Release #101-2024
X@QueensDAKatz

QUEENS COUNTY DISTRICT ATTORNEY
125-01 QUEENS BOULEVARD
KEW GARDENS, NEW YORK 11415-1568

718.286.6000
WWW.QUEENSDA.ORG

MELINDA KATZ
DISTRICT ATTORNEY

FOR IMMEDIATE RELEASE
MONDAY, AUGUST 12, 2024

CONTACT: PRESS OFFICE (718) 286-6315
QDACommunications@queensda.org

CRYPTOCURRENCY HACKER NETWORK DISMANTLED; SEVEN DEFENDANTS INDICTED FOR STEALING MORE THAN $300,000 IN BITCOIN FROM QUEENS RESIDENT

Five Of the Defendants, Including Alleged 20-Year-Old Mastermind, His Mother and Father Arrested in California; Two Other Defendants Are Being Sought

Queens District Attorney Melinda Katz announced that seven defendants have been indicted by a grand jury on charges of grand larceny, money laundering, identity theft and other related crimes following a long-term investigation into a hack of a private cryptocurrency wallet belonging to a Queens resident. Bitcoin was removed from the victim's Blockchain.com wallet through two unauthorized transactions in November 2022. At the time of the hack, the 5.75 bitcoins were valued at approximately $92,000. Today, that same cryptocurrency amount is valued at over $300,000.

The stolen bitcoin was allegedly laundered by the defendants through a "peel chain," a technique used to transfer large amounts of illegally obtained cryptocurrency by funding a long series of small transactions. The District Attorney's Cyber Crimes Unit traced more than 250 individual transactions most of which went to different accounts on the payment processing App Cash App. Investigators were able to conclusively link these accounts to the defendants.

District Attorney Katz said: "The individuals allegedly responsible for this operation went through a meticulous series of steps to hide their criminal activity. My dedicated Cyber Crime and Cryptocurrency Unit and Detectives Bureau worked this case for months to figure out who was behind these transactions and to bring those people to justice. I thank Assembly Member Clyde Vanel for alerting us to this important case and encourage any Queens resident who may have been a victim of cryptocurrency theft to contact our Cyber Crimes team at 718-286-6673 or CyberCrimes@queensda.org."

Assembly Member Clyde Vanel said: "We are encouraged by the efforts of the Queens District Attorney Melinda Katz to protect Queens residents from technology-related fraud. We want to help ensure that Queens residents are able to invest, transact and transfer value in a safe manner. Today shows that we will bring justice to those who attempt to defraud Queens residents."

Alleged mastermind Aaron Peterson Jr., 20, his father, Aaron Peterson, 39, and his mother, Autumn Clark, 37, all of Sacramento County, CA, were extradited and arraigned Friday on a seven-count indictment charging them with grand larceny in the second degree, money laundering in the second degree, two counts of identity theft in the first degree, computer trespass, and conspiracy in the fourth degree.

Supreme Court Justice Marcia Hirsch ordered the defendants to return to court on October 15. They each face a potential maximum sentence of 5 to 15 years in prison if convicted of the top count.

Co-defendants Dontay Brown, 39, of Sacramento County, CA, and Ronald Lamar Moland, Jr., 22, of Solano County, CA, are expected to be arraigned at a later date. Two other defendants are still being sought.

According to the charges:

- On November 28, 2022, 5.75 bitcoins were removed from the victim's private cryptocurrency wallet through two unauthorized transactions.

- The Queens District Attorney's Office was alerted to the case shortly afterward by Assembly Member Clyde Vanel and an investigation was launched.

- Using specialized investigative techniques, members of the Queens District Attorney's Cyber Crime Unit and Detectives Bureau uncovered more than 250 transactions over the course of eight months used as a means to launder the money. This practice is commonly referred to as a "peel chain," a method of hiding cryptocurrency transactions by sending small amounts to individual bitcoin wallets on various dates.

- The trace of the funds further revealed the movement of the stolen funds to various deposit addresses belonging to Cash App and other financial services that were then identified and subpoenaed.

- Each of the seven defendants was identified as the account owner in receipt of the stolen funds as follows:

    - Approximately $22,500 to a Cash App account belonging to defendant Clark over the course of 18 transactions.

    - Approximately $16,000 to a Cash App account belonging to an unapprehended defendant over the course of 24 transactions.

    - Approximately $22,000 to a Cash App account belonging to defendant Moland over the course of eight transactions.

    - Approximately $19,700 to a Cash App account belonging to defendant Brown over the course of three transactions.

    - Approximately $9,500 to a Cash App account belonging to defendant Peterson Sr. over the course of 33 transactions.

    - Approximately $680 to a Cash App account belonging to an unapprehended defendant over the course of two transactions.

- After the money was laundered through the Cash App accounts, the co-conspirators each withdrew a certain amount of cash for their personal use. The remaining funds were sent to a centralized "pool account" belonging to Peterson Jr.

- Peterson Jr. used the funds on personal luxury purchases including a diamond pendant necklace and a new Mercedes-Benz.

- On July 24, Peterson Jr., Peterson Sr., Clark, Brown and Moland Jr., were apprehended by local authorities at their respective places of residence in California pursuant to the indictment warrant.

The investigation was conducted by Sergeant Linda DenDekker of the District Attorney's Detective Bureau, with the assistance of Detective Investigator Daniel Yi Suh, under the supervision of Lieutenant Joseph Falgiano and under the overall supervision of Chief Investigator Robert C. LaPollo.

FTI Consulting as well as the California Department of Justice's Division of Criminal Law, Cybercrime Section and the Division of Law Enforcement, Bureau of Investigation's White Collar Investigation Team, provided crucial assistance.

Assistant District Attorneys Elizabeth Speck, Section Chief of the Cybercrime Unit, and Senior Assistant District Attorney Catherine Jahn from the District Attorney's Major Economic Crimes Bureau are prosecuting the case under the supervision of Jonathan Scharf, Deputy Chief and Cryptocurrency Investigations Coordinator, Catherine Kane, Senior Deputy Chief, Mary Lowenburg, Bureau Chief, and under the overall supervision of Executive Assistant District Attorney for Investigations Gerard Brave.

Criminal complaints and indictments are accusations. A defendant is presumed innocent until proven guilty.

#

Note to Editors: Archived press releases are available at www.queensda.org.