOLA

17. FBI investigators provided information to British criminal investigators relating to UK-based IP addresses used to access the “bridgetclark” NameCheap account as well as information gathered during the course of the FBI’s investigation. The 86.191.189.88 IP address, at the relevant time, was subscribed to a BT customer identified as Samiat Egbinola (Egbinola’s wife) of 56 Francisco Close, Chafford Hundred, Essex, RM16 6YD. Also residing at that address is Olabanji Oladotun Egbinola.

18. Olabanji Oladotun Egbinola has a history of convictions for fraud crimes and connection to fraud-related activities in the United Kingdom. He has a 2008 conviction for Possession of Control Articles in Use of Fraud, which involved money laundering a large quantity of U.S. dollars and Egbinola’s possession of a computer with bank account information for up to 80 who were victims of fraud. Egbinola also has convictions in 2000, for Theft and Fraud by False Rep – Using False Instrument with Intent to Be Accepted as Genuine, and in 1999, for Using False Instrument with Intent to Be Accepted as Genuine.

19. Egbinola also has links to other known BEC bad actors. U.S. government records show that, during two prior trips to Los Angeles, California, in 2015 and 2019, Egbinola listed the personal email address aegbinola@gmail.com on government travel documents. Evidence obtained pursuant to a search warrant for the aegbinola@gmail.com account shows that Egbinola exchanged multiple emails with johnedwards79@yahoo.co.uk. Investigators know that the latter account has been used as an integral part of a separate but similar BEC fraud scheme being prosecuted in U.S. District Court for the Western District of North Carolina. Evidence obtained by investigators there revealed that a British citizen, Oludayo Kolwole

Adeagbo,² managed the johndwards79@yahoo.co.uk account, which contained emails with invoices from a company that sold construction project information, as well as emails from a VPN provider.

PROCEDURAL HISTORY OF THE CASE

The Charging Process

20. Outside the context of a negotiated guilty plea between the defendant and the government, under the federal law of the United States there are two ways to commence a criminal prosecution. The first is by indictment. An indictment is a charging document that is issued by a grand jury after considering evidence in a case and finding that there is probable cause that the named defendant committed the offense(s) listed in the indictment. The United States' Constitution creates the express requirement that “[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury....” While the grand jury is technically an arm of the court, it is an independent body composed of private citizens—not less than 16 and not more than 23 people—whom the United States District Court has selected at random from the residents of the judicial district in which the court resides. The purpose of the grand jury is to review the evidence of crimes, including sworn testimony, presented to it by United States law enforcement authorities. After independently reviewing this evidence, if at least 12 jurors find that the evidence provides probable cause to believe that a

² On April 17, 2019, a grand jury sitting in U.S. District Court for the Western District of North Carolina returned an indictment, criminal case number 5:19-CR-34-FDW, charging Adeagbo and another British citizen, Donald Ikenna Echeazu, with: 1) conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349; 2) conspiracy to commit money-laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i), 1956(h), and 1957(a); and 3) aiding and abetting aggregated identity theft, in violation of Title 18, United States Code, Sections 2 and 1028A(a)(1).

particular person committed the crime, the grand jury may return an indictment that formally charges the person, who is now the defendant, thereby initiating criminal proceedings. Once the indictment is filed with the court, the clerk of the court, at the direction of a judge, normally issues a warrant for the defendant's arrest.

21. The second way to commence a federal criminal prosecution is by criminal complaint, which is a written statement of the essential facts constituting the offense charged. To obtain a complaint, an affiant must swear to the written statement of facts under oath before a magistrate judge or, if none is reasonably available, before a state or local judicial officer. The written statement of facts establishing probable cause that the named defendant committed the charged offense is typically contained in a separate affidavit accompanying the criminal complaint.

22. On December 19, 2019, a criminal complaint, case number 3:19-mj-224, was filed in the United States District Court for the Eastern District of Virginia, charging Egbinola with criminal offenses against the laws of the United States.

23. It is the practice of the United States District Court for the Eastern District of Virginia to retain the original criminal complaint and file it with the records of the court. Consequently, I have obtained a copy of the criminal complaint from the clerk of the court and have attached it to this affidavit as **Exhibit A**.

24. On December 19, 2019, based on the criminal complaint, the United States District Court for the Eastern District of Virginia issued an arrest warrant for Egbinola. It is the practice of the United States District Court for the Eastern District of Virginia to retain the original arrest warrant and file it with the records of the court. I have therefore obtained a copy

of the arrest warrant from the clerk of the court and have attached it to this affidavit as

Exhibit B.

The Charges and Pertinent United States Law

25. The criminal complaint charges in four counts that Egbinola committed the following offenses:

- Count 1: Wire Fraud, in violation of Title 18, United States Code, Section 1343, which carries a maximum penalty of 20 years' imprisonment;
- Count 2: Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349, which carries a maximum penalty of 20 years' imprisonment;
- Count 3: Money Laundering, in violation of Title 18, United States Code, Section 1956(a)(1), which carries a maximum penalty of 20 years' imprisonment; and
- Count 4: Conspiracy to Commit Money Laundering, in violation of Title 18, United States Code, Section 1956(h), which carries a maximum penalty of 20 years' imprisonment.

26. The United States requests the extradition of Egbinola for all of these offenses.

Each count charges a separate offense. Each offense is punishable under a statute that: 1) was the duly enacted law of the United States at the time the offense was committed; 2) was the duly enacted law of the United States at the time the criminal complaint was filed; and 3) is currently in effect. Each offense is a felony offense punishable under United States law by more than one year of imprisonment. I have attached copies of the pertinent sections of these statutes and the applicable penalty provisions to this affidavit as **Exhibit C**.

27. Count One charges Egbinola with wire fraud in violation of Title 18, United States Code, Section 1343. The two elements the government must prove to convict the defendant of wire fraud are: 1) that the defendant devised or intended to devise a scheme to

defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises that were material; and 2) that for the purpose of executing the scheme, the defendant transmitted or caused to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce any writings, signs, signals, pictures, or sounds.

28. Count Two charges Egbinola with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349. To satisfy its burden of proof and convict someone of wire fraud conspiracy, at trial the government must establish that: 1) two or more persons entered an agreement to commit the underlying offense (i.e., wire fraud); 2) each defendant joined the conspiracy to commit the underlying offense; and 3) each defendant did so with the intent to further its unlawful purpose.

29. Under United States law, a conspiracy is an agreement to commit one or more criminal offenses. The agreement on which the conspiracy is based need not be expressly written or spoken, but may simply be a tacit understanding by two or more persons to do something illegal. Criminal conspirators enter into a joint venture in which each participant becomes a partner or agent of every other member. A conspirator need not have full knowledge of all the unlawful scheme's details or every co-conspirator's identity. If a person understands the unlawful nature of a plan, and knowingly and willfully agrees to it, he is guilty of conspiracy, even when he belatedly joins or plays a minor part in the conspiracy. A conspirator can be held responsible for all reasonably foreseeable actions undertaken by others in furtherance of the conspiracy. Because of the nature of this criminal partnership, statements made by a conspirator

during the course of and in furtherance of the conspiracy are admissible against all conspiracy members, not just the declarant.

30. The crime of conspiracy is an independent offense, separate and distinct from the commission of any specific “substantive crimes.” Consequently, a conspirator can be found guilty of the crime of conspiracy to commit an offense even where the substantive crime that was the purpose of the conspiracy is not committed. The Congress of the United States has deemed it appropriate to make conspiracy, standing alone, a separate crime, even if the conspiracy is not successful, because collective criminal planning poses a greater threat to the public safety and welfare than individual conduct and increases the likelihood of success of a particular criminal venture.

31. Regarding Counts One and Two, the government’s evidence will establish that Egbinola controlled the email account accounts@kjellstromleegroup.com that was used to impersonate “Rachel Moore” with the Kjellstrom and Lee construction company and trick employees of VCU into wiring \$469,819.49 to a bank account that the conspiracy members controlled. The government’s evidence will further establish that the conspirators used a NameCheap account under the name “bridgetclark” to register more than 60 Internet domain names that were deceptively similar to the true Internet domains for various construction companies, including Kjellstrom and Lee. The government will prove this with testimony from employees of VCU and Kjellstrom and Lee, bank records, Internet business records and computer forensics.

32. Count Three charges Egbinola with money laundering, in violation of Title 18, United States Code, Section 1956(a)(1). To prove the defendant guilty of money laundering, the

government must prove the following four elements: 1) that the defendant conducted or attempted to conduct a financial transaction having at least a minimal effect on interstate commerce or involving the use of a financial institution which is engaged in, or the activities of which have at least a minimal effect on, interstate or foreign commerce; 2) that the property that was the subject of the transaction involved the proceeds of specified unlawful activity; 3) that the defendant knew that the property involved represented the proceeds of some form of unlawful activity; and 4) that the defendant engaged in the financial transaction with the intent to promote the carrying on of specified unlawful activity.

33. “Financial transaction” as defined in Title 18, United States Code, Section 1956(c)(4), means a transaction which in any way or degree affects interstate or foreign commerce involving the movement of funds by wire or other means or involving one or more monetary instruments.

34. The definition of “specified unlawful activity” is given in Title 18, United States Code, Section 1956(c)(7), which lists several categories of offenses that constitute “specified unlawful activity.” Wire fraud is included as a “specified unlawful activity” under Title 18, United States Code, Section 1956(c)(7)(A), which in turn incorporates the list of “racketeering activities,” including wire fraud, set forth in Title 18, United States Code, Section 1961(1).

35. Count Four charges Egbisola with conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h). To satisfy its burden and convict someone of this offense, the government must prove that: 1) a conspiracy, agreement, or understanding to commit money laundering was formed or entered into by two or more persons at or about the time alleged; 2) at some time during the existence or life of the conspiracy,

agreement, or understanding, the defendant knew that the property involved represented the proceeds of some form of specified unlawful activity; and 3) the defendant knowingly and voluntarily joined the conspiracy, agreement, or understanding.

36. For Counts Three and Four, the government's evidence will establish that Egbinola persuaded employees of VCU to wire \$469,819.49 to a Bank of Hope account controlled by an individual identified as "H.C." The Bank of Hope account received that wire on December 21, 2018. From December 21, 2018, through December 24, 2018, two authorized signers for this account initiated four wire transfers and wrote 38 checks totaling \$452,736.90, or approximately 96% of the \$469,819.49 received from VCU. These payments involved 25 different payees, and the majority were for amounts close to but less than \$10,000 in what appears to have been an effort to avoid currency transaction reporting requirements under United States federal law. The government will prove this with bank records, Internet business records, computer forensics, testimony from S.C., and testimony from FBI investigators pertaining to an interview conducted with H.C.

Description of Fugitive

37. Olabanji Oladotun Egbinola, a/k/a Abayomi Egbinola, is a dual Nigerian-United Kingdom citizen born on August 13, 1979. He is described as a black male, with cropped black hair and brown eyes. He holds UK passport number 801844301. Egbinola holds a Nigerian passport number A07722968, a photograph of which investigators discovered while reviewing evidence obtained pursuant to the search warrant executed on his aegbinola@gmail.com account. Copies of his Nigerian passport and UK passport information are attached as **Exhibit D**.

CONCLUSION

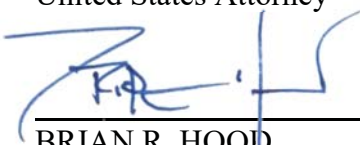
37. I have attached the following documents in support of this request for the extradition of Egbinola:

- A. **Exhibit A** is a copy of the criminal complaint;
- B. **Exhibit B** is a copy of the arrest warrant;
- C. **Exhibit C** is a copy of the pertinent sections of the following statutes and their penalties:
 - 1. Title 18, United States Code, Section 1343
 - 2. Title 18, United States Code, Section 1349
 - 3. Title 18, United States Code, Section 1956(a)(1)
 - 4. Title 18, United States Code, Section 1956(h)
 - 5. Title 18, United States Code, Section 1956(c)(4)
 - 6. Title 18, United States Code, Section 1956(c)(7)
 - 7. Title 18, United States Code, Section 1961(1)
- D. **Exhibit D** is a copy of Egbinola's UK passport information as well as a copy of his Nigerian passport.

38. I have thoroughly reviewed the government's evidence against Egbinola and attest that the evidence indicates that Egbinola is guilty of the offenses charged in the Criminal Complaint.


Executed this 4th day of June, 2020, at Richmond, Virginia, United States of America.

G. ZACHARY TERWILLGER
United States Attorney

A handwritten signature in blue ink, appearing to read "B.R. Hood", is written over a horizontal line.

BRIAN R. HOOD
Assistant United States Attorney

Sworn to me by the affiant using reliable electronic means, specifically telephone, on this 4th day of June, 2020, at Richmond, Virginia, United States of America.

/s/ 
Roderick C. Young
United States Magistrate Judge