

Three Nigerian Nationals Extradited to the United States from the United Kingdom for Participating in Business Email Compromise Fraud Schemes

[justice.gov/opa/pr/three-nigerian-nationals-extradited-united-states-united-kingdom-participating-business-email](https://www.justice.gov/opa/pr/three-nigerian-nationals-extradited-united-states-united-kingdom-participating-business-email)



Press Release

Wednesday, August 10, 2022

For Immediate Release

Office of Public Affairs

Three Nigerian citizens were extradited from the United Kingdom (UK) and arrived in the United States in relation to their alleged participation in multimillion-dollar cyber-enabled business email compromise (BEC) fraud schemes in the Western District of North Carolina, Southern District of Texas and Eastern District of Virginia. The scams allegedly perpetrated by the defendants and their co-conspirators targeted unsuspecting victims including universities in North Carolina, Texas and Virginia, and attempted to cause more than \$5 million in losses.

BEC, also known as “cyber-enabled financial fraud,” is a sophisticated scam often targeting employees with access to company finances, businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The same criminal organizations that perpetrate BEC also exploit individual victims, often real estate purchasers, the elderly, and others, by convincing them to make wire transfers to bank accounts controlled by the criminals. This is often accomplished by impersonating a key employee or business partner after obtaining access to that person’s email account or sometimes done through romance and lottery scams. BEC scams may involve fraudulent requests for checks rather than wire transfers; they may target sensitive information such as personally identifiable information (PII) or employee tax records instead of, or in addition to, money; and they may not involve an actual “compromise” of an email account or computer network. Foreign citizens perpetrate many BEC scams. Those individuals are often members of transnational criminal organizations, which originated in Nigeria but have spread throughout the world.

Western District of North Carolina

Oludayo Kolawole John Adeagbo aka John Edwards and John Dayo, 43, a Nigerian citizen and UK resident, and Donald Ikenna Echeazu aka Donald Smith and Donald Dodient, 40, a dual UK and Nigerian citizen, are charged with wire fraud conspiracy, money laundering conspiracy and aggravated identity theft for defrauding a North Carolina university (the University) of more than \$1.9 million via a business email compromise scheme. The indictment was returned by a federal grand jury in the Western District of North Carolina on April 17, 2019, and was unsealed yesterday following Echeazu's initial appearance in federal court in Charlotte.

According to allegations contained in the indictment, from Aug. 30, 2016, to Jan. 12, 2017, Adeagbo and Echeazu conspired with other individuals to obtain information about significant construction projects occurring throughout the United States, including an ongoing multi-million-dollar project at the victim University. To execute the scheme, the defendants allegedly registered a domain name similar to that of the legitimate construction company in charge of the University's project and created an email address that closely resembled that of an employee of the construction company. Using the fake email address, the co-conspirators allegedly deceived and directed the University to wire a payment of more than \$1.9 million to a bank account controlled by an individual working under the direction of defendants. Upon receiving the payment, the co-conspirators allegedly laundered the stolen proceeds through a series of financial transactions designed to conceal the fraud.

The wire fraud conspiracy charge and the money laundering conspiracy charge each carry a maximum statutory sentence of 20 years in prison. The aggravated identity theft charge carries a mandatory two-year prison sentence consecutive to any other term imposed.

The FBI Charlotte Field Office conducted the investigation. Assistant U.S. Attorney Graham Billings of the Western District of North Carolina is prosecuting the case.

Southern District of Texas

Oludayo Kolawole John Adeagbo aka John Edwards and John Dayo, 43, a Nigerian citizen and UK resident, is also charged in the Southern District of Texas with conspiracy to commit wire fraud and wire fraud. A federal grand jury returned the indictment March 30, 2022, which was unsealed on Aug. 3, 2022 before he was extradited to the United States.

From November 2016 until July 2018, Adeagbo allegedly conspired with others to participate in cyber-enabled business email compromises in an attempt to steal more than \$3 million from victims in Texas, including local government entities, construction companies and a Houston-area college. The indictment alleges Adeagbo and his co-conspirators registered domain names that looked similar to legitimate companies. They then sent emails from those domains pretending to be employees at those companies, according to the charges. The conspirators allegedly sent emails to clients or customers of the companies they impersonated and deceived those customers into sending wire payments to bank accounts they controlled.

Adeagbo faces up to 20 years in prison, if convicted on the charges.

The FBI Houston Cyber Task Force conducted the investigation with the assistance of the FBI Cyber and Criminal Investigative Divisions. The United Kingdom's National Crime Agency, Metropolitan Police Service, City of London Police and Crown Prosecution Service also provided substantial assistance. Assistant U.S. Attorney Rodolfo Ramirez for the Southern District of Texas is prosecuting the case along with Trial Attorney Brian Mund of the Justice Department's Criminal Division Computer Crime and Intellectual Property Section (CCIPS).

Eastern District of Virginia

Olabanji Egbinola, 42, is charged with wire fraud, conspiracy to commit wire fraud, money laundering, and conspiracy to commit money laundering.

According to a criminal complaint issued by the U.S. District Court for the Eastern District of Virginia, from Sept. 26, 2018, to Dec. 26, 2018, Egbinola is alleged to have conspired with others to defraud a Virginia-based university. Egbinola and co-conspirators created and used a fraudulent email account that incorporated the name of a construction company that had a large, ongoing contract with the university. Using this email account, Egbinola and co-conspirators deceived the university into transferring \$469,819.49 to a bank account controlled by Egbinola and co-conspirators. That money was quickly laundered and transferred overseas through numerous transactions. Evidence obtained during the investigation showed that Egbinola repeatedly accessed the email account used to defraud the Virginia university.

The FBI Richmond Division conducted the investigation. Assistant U.S. Attorney Brian Hood of for the Eastern District of Virginia is prosecuting the case.

All three defendants were arrested April 23, 2020, by UK authorities at the request of the United States and ordered extradited on Sept. 3, 2021. All three defendants filed appeals, all of which were rejected by the UK High Court on July 12, 2022.

The Justice Department's Office of International Affairs provided substantial assistance in securing the arrest and extradition of all three defendants. The U.S. Marshals Service also assisted by transporting the defendants from the UK to the United States.

Victims are encouraged to file a complaint online with the IC3 at [bec.ic3.gov](https://www.ic3.gov). The IC3 staff reviews complaints, looking for patterns or other indicators of significant criminal activity, and refers investigative packages of complaints to the appropriate law enforcement authorities in a particular city or region. The FBI provides a variety of resources relating to BEC scams through the IC3, which can be reached at www.ic3.gov. For more information on BEC scams, visit: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>.

The charges contained in an indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated August 12, 2022

Topics

Cybercrime

Financial Fraud

Press Release Number: 22-861