PRESS RELEASE

Maryland Man Sentenced to Over Five Years in Federal Prison for COVID-19 Fraud and Aggravated Identity Theft Schemes

Friday, June 2, 2023

For Immediate Release
U.S. Attorney's Office, District of Maryland

Defendant and Co-Conspirators Caused Losses Exceeding $1.5 Million, Including Defrauding a Community College of Over $290,000

Baltimore, Maryland – U.S. District Judge Stephanie A. Gallagher sentenced Olaolu Alabi, age 40, of Owings Mills, Maryland, to 66 months in federal prison, followed by three years of supervised release, after Alabi pleaded guilty to conspiracy to commit wire fraud, conspiracy to commit access device fraud and aggravated identity theft, in relation to multiple financial fraud schemes. Judge Gallagher also ordered Alabi to pay a forfeiture money judgment of $500,000 and will determine the amount of restitution at a later date.

The sentence was announced by United States Attorney for the District of Maryland Erek L. Barron; Special Agent in Charge James C. Harris of Homeland Security Investigations ("HIS") Baltimore; Special Agent in Charge Karen L. Brown Cleveland of the U.S. Department of State, Diplomatic Security Service ("DSS"), Washington Field Office; Special Agent in Charge Troy Springer, of the National Capital Region of the U.S. Department of Labor-Office of Inspector General ("DOL-OIG"); and Postal Inspector in Charge Damon E. Wood of the U.S. Postal Inspection Service – Washington Division.

According to his plea agreement, from June 2019 until August 5, 2020, Alabi conspired with multiple individuals to defraud victim businesses, individuals and financial institutions through business email compromise schemes and/or COVID-19 Coronavirus Aid, Relief, and Economic Security ("CARES") Act unemployment insurance ("UI")fraud

schemes to obtain more than $1.5 million. From March 2020 to August 2020, Alabi and his co-conspirators used and trafficked in unauthorized access devices and in that scheme alone, they obtained more than $400,000 in UI and other COVID-19 related benefits that were loaded onto debit cards. Alabi admitted that he personally obtained at least $500,000 from his participation in these fraud schemes, which he used for his personal benefit, including a trip to Hawaii for himself and two friends.

As detailed in the plea agreement, Alabi used the personal identifying information ("PII") of individuals without their knowledge or permission to fraudulently obtain identity documents and obtain UI benefits. For example, Alabi obtained a driver's license in the name of one victim and obtained fraudulent UI benefits in the names of two other victims. Alabi also used at least two aliases, obtaining fake passports and backup documentation for each of his aliases. Alabi used the fraudulent documents to open bank accounts in the names of identity theft victims and in his aliases, which were used to deposit proceeds of the fraud schemes. In addition, Alabi created limited liability companies ("LLCs") which were used in the fraud schemes to hide the conspirators' identities and frustrate the efforts of financial institutions and law enforcement.

Alabi admitted using an encrypted text messaging application to communicate with his co-conspirators, including Idowu Raji, about the timing of victim fund deposits into accounts Alabi controlled, withdrawing the fraud proceeds from the bank accounts receiving the funds, and using debit cards loaded with UI funds. Alabi also had in-person conversations with co-conspirator Raji.

Further, on September 30, 2019, Alabi deposited a $44,180.55 check, made payable to one of the LLCs he'd established, into a bank account opened in the name of that company. The check was part of more than $300,000 that had been obtained from a victim business, Victim T. As part of a business email compromise ("BEC") scheme, Victim T sent the money to accounts controlled by Alabi's co-conspirators, thinking that it was paying its actual debts. A cashier's check for $44,173.50, also part of the $300,000 obtained from Victim T, was deposited into another bank account controlled by Alabi. In another instance, fraudulent emails from Alabi's co-conspirators about paying an invoice caused Victim LSI, a company in Ohio, to send or transfer more than $500,000 to accounts controlled by Alabi and the co-conspirators.

Alabi also admitted that in April 2020 a separate victim, a community college lost $293,565, based on fraudulent emails purporting to be from one of its vendors. The emails advised that the vendor was no longer accepting checks for payment and provided wiring instructions. The emails came from the vendor point of contact's real email address after the conspirators gained access to the account. The victim community college wired the funds into a bank account controlled by the conspirators,

who then transferred the funds to other accounts and purchased cashier's checks. Eventually, the vendor reached out to the victim community college about the overdue amount and the community college then realized it had been defrauded, causing a significant hardship for the community college.

On August 5, 2020, federal agents executed a search warrant at Alabi's residence and seized and searched his cell phone. Conversations in the messaging app included exchanges related to fraudulent unemployment insurance claims. For example, as detailed in messages, on June 30, 2020, Alabi travelled to Raji's residence and picked up debit cards containing unemployment insurance benefits obtained using the personal identifying information of real persons. Alabi then went to a U.S. Post Office where he used the debit cards from Raji to purchase a total of 19 separate $1,000 money orders.

On May 20, 2022, co-conspirator Idowu Raji, age 41, of Baltimore County, Maryland, was sentenced to 94 months in federal prison for conspiracy to commit access device fraud, access device fraud, and aggravated identity theft. The Court also ordered Raji to pay $1,793,472 in restitution.

The District of Maryland Strike Force is one of three strike forces established throughout the United States by the U.S. Department of Justice to investigate and prosecute COVID-19 fraud, including fraud relating to the Coronavirus Aid, Relief, and Economic Security ("CARES") Act. The CARES Act was designed to provide emergency financial assistance to Americans suffering the economic effects caused by the COVID-19 pandemic. The strike forces focus on large-scale, multi-state pandemic relief fraud perpetrated by criminal organizations and transnational actors. The strike forces are interagency law enforcement efforts, using prosecutor-led and data analyst-driven teams designed to identify and bring to justice those who stole pandemic relief funds.

For more information on the Department's response to the pandemic, please visit https://www.justice.gov/coronavirus. Anyone with information about allegations of attempted fraud involving COVID-19 can report it by calling the Department of Justice's National Center for Disaster Fraud (NCDF) Hotline at 866-720-5721 or via the NCDF Web Complaint Form at: https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form.

United States Attorney Erek L. Barron commended HSI, DSS, DOL-OIG, and the U.S. Postal Inspection Service for their work in the investigation. Mr. Barron thanked Assistant U.S. Attorney Harry M. Gruber, who prosecuted the case. He also recognized the assistance of the Maryland COVID-19 Strike Force Paralegal Specialist Joanna B.N. Huber.

For more information on the Maryland U.S. Attorney's Office, its priorities, and resources available to help the community, please visit www.justice.gov/usao-md.

# # #

Contact
Marcia Lubin
(410) 209-4854

Updated June 2, 2023

Topics

CORONAVIRUS

FINANCIAL FRAUD

IDENTITY THEFT

Component

USAO - Maryland