PRESS RELEASE

CEO of Dozens of Companies and Entities in Florida and New Jersey Admits Role in Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment

Tuesday, June 6, 2023

For Immediate Release

U.S. Attorney's Office, District of New Jersey

TRENTON, N.J. – A Florida resident and dual citizen of the United States and Turkey pleaded guilty to running an extensive operation over many years to traffic in fraudulent and counterfeit Cisco networking equipment, Attorney for the United States Vikas Khanna, District of New Jersey, and Assistant Attorney General Kenneth A. Polite Jr. announced today.

Onur Aksoy, aka “Ron Aksoy” and “Dave Durden,” 39, of Miami, Florida, pleaded guilty before U.S. District Judge Peter G. Sheridan in Trenton federal court on June 5, 2023, to two counts of an indictment charging him with conspiring with others to traffic in counterfeit goods, to commit mail fraud, and to commit wire fraud (Count 1); and mail fraud (Count 4).

According to documents filed in this case and statements made in court:

Aksoy ran at least 19 companies formed in New Jersey and Florida as well as at least 15 Amazon storefronts, at least 10 eBay storefronts, and multiple other entities (collectively, the “Pro Network Entities”) that imported from suppliers in China and Hong Kong tens of thousands of low-quality, modified computer networking devices with counterfeit Cisco labels, stickers, boxes, documentation, and packaging, all bearing counterfeit trademarks registered and owned by Cisco, that made the goods falsely appear to be new, genuine, and high-quality devices manufactured and authorized by Cisco. The devices had an estimated total retail value of hundreds of millions of dollars. Moreover, the Pro Network Entities generated over $100 million in revenue, and Aksoy received millions of dollars for his personal gain.

The devices the Pro Network Entities imported from China and Hong Kong were typically older, lower-model products – some of which had been sold or discarded – which Chinese counterfeiters then modified to appear to be genuine versions of new, enhanced, and more expensive Cisco devices. The Chinese counterfeiters often added pirated Cisco software and unauthorized, low-quality, or unreliable components – including components to circumvent technological measures added by Cisco to the software to check for software license compliance and to authenticate the hardware. Finally, to make the devices appear new, genuine, high-quality, and factory-sealed by Cisco, the Chinese counterfeiters allegedly added counterfeited Cisco labels, stickers, boxes, documentation, packaging, and other materials.

Fraudulent and counterfeit products sold by the Pro Network Entities suffered from numerous performance, functionality, and safety problems. Often, they would simply fail or otherwise malfunction, causing significant damage to their users’ networks and operations – in some cases, costing users tens of thousands of dollars. Customers of Aksoy’s fraudulent and counterfeit devices included hospitals, schools, government agencies, and the military.

Between 2014 and 2022, Customs and Border Protection (CBP) seized approximately 180 shipments of counterfeit Cisco devices being shipped to the Pro Network Entities from China and Hong Kong. In response to some of these seizures, Aksoy falsely submitted official paperwork to CBP under the alias “Dave Durden,” an identity that he used to communicate with Chinese co-conspirators. To try to avoid CBP scrutiny, Chinese co-conspirators broke the shipments up into smaller parcels and shipped them on different days, and Aksoy used a fake delivery address in Ohio. After CBP seized a shipment of counterfeit Cisco

products to Aksoy and the Pro Network Entities and sent a seizure notice, Aksoy often continued to order counterfeit Cisco products from the same supplier.

Between 2014 and 2019, Cisco sent seven letters to Aksoy asking him to cease and desist his trafficking of counterfeit goods. Aksoy responded to at least two of these letters by causing his attorney to provide Cisco with forged documents. In July 2021, agents executed a search warrant at Aksoy's warehouse and seized 1,156 counterfeit Cisco devices with a retail value of over $7 million.

The charge of conspiracy to which Aksoy pleaded guilty carries a maximum penalty of five years in prison. The charge of mail fraud to which Aksoy pleaded guilty carries a maximum penalty of 20 years in prison. Both offenses carry a fine of $250,000 or twice the gross gain or loss from the offense, whichever is greater. Pursuant to the plea agreement that the court conditionally accepted pending sentencing, Askoy faces a sentence of four to six years and six months in prison and must forfeit $15 million in illicit gains from his scheme and make full restitution to his victims. Sentencing is scheduled for Nov. 6, 2023.

Attorney for the United States Khanna and Assistant Attorney General Polite credited special agents and members of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) Los Angeles, under the direction of Acting Special Agent in Charge Eddy Wang; the U.S. Department of Defense, Defense Criminal Investigative Service, Western Field Office, under the direction of Special Agent in Charge Bryan Denny; the General Services Administration, Office of Inspector General, Southeast and Caribbean Division, under the direction of Special Agent in Charge Floyd Martinez; the U.S. Navy, Naval Criminal Investigative Service, Economic Crimes Field Office, under the direction of Special Agent in Charge Greg Gross; HSI Miami, under the direction of Special Agent in Charge Anthony Salisbury; and HSI Newark, under the direction of Special Agent in Charge Ricky J. Patel, with the investigation leading to today's guilty plea.

The CBP Electronics Center of Excellence; the CBP Los Angeles National Targeting and Analysis Center; and the CBP Office of Trade, Regulatory Audit and Agency Advisory Services, Miami Field Office, provided valuable assistance.

Anyone who believes they may be a victim of Aksoy or the Pro Network Entities, please visit http://www.justice.gov/largecases or https://www.justice.gov/usao-nj/united-states-v-onur-aksoy-pro-network for more information.

The Pro Network Entities include at least the following:

Pro Network Companies	Approximate Month and Year of Formation	State of Formation

Pro Network LLC	August 2013	New Jersey
Netech Solutions LLC	November 2016	Florida
Target Network Solutions LLC	January 2017	Florida
Easy Network LLC	April 2017	New Jersey
ACE NETUS LLC (a/k/a Ace Network)	April 2017	New Jersey
My Network Dealer LLC	April 2017	New Jersey
1701 Doral LLC	May 2017	New Jersey
Maytech Trading LLC	August 2017	Florida
NFD Trading LLC	September 2017	Florida
Kenet Solutions LLC	September 2017	Florida
Team Tech Global LLC	January 2018	New Jersey

Tenek Trading LLC	January 2018	Florida
The Network Gears LLC	February 2018	Florida
All Networking Solutions LLC (a/k/a All Network)	April 2018	Florida
San Network LLC	October 2018	Florida
Pro Network US Inc.	January 2019	Florida
Jms Tek LLC	August 2019	Florida
Renewed Equipment LLC	August 2021	Florida
Pro Ship US LLC	August 2021	Florida

Pro Network Amazon Storefronts	**Approximate Date of Earliest Known Activity**
Albus Trade Hub	January 2014
EasyNetworkUS	March 2014

Get Better Trade	July 2015
Mercadeal	February 2017
Netech Solutions	February 2018
Netkco LLC	September 2014
NFD Trading LLC	January 2018
Palm Network Solutions	June 2017
Renewed Equip	August 2017
Servtaur	August 2019
Smart Network	July 2017
SOS Tech Trade	August 2017
Target-Solutions	September 2020

TeamTech Global	March 2016
TradeOrigin US	August 2015

Pro Network eBay Storefronts	Approximate Date of Earliest Known Activity
connectwus	March 2014
futuretechneeds	July 2017
getbettertrade	July 2017
getontrade	April 2016
maytechtradingllc	October 2017
netechsolutions	April 2017
netkco	September 2014
nfdtrading	February 2018

smartnetworkusa	January 2014
tenektradingllc	May 2018

The government is represented by Assistant U.S. Attorney Andrew M. Trombly of the Cybercrime Unit in Newark, Senior Counsel Matthew A. Lamberti of the Department of Justice Computer Crime and Intellectual Property Section in Washington, D.C., and Senior Trial Counsel Barbara Ward of the Asset Recovery and Money Laundering Unit in Newark.

aksoy.indictment.pdf (784.98 KB)

Updated June 6, 2023

Topic

FINANCIAL FRAUD

Component

USAO - New Jersey

Press Release Number: 23-164