PRESS RELEASE

Eastern District of Texas Announces Multi-Year Investigation into Transnational Cryptocurrency Money Laundering Networks

Wednesday, November 30, 2022

For Immediate Release

U.S. Attorney's Office, Eastern District of Texas

Operation Crypto Runner Targets Foreign and Domestic Networks Laundering Money Stolen from United States Fraud Victims

TYLER, Texas – According to court documents unsealed today, 21 individuals have been charged for their roles in transnational money laundering networks, including those that laundered millions of dollars stolen from United States fraud victims through romance scams, business email compromises, technical support schemes, and other fraud schemes.

U.S. Attorney Brit Featherston of the Eastern District of Texas, William Smarr, Special Agent in Charge of the U.S. Secret Service's (USSS) Dallas Field Office, and Inspector in Charge Thomas Noyes of the U.S. Postal Inspection Service announced Operation Crypto Runner, an Organized Crime Drug Enforcement Task Forces (OCDETF) investigation into transnational cryptocurrency money laundering networks that facilitate the movement of fraud proceeds from victims in the United States to foreign criminal organizations.

"These defendants orchestrated highly organized and sophisticated schemes to launder fraud proceeds through cryptocurrency," said U.S. Attorney Brit Featherston. "Today's announcement sends a clear message that money laundering networks that service fraud schemes targeting American victims, especially the elderly, will not be tolerated, and those operating such networks will be held accountable. By acting as domestic money launderers for foreign co-conspirators, these defendants played indispensable roles that allowed foreign actors to reach from overseas to target victims in communities across the United States."

"Today's announcement demonstrates the investigative capabilities of the Secret Service and highlights the success of our collaborative efforts through Operation Crypto Runner to dismantle and disrupt transnational money laundering networks," said William Smarr, Special Agent in Charge of the U.S. Secret Service's Dallas Field Office. "These arrests are just the beginning. We are committed to bringing each of the remaining perpetrators to justice."

"These cases stem from a multi-year operation initiated in the Eastern District of Texas by Postal Inspectors and the Secret Service," said Thomas Noyes, Inspector in Charge of the Postal Inspection Service's Fort Worth Division. "Cybercrime has become an all-too-common way for foreign criminal actors to prey on Americans. Interagency cooperation is essential to be effective in disrupting organized crime. I commend the exceptional work of our law enforcement partners and emphasize our agency's ongoing commitment to combatting fraud and money laundering schemes."

To date, the Operation has disrupted more than $300 million in annual money laundering transactions, seized and forfeited millions in cash and cryptocurrency, and identified thousands of victims.

Some of the schemes alleged in the indictments include the following:

- *U.S. v. Zenobia Walker*, 6:20-CR-91-JCB/KNM (11/19/2020)

Zenobia Walker, 65, of Temple Hills, Maryland, pleaded guilty on January 6, 2022, to conspiracy to operate an unlicensed money transmitting business and was sentenced to 18 months in federal prison on November 2, 2022. Walker was involved in a scheme in which she received cash by mail, money orders, wire transfers, and cashier's checks obtained from victims of romance scams and from victims of other fraud schemes. The funds were deposited into

Walker's personal bank accounts and withdrawn and deposited into other bank accounts in order to exchange the funds for cryptocurrency. Between December 2019 and September 2020, Walker exchanged $308,800.00 for cryptocurrency on behalf of her foreign co-conspirators.

- *U.S. v. Tulasidas Konda*, 6:20-CR-31-JDK/JDL (4/23/2021)

Tulasidas Konda, 57, of Amelia Court House, Virginia, pleaded guilty on May 5, 2021, to conspiracy to commit money laundering. Konda led and organized a multi-year money laundering conspiracy involving the laundering of criminal proceeds derived from various scams. Konda's organization opened bank accounts and mailboxes that were used to receive and transact victim funds, received the victim funds, engaged in subsequent financial transactions, routinely structured in amounts under $10,000 in an effort to evade reporting requirements and to conceal the nature and source of the criminal proceeds, and moved the criminal proceeds to foreign co-conspirators. Konda's organization routinely exchanged the criminal proceeds for cryptocurrency and directed the cryptocurrency to wallets under the control of their foreign co-conspirators. In the course of the operation, Konda was personally responsible for laundering $4,172,061.58 in criminal proceeds.

- *U.S. v. Deependra Bhusal*, 6:21-CR-32-JDK/JDL (4/23/2021)

Deependra Bhusal, 46, of Irving, Texas, pleaded guilty on April 30, 2021, to conspiracy to commit money laundering and was sentenced to 46 months in federal prison on April 6, 2022. Bhusal was a key member of the Konda Organization. In the course of the operation, Bhusal was personally responsible for laundering $1,437,358.99 in criminal proceeds.

- *U.S. v. Lois Boyd, et al.*, 6:21-CR-43-JDK/KNM (6/16/2021)

Lois Boyd, 76, of Amelia Court House, Virginia, pleaded guilty on June 14, 2022, to a violation of the Travel Act. Boyd, also a member of the Konda Organization, is alleged to have conspired with others to receive victim money derived from a variety of fraud schemes and launder the proceeds through cryptocurrency. Boyd routinely structured deposits in order to avoid transaction reporting requirements and to conceal the nature and source of the criminal proceeds. Boyd and others in the Konda Organization exchanged the criminal proceeds for cryptocurrency and directed the cryptocurrency to wallets under the control of their foreign co-conspirators. In August 2020, Boyd and others traveled to Longview, Texas, where they attempted to exchange more than $450,000 for Bitcoin.

- *U.S. v. John Khuu*, 6:22-CR-62-JCB/JDL (5/18/2022)

John Khuu, 27, of San Francisco, California was named in an indictment returned by a federal grand jury charging him in a money laundering conspiracy. According to the indictment, Khuu is alleged to have conspired with others to launder the proceeds of his drug trafficking organization through cryptocurrency. The defendant allegedly distributed counterfeit

pharmaceutical pills and other controlled substances on dark web markets to customers across the United States. Customers paid for their purchases by transferring cryptocurrency, usually Bitcoin, from their dark web market customer accounts to one of Khuu's vendor accounts. Khuu and his co-conspirators traded the Bitcoin for U.S. currency and laundered the proceeds through hundreds of transactions and dozens of financial accounts. During the course of the conspiracy, Khuu and his co-conspirators allegedly laundered more than $5,350,000.00. On August 17, 2022, Khuu was also charged by a federal grand jury in the Northern District of California in a two-count indictment charging him with unlawful importation of a controlled substance.

- *U.S. v. Randall V. Rule, et al*., 6:22-CR-64-JDK/KNM (5/18/2022)

Randall V. Rule, 71, of Reno, Nevada, and Gregory C. Nysewander, 64, formerly of Irmo, South Carolina, were named in an indictment returned by a federal grand jury charging them with money laundering conspiracy, money laundering, and a conspiracy to violate the Bank Secrecy Act. According to the indictment, Rule and Nysewander are alleged to have conspired with others to launder the proceeds of wire fraud and mail fraud schemes through cryptocurrency. The defendants converted funds from romance scams, business email compromises, and real estate scams, and other fraudulent schemes into cryptocurrency and sent the cryptocurrency to accounts controlled by foreign and domestic co-conspirators. The defendants and their co-conspirators made false representations and concealed material facts, in order to avoid discovery of the fraudulent nature of deposits, wires, and transfers, such as providing instructions to co-conspirators and victims to label wire transfers as "loan repayments" and "advertising." The defendants also made false representations and concealed material facts when completing account opening documents and when communicating with financial institutions and cryptocurrency exchanges. During the course of the conspiracy, Rule, Nysewander, and their co-conspirators allegedly laundered more than $2.4 million. Rule and Nysewander are also charged with willfully violating the money services business requirements of the Bank Secrecy Act.

- *U.S. v. Sharena Seay*, 6:22-CR-110-JDK/JDL (8/17/2022)

Sharena Seay, 37, of Jacksonville, Florida, was named in an indictment returned by a federal grand jury charging her with money laundering. According to the indictment, Seay is alleged to have laundered the proceeds of her drug trafficking operations through cryptocurrency. The defendant allegedly supplied alpha-Pyrrolidinopentiophenone (alpha-PVP), which is often called "flakka," and similar synthetic cathinones, such as Eutylone or alpha-PiHP. Seay distributed alpha-PVP and other controlled substances to various customers across the United States. Customers who purchased controlled substances from Seay paid for their purchases with cash. Seay laundered the cash proceeds through cryptocurrency in order to purchase more controlled substances on the dark web and to conceal her criminal activity. During the course of the conspiracy, Seay allegedly laundered more than $1.2 million.

- *U.S. v. Fnu Ankush, et al.*, 6:22-CR-111-JCB/KNM (8/17/2022)

Fnu Ankush, 35, of Fishers, Indiana, Jenisha Katuwal, 40, of Fishers, Indiana, Sukhwinder Sandhu, 44, of Philadelphia, Pennsylvania, Inder Singh, 37, of Philadelphia, Pennsylvania, Mukul Khanna, 37, of Philadelphia, Pennsylvania, Satinder Singh, 36, of Philadelphia, Pennsylvania, Ramneek Singh, 28, of Levittown, New York, Muninder Singh, 52, of Fairfax, Virginia, Sandeep Heir, 43, of Fresno, California, and Rachel Mullins, 36, of Jacksonville, Florida, were named in an indictment returned by a federal grand jury charging them in a wire and mail fraud conspiracy. According to the indictment, the defendants facilitated technical support schemes by creating a financial infrastructure in the United States that involved establishing shell companies with names intended to resemble names of legitimate companies. The defendants opened and controlled business bank accounts in the names of the shell companies in order to facilitate the computer tech scheme. The defendants also established websites for many of the shell companies in order to make the shell companies appear legitimate. Then, through false and fraudulent pretenses, representations, and promises, and concealment of material facts, the defendants and their co-conspirators persuaded victims to deposit, wire, or transfer funds into designated bank accounts or to mail funds to designated addresses.

These efforts are part of Operation Crypto Runner, an Organized Crime Drug Enforcement Task Forces (OCDETF) operation. OCDETF identifies, disrupts, and dismantles the highest-level criminal organizations that threaten the United States using a prosecutor-led, intelligence-driven, multi-agency approach. Additional information about the OCDETF Program can be found at https://www.justice.gov/OCDETF.

In October 2017, the Elder Abuse Prevention and Prosecution Act (EAPPA) was signed into law. The EAPPA's purpose is to increase the federal government's focus on preventing elder abuse and exploitation. Subsequently, the Department of Justice launched the Elder Justice Initiative (EJI). Through the EJI, the Department has participated in hundreds of criminal and civil enforcement actions involving misconduct that targeted vulnerable seniors. The Department has conducted hundreds of trainings and outreach sessions across the country. The EJI website contains useful information, including educational resources about prevalent financial scams so you can guard against them.

In August 2020, the Eastern District of Texas announced its own initiative, in partnership with law enforcement and private financial institutions, to identify and prosecute transnational elder fraud. This EDTX initiative is designed to combat these criminal organizations, both foreign and domestic, as well their networks of associates and money mules who launder the stolen funds.

The investigations arising from the operation are being conducted by the U.S. Secret Service and the U.S. Postal Inspection Service and are being led and prosecuted by Assistant U.S. Attorneys Nathaniel C. Kummerfeld and L. Frank Coan, Jr., with assistance from the Criminal

Division's Fraud Section and Computer Crime and Intellectual Property Section and the Department's Office of International Affairs.

###

Updated November 30, 2022

Topics

ELDER JUSTICE | FINANCIAL FRAUD

Component

Federal Bureau of Investigation (FBI)

Organized Crime Drug Enforcement Task Forces

USAO - Texas, Eastern

Related Content

PRESS RELEASE

San Antonio Fraudster Sentenced to Prison

December 1, 2022

PRESS RELEASE

Eastern District of Texas Announces Multi-Year Investigation into Transnational Cryptocurrency Money Laundering Networks

November 30, 2022

PRESS RELEASE

Former Officers of Non-Profit Dedicated to Helping Children Plead Guilty to Using Organization's Funds for Personal Gain

November 30, 2022

Eastern District of Texas

Beaumont Office:
550 Fannin, Suite 1250
Beaumont, Texas 77701

Email USAO-EDTX

Beaumont: 409-839-2538

Stay Connected

Archives

Budget & Performance

FOIA

Accessibility

Legal Policies & Disclaimers

Privacy Policy

For Employees

Information Quality

Office of the Inspector General

No FEAR Act Data

Small Business

Vote.gov

Español

Have a question about Government Services?

Contact USA.gov