NEWS RELEASE

For Immediate Distribution

July 3, 2020

Nicola T. Hanna
United States Attorney
Central District of California

Thom Mrozek
Director of Media Relations
thom.mrozek@usdoj.gov
(213) 894-6947

Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes

LOS ANGELES – A Dubai resident who flaunted his extravagant lifestyle on social media has arrived in the United States to face criminal charges alleging he conspired to launder hundreds of millions of dollars from business email compromise (BEC) frauds and other scams, including schemes targeting a U.S. law firm, a foreign bank and an English Premier League soccer club.

Ramon Olorunwa Abbas, 37, a.k.a. "Ray Hushpuppi" and "Hush," a Nigerian national, arrived in Chicago Thursday evening after being expelled from the United Arab Emirates (UAE). Abbas made his initial U.S. court appearance this morning in Chicago, and he is expected to be transferred to Los Angeles in the coming weeks.

Abbas was arrested last month by UAE law enforcement officials. FBI special agents earlier this week obtained custody of Abbas and brought him to the United States to face a charge of conspiring to engage in money laundering that is alleged in a criminal complaint filed on June 25 by federal prosecutors in Los Angeles.

According to an affidavit filed with the complaint, Abbas maintains social media accounts that frequently showed him in designer clothes, wearing expensive watches, and posing in or with luxury cars and charter jets. "The FBI's investigation has revealed that Abbas finances this opulent lifestyle through crime, and that he is one of the leaders of a transnational network that facilitates computer intrusions, fraudulent schemes (including BEC schemes), and money laundering, targeting victims around the world in schemes designed to steal hundreds of millions of dollars," according to the affidavit.

The affidavit describes BEC schemes as often involving a computer hacker gaining unauthorized access to a business' email account, blocking or redirecting communications to and/or from that email account, and then using the compromised email account or a separate fraudulent email account to communicate with personnel from a victim company and to attempt to trick them into making an unauthorized wire transfer.

“BEC schemes are one of the most difficult cybercrimes we encounter as they typically involve a coordinated group of con artists scattered around the world who have experience with computer hacking and exploiting the international financial system,” said United States Attorney Nick Hanna. “This case targets a key player in a large, transnational conspiracy who was living an opulent lifestyle in another country while allegedly providing safe havens for stolen money around the world. As this case demonstrates, my office will continue to hold such criminals accountable, no matter where they live.”

“In 2019 alone, the FBI recorded $1.7 billion in losses by companies and individuals victimized through business email compromise scams, the type of scheme Mr. Abbas is charged with conducting from abroad,” said Paul Delacourt, the Assistant Director in Charge of the FBI’s Los Angeles Field Office. “While this arrest has effectively taken a major alleged BEC player offline, BEC scams represent the most financially costly type of scheme reported to the FBI. I urge anyone who transfers funds personally or on behalf of a company to educate themselves about BEC so they can identify this insidious scheme before losing sizable amounts of money.”

“This was a challenging case, one that spanned international boundaries, traditional financial systems and the digital sphere,” said Jesse Baker, Special Agent in Charge of the United States Secret Service, Los Angles Field Office. “Technology has essentially erased geographic boundaries leaving trans-national criminal syndicates to believe that they are beyond the reach of law enforcement. The success in this case was the direct result of our trusted partnerships between the Department of Justice and our federal law enforcement colleagues. These partnerships helped dismantle a sophisticated organized crime group who preyed upon unsuspecting businesses. It is thanks to these partnerships that the American people can feel a bit more secure today.”

The affidavit alleges that Abbas and others committed a BEC scheme that defrauded a client of a New York-based law firm out of approximately $922,857 in October 2019. Abbas and co-conspirators allegedly tricked one of the law firm’s paralegals into wiring money intended for the client’s real estate refinancing to a bank account that was controlled by Abbas and the co-conspirators.

The affidavit also alleges that Abbas conspired to launder funds stolen in a $14.7 million cyber-heist from a foreign financial institution in February 2019, in which the stolen money was sent to bank accounts around the world. Abbas allegedly provided a co-conspirator with two bank accounts in Europe that Abbas anticipated each would receive €5 million (about $5.6 million) of the fraudulently obtained funds.

Abbas and others further conspired to launder hundreds of millions of dollars from other fraudulent schemes and computer intrusions, including one scheme to steal £100 million (approximately $124 million) from an English Premier League soccer club, the complaint alleges.

A criminal complaint contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt.

If convicted of conspiracy to engage in money laundering, Abbas would face a statutory maximum sentence of 20 years in federal prison.

The FBI led the investigation of Abbas, and the United States Secret Service was also involved and provided substantial assistance. The FBI further thanks the government of the United Arab Emirates and the Dubai Police Department for their substantial assistance.

This case is being prosecuted by Assistant United States Attorneys Anil J. Antony and Joseph B. Woodring of the Cyber and Intellectual Property Crimes Section. The Criminal Division's Office of International Affairs provided substantial assistance in this matter.

Release No. 20-118