Department of Justice

U.S. Attorney's Office

Eastern District of Michigan

FOR IMMEDIATE RELEASE Wednesday, September 7, 2022

SEVEN PEOPLE INDICTED FOR $28 MILLION CELLPHONE FRAUD AND IDENTITY THEFT SCHEME

DETROIT - Seven individuals were indicted by a federal grand jury in Detroit charging them with conspiracy to commit wire fraud, and aggravated identity theft related to a $28 million cellphone upgrade fraud scheme spanning multiple states, announced United States Attorney Dawn N. Ison.

Ison was joined in the announcement by Angie M. Salazar, Special Agent in Charge, Department of Homeland Security, Homeland Security Investigations.

Charged were:

EMMANUEL LUTER, 31, of Atlanta, Georgia (formerly of Southfield, Michigan)

JOSEPH INGRAM, 31, of Atlanta, Georgia (formerly of Southfield, Michigan)

DALONTAE DAVIS, 31, of Sachse, Texas (formerly of Southfield, Michigan)

DONNELL TAYLOR, 30, of Southfield, Michigan

DOMINIQUE BARNES, 33, of Southfield, Michigan

DELANO BUSH, 32, of Southfield, Michigan

JOSHUA MOTLEY, 33, of Detroit, Michigan

According to the indictment, unsealed today, the defendants, a group that referred to themselves as the "Clear Gods", engaged in an ongoing scheme to defraud, using the personally identifiable information (PII) of other people to acquire significant numbers of Apple-branded cellular devices on credit, which were then resold for profit.

The defendants did this by first purchasing individuals' PII from various locations, including from "dump sites" on the internet. The defendants then used the unlawfully acquired PII to open customer cellular accounts with AT&T. Following the successful completion of a credit check, the defendants would add themselves or their associates as "authorized users" on the fraudulent account, allowing those seemingly authorized individuals to charge devices to the customer accounts. The authorized users would then enter one of a variety of retail stores, in a variety of states—most frequently Apple stores—to "upgrade" the service lines on the fraudulent cellular accounts. These devices were then "charged" to the fraudulent customer cellular accounts or otherwise purchased on credit, with defendants typically needing to pay, at most, a small upgrade fee per device. The defendants would then reverse or "clear" the upgrades from the service lines, often allowing them to repeat the previous step of the scheme at another Apple store location.

The members of the conspiracy employed various methods to gain unauthorized access to AT&T's computer systems for the purpose of creating AT&T accounts, fraudulently adding authorized users, and for clearing the fraudulent upgrades from the service lines. At the beginning of the scheme, this

involved the collusive-acquisition or theft of RSA tokens and employee IDs, allowing defendants to later open new accounts (and make changes to existing accounts) by calling into one an internal AT&T support hotline and impersonating AT&T Retail Sales employees.

As the scheme progressed and AT&T restricted employee tokens to allow access exclusively via AT&T equipment (as opposed to remote-access using personal computing equipment), members of the conspiracy took steps to acquire actual AT&T-networked devices—this included social engineering and sleight-of-hand "swapping" of broken or disabled tablets for active tablets from retail sales employees; the outright theft (or collusive acquisition) of retail sales employees' tablet-computers; and the occasional, strong-armed theft of desktop computer towers from AT&T stores. Throughout the scheme, the defendants routinely sought out and worked with corrupt AT&T retail store employees.

As alleged in the indictment, from as early as June 2017 and continuing through at least September 2019, Defendants conducted more than 26,000 fraudulent transactions, resulting in a loss of more than $28 million dollars.

United States Attorney Ison stated, "As alleged in the indictment, the defendants engaged in an incredibly sophisticated scheme to defraud, evolving their tactics over time in what was ultimately a failed attempt to evade detection and avoid prosecution. This indictment is the culmination of significant efforts by multiple law enforcement agencies across multiple jurisdictions. I want to commend all of those involved for their work to unravel this scheme and prosecute those responsible.

"HSI with our law enforcement partners persevered to unravel the sophisticated scheme which ultimately led to this indictment," said Special Agent in Charge of HSI Detroit Angie Salazar. "These types of crimes are often mislabeled as victimless, which could not be farther from the truth. Oftentimes victims of fraud are required to spend many years clearing up financial issues and fixing incorrect personal identifying information caused solely by the greed of these criminals. HSI will continue to investigate those criminals who seek to exploit the trade, travel, or finance of the United States."

It is important to note that an indictment is merely a charge and should not be considered as evidence of guilt. The defendants are presumed innocent until proven guilty in a court of law.

The case is assigned to U.S. District Court Judge Laurie J. Michelson. The case was investigated by agents from the Detroit Metro Airport resident agency of the Department of Homeland Security, Homeland Security Investigations (HSI), with assistance from the Social Security Administration Office of the Inspector General (SSA-OIG), the Department of Labor Office of the Inspector General (DOL-OIG), the Detroit Metro Airport Police Department, the Taylor Police Department, and the Wayne State University Police Department. The case is being prosecuted by Assistant U.S. Attorney Ryan A. Particka.

Topic(s):
Financial Fraud

Component(s):
USAO - Michigan, Eastern