



PRESS RELEASE

Two Individuals Charged in Multi-Million Dollar Scheme to Defraud Rideshare Customers, Drivers and Others



Wednesday, August 28, 2024

For Immediate Release

U.S. Attorney's Office, Eastern District
of New York

Defendants Allegedly Sold Hundreds of Subscriptions for “Screwber,” GPS “Spoofing,” and Other Manipulated Applications in Rideshare Scheme

Earlier today, in federal court in Brooklyn, an indictment was unsealed charging Eliahou Paldiel and Carlos Arturo Suarez Palacios (Suarez) with wire fraud and money laundering conspiracies relating to a wide-ranging scheme in which the defendants sold hacked smartphones and fraudulent applications to more than 800 rideshare drivers (Driver Co-conspirators). The applications enabled the Driver Co-conspirators to “spoof” GPS locations to fraudulently obtain “surge” fees and to otherwise manipulate legitimate rideshare applications to enrich themselves to the detriment of riders, law-abiding drivers and rideshare companies. If convicted, the defendants face up to 20 years in prison on each of the two counts.

This morning, Paldiel was arrested in Brooklyn and Suarez was arrested in Brick Township, New Jersey. The defendants will be arraigned later this afternoon before United States Magistrate Judge Marcia M. Henry.

Breon Peace, United States Attorney for the Eastern District of New York, and Christie M. Curtis, Acting Assistant Director in Charge, Federal Bureau of Investigation, New York Field Office (FBI), announced the arrests and charges.

“As alleged, the defendants sought to enrich themselves by corrupting the rideshare market at the expense of unsuspecting passengers and hardworking drivers who play by the rules,” stated United States Attorney Peace. “My Office remains steadfast in ensuring that, no matter how complex the scheme, individuals who violate the law will be caught and held accountable. The defendants learned an important lesson in these charges: there is no such thing as a free ride.”

“Eliahou Paldiel and Carlos Suarez allegedly developed a rideshare application that fraudulently manipulated a driver’s GPS location to obtain unlawful surge fare pricing, defrauding customers and legitimate drivers. For almost six years, this alleged conspiracy offered an unfair financial advantage to more than 800 participants and disrupted the integrity of nationwide rideshare services, earning the participants more than \$40 million. The FBI will continue to dismantle all fraudulent schemes, even as criminals attempt to create innovative scams for selfish gains,” stated FBI Acting Assistant Director in Charge Curtis.

Rideshare Company-1 is a multinational company headquartered in the United States that provides ridesharing services. It operates primarily through its smartphone application (the Rideshare Company-1 Application), connecting users with drivers for on-demand transportation and delivery services.

As alleged in the indictment and other court filings, between November 2018 and August 2024, Paldiel and Suarez engaged in a scheme to defraud Rideshare Company-1’s users and drivers by causing passengers to collectively pay millions of dollars in fraudulent “surge” fees to hundreds of participating Driver Co-conspirators, and depriving legitimate rideshare drivers of their true share of “surge” fares and the most lucrative trips. In addition, the fraudulent devices and applications sold by the defendants for profit enabled the Driver Co-conspirators to cherry-pick high-fare rides by obtaining proprietary information and to “queue” in areas where they were not physically present.

The defendants allegedly sold scheme applications to Driver Co-conspirators on manipulated — also known as “jailbroken” or “rooted” — cellular devices (the Scheme Devices). A jailbroken or rooted cellular device has had its operating system security restrictions modified or removed, thereby allowing the installation of software, including applications, that the device manufacturer had not made available for the device. Driver Co-conspirators utilized the Rideshare Company-1 Application on their Scheme Devices.

Fake GPS “Spoofing” App

Fake GPS was a GPS spoofing application developed by the defendants and others. Fake GPS enabled Driver Co-conspirators to manipulate or “spoof” their locations within the

Rideshare Company-1 Application and make it appear as if they were located in an area with surging fares when, in fact, they were not.

Screwber App

Screwber is an application developed by the defendants and others that provided Driver Co-conspirators with information about prospective Rideshare Company-1 rides that was not otherwise available to Rideshare Company-1 drivers prior to accepting such rides. For example, Screwber enabled Driver Co-conspirators to obtain prospective riders' destinations and approximate fares for prospective trips, thereby allowing Driver Co-conspirators to accept or decline the prospective rides based on information to which they were otherwise not entitled and, in turn, cherry-pick only the most profitable and lucrative rides offered to them through the Rideshare Company-1 Application.

Rideshare Application

The defendants caused outdated versions of the Rideshare Company-1 Application to be downloaded onto the Scheme Devices provided to Driver Co-conspirators. By installing outdated versions of the Rideshare Company-1 Application, the defendants ensured that the Fake GPS and Screwber applications were not detected by security features implemented in newer versions of the Rideshare Company-1 Application.

As part of the scheme, the defendants sent Driver Co-conspirators information about how to avoid detection, such as the following: "Using 2 iPhones with FakeGPS is very very risky. If you need FakeGPS for airport I recommend doing it one time a day. Do it when you wake up in the morning before you go to the airport." The defendants also spoke with one another about their strategy to profit from the Driver Co-conspirators. For example, on or about November 2, 2018, Suarez wrote to Paldiel, "You know Screwber is like drugs .. once you get into it you'll get withdrawals when you can't get your fix." In another message, Paldiel wrote to Suarez regarding the Driver Co-conspirators, "I get them hooked on the software, even a drug deal[er] throws in a few extra grams of weed in the beginning."

During the course of the scheme, the Driver Co-conspirators, using the defendants' fraudulent devices and applications, allegedly earned over approximately \$40 million from rideshare customers. The defendants received more than \$1.5 million from Driver Co-conspirators through one peer-to-peer payment service alone.

If you have information related to this case, please contact FBI at NY_RideShareTips@fbi.gov

The charges in the indictment are allegations, and the defendants are presumed innocent unless and until proven guilty. If convicted, the defendants face up to 20 years in prison on each of the two counts.

In July 2022, Mr. Peace was selected as the Chairperson of the White Collar Fraud subcommittee for the Attorney General's Advisory Committee (AGAC). As the leader of the subcommittee, Mr. Peace plays a key role in making recommendations to the AGAC to facilitate the prevention, investigation and prosecution of various financially motivated, non-

violent crimes including wire fraud and money laundering conspiracies — the crimes that the defendants committed in this case.

The government’s case is being handled by the Office’s Business and Securities Fraud Section. Assistant United States Attorneys Matthew R. Galeotti, Dana Rehnquist and Elias Laris are in charge of the prosecution, with assistance from Paralegal Specialist Madison Bates.

The Defendants:

ELIAHOU PALDIEL

Age: 52

Queens, New York

CARLOS ARTURO SUAREZ PALACIOS

Age: 54

Brick Township, New Jersey

E.D.N.Y. Docket No. 24-CR-239 (MMH) (ARR)

Contact

John Marzulli

Danielle Blustein Hass

U.S. Attorney's Office

(718) 254-6323

Updated August 28, 2024

Topic

FINANCIAL FRAUD

Component

[USAO - New York, Eastern](#)

Related Content
