

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 22-
	:	
ONUR AKSOY	:	<u>Count 1</u>
a/k/a "Ron Aksoy"	:	18 U.S.C. § 371
a/k/a "Dave Durden"	:	(Conspiracy to Traffic in Counterfeit Goods and to Commit Mail and Wire Fraud)
	:	
	:	<u>Counts 2-4</u>
	:	18 U.S.C. §§ 1341 and 2
	:	(Mail Fraud)
	:	
	:	<u>Counts 5-8</u>
	:	18 U.S.C. §§ 1343 and 2
	:	(Wire Fraud)
	:	
	:	<u>Counts 9-11</u>
	:	18 U.S.C. §§ 2320(a)(1) and 2
	:	(Trafficking in Counterfeit Goods)

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT 1
**(Conspiracy to Traffic in Counterfeit Goods
and to Commit Mail and Wire Fraud – 18 U.S.C. § 371)**

Introduction

1. From at least as early as in or about August 2013 through at least as recently as in or about April 2022, defendant ONUR AKSOY ("AKSOY"), also known as "Ron Aksoy" and also known as "Dave Durden," ran a massive operation to traffic in fraudulent and counterfeit goods. During this period,

AKSOY conspired with suppliers in China and Hong Kong and others to import low-quality, modified computer networking devices with counterfeit labels, stickers, boxes, documentation, and packaging that made the goods falsely appear to be new, genuine, and high-quality devices manufactured and authorized by Cisco Systems, Inc. ("Cisco"). AKSOY and his coconspirators then resold those devices in the United States and around the world, falsely representing those devices to buyers as new, genuine, and high-quality Cisco products. During the conspiracy, AKSOY and his coconspirators imported and resold tens of thousands of these fraudulent and counterfeit devices, new and genuine versions of which carried an estimated total retail value of over one billion dollars.

Background

2. At various times relevant to this Indictment:
 - a. AKSOY was a New Jersey resident from at least as early as in or about 2013 through in or about August 2016. AKSOY has been a Florida resident since in or about August 2016.
 - b. AKSOY created, owned, and controlled "Pro Network," a criminal operation that purported to be in the business of selling genuine, high-quality computer networking equipment.
 - c. AKSOY operated Pro Network through a multitude of business entities under his full ownership and control (the "Pro Network

Entities”), which included Pro Network LLC, a New Jersey entity formed in August 2013, and Pro Network US Inc., a Florida entity formed in January 2019. The Pro Network Entities also included other front business entities, many associated with the names of other individuals but each under AKSOY’s full ownership and control, including at least the following:



Pro Network Entity	Approximate Month and Year of Formation	State of Formation
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
Jms Tek LLC	August 2019	Florida
Renewed Equipment LLC	August 2021	Florida
Pro Ship US LLC	August 2021	Florida

The Pro Network Entities also included a number of other merchant names, also under AKSOY’s full ownership and control, for which legal business

entities were never formed. The Pro Network Entities all purported to be in the business of selling genuine, high-quality computer networking equipment.

d. Cisco was a multinational corporation headquartered in San Jose, California that designed, manufactured, and sold computer networking equipment. The computer networking equipment that Cisco manufactured and sold included, but was not limited to, switches, which were devices that connect computers within a network; routers, which were devices that connect multiple networks together; and transceivers, which were devices that connect a single computer to a network.

e. Since at least as early as in or about January 2013, Cisco owned multiple trademarks registered on the principal register of the United States Patent and Trademark Office (the "Cisco Marks"), including the following, all of which were in use and used on or in connection with Cisco's goods and services:

Mark	Type	USPTO Registration Number	Designated Goods and Services
	Word and design	3759451	Computer networking equipment, including telecommunications switches
	Word	3709076	Computer networking equipment, including telecommunications switches

f. Cisco offered a warranty and technical service program for its products called “Smart Net.” Obtaining Smart Net coverage for a given Cisco device required an additional purchase from Cisco beyond the product itself. Because genuine Cisco devices each bore a unique serial number, once Smart Net coverage had been purchased for a given serial number, no other Cisco devices bearing that serial number would be eligible for Smart Net coverage.

g. Cisco maintained the “Device Coverage Checker,” an online tool that allowed users to enter the serial number of a Cisco device to determine if that product was already covered by Smart Net. Users were required to register for a Cisco account in order to access the Device Coverage Checker.

h. All wire transfers processed through the Fedwire Funds

Service ("Fedwire") were processed in a way that caused an electronic communication to travel through a Federal Reserve facility in East Rutherford, New Jersey.

The Conspiracy

3. From at least as early as in or about August 2013 through at least as recently as in or about April 2022, in Monmouth County, in the District of New Jersey, and elsewhere, the defendant,

ONUR AKSOY,
a/k/a "Ron Aksoy,"
a/k/a "Dave Durden,"

did knowingly and intentionally conspire and agree with others (collectively, the "Coconspirators") to commit offenses against the United States, namely:

a. To intentionally traffic in goods, specifically, computer networking equipment, while knowingly using on and in connection with such goods counterfeit marks, namely spurious marks that were identical to and substantially indistinguishable from marks that were in use and registered by Cisco on the principal register of the United States Patent and Trademark Office for those goods, the use of which counterfeit marks was likely to cause confusion, to cause mistake, and to deceive, contrary to Title 18, United States Code, Section 2320(a)(1); and

b. To devise a scheme and artifice to defraud, and to obtain monies, funds and other property by means of materially false and fraudulent

pretenses, representations, and promises, and, for the purpose of executing such a scheme and artifice to defraud, to knowingly cause to be delivered according to the directions thereon matters and things to be sent and delivered by a private and commercial interstate carrier, namely shipments of purported computer networking equipment, contrary to Title 18, United States Code, Sections 1341; and

c. To devise a scheme and artifice to defraud, and to obtain monies, funds and other property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such a scheme and artifice to defraud, to knowingly transmit and cause to be transmitted by means of wire, radio, and television communications in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, namely wire transfers of funds, contrary to Title 18, United States Code, Section 1343.

Goal of the Conspiracy

4. The goal of the conspiracy was for AKSOY and the Coconspirators to enrich themselves by (a) importing from China and Hong Kong into the United States low-quality, modified computer networking devices with counterfeit Cisco labels, stickers, boxes, documentation, and packaging that made the goods falsely appear to be new, genuine, and high-quality devices manufactured and authorized by Cisco (the "Counterfeit Cisco Products") and

(b) selling the Counterfeit Cisco Products to others by falsely representing them as new, genuine, and high-quality Cisco equipment.

Manner and Means of the Conspiracy

5. It was part of the conspiracy that:

a. Beginning at least as early as in or about 2014, AKSOY would regularly purchase large quantities of Counterfeit Cisco Products from various illicit suppliers based in China and Hong Kong (the “Supplier Coconspirators”), causing those products to be shipped from China and Hong Kong to the United States.

b. Many of the Counterfeit Cisco Products shipped to AKSOY by the Supplier Coconspirators were derived from what were originally genuine Cisco products—typically older, lower-model, or less expensive Cisco products, some of which had been sold or discarded—that the Supplier Coconspirators would obtain and then modify without authorization to make the devices appear as genuine versions of higher-model, enhanced, and more expensive Cisco products. To do so, the Supplier Coconspirators would make unauthorized modifications to both the hardware and the software of these devices, including the insertion into the devices of copyrighted Cisco software pirated by the Supplier Coconspirators and the installation onto the devices of unauthorized, low-quality, and unreliable components, including components to circumvent technological measures that Cisco had added to the software to

check for software license compliance and to authenticate the hardware. The Counterfeit Cisco Products built, modified, sold, and shipped by the Supplier Coconspirators bore counterfeit Cisco labels, stickers, boxes, documentation, and packaging, which falsely suggested that the products were new, genuine, and high-quality devices manufactured and authorized by Cisco.

c. In part as a result of the modifications made to the devices, the Counterfeit Cisco Products suffered from numerous and significant performance, functionality, and safety problems. At times, the Counterfeit Cisco Products would simply fail or otherwise malfunction, causing substantial damage to their users' networks and operations and, in some cases, costing the users tens of thousands of dollars.

d. To make their Counterfeit Cisco Products appear as new, genuine, high-quality, and factory-sealed, the Supplier Coconspirators would also fabricate fictitious identifiers for those devices, including false serial numbers—which would frequently be serial numbers that Cisco had applied to previously manufactured genuine products. The Supplier Coconspirators would then generate fraudulent labels, bearing counterfeit Cisco Marks, listing a product's fictitious identifiers and affix those labels to the same places on and inside the devices where Cisco itself affixes such labels to genuine products. The Supplier Coconspirators would also generate and apply fraudulent labels and packaging bearing counterfeit Cisco Marks to the boxes

in which the Counterfeit Cisco Products were shipped in order to make the Counterfeit Cisco Products appear as new, genuine, high-quality, and factory-sealed.

e. AKSOY and his subordinates at Pro Network (collectively, the “Pro Network Coconspirators”) would purchase Counterfeit Cisco Products from the Supplier Coconspirators for as much as approximately 99 percent off of Cisco’s manufacturer’s suggested retail price (“MSRP”), far below the prices offered for genuine Cisco products by authorized Cisco resellers.

f. AKSOY and the Supplier Coconspirators would take a variety of measures to evade detection by U.S. Customs and Border Protection (“CBP”) of the Counterfeit Cisco Products as they were being imported into the United States. For example:

i. AKSOY and the Supplier Coconspirators would routinely break up large orders of Counterfeit Cisco Products into multiple smaller shipments dispatched on different days. For instance, in one email sent from a Supplier Coconspirator to AKSOY on or about December 15, 2017, the Supplier Coconspirator informed AKSOY that it had separated certain orders placed by AKSOY into two different shipments, explaining: “**Consideration of the customs risk**, the goods separation. Hope you understand.” (Emphasis added.)

ii. On multiple occasions, AKSOY instructed the Supplier

Coconspirators to ship Counterfeit Cisco Products to two undeliverable addresses in Ohio (the “Ohio Addresses”). Then, and only after those shipments had cleared inspection by CBP, AKSOY and the Pro Network Coconspirators instructed the carriers for those shipments to change the final shipping address to Pro Network’s warehouse and headquarters in Doral, Florida (the “Pro Network Warehouse”).

g. AKSOY would wire payment for the Counterfeit Cisco Products to the Supplier Coconspirators’ overseas bank accounts from U.S. bank accounts under his ownership and control. In all, AKSOY wired at least approximately \$55 million to Supplier Coconspirator bank accounts.

h. After purchasing and receiving Counterfeit Cisco Products from the Supplier Coconspirators, AKSOY and the Pro Network Coconspirators would then sell those counterfeit products using the Pro Network Entities through a variety of channels, including Amazon, eBay, and direct sales, some of which were brokered through Pro Network’s own website. AKSOY and the Pro Network Coconspirators would sell the Counterfeit Cisco Products for as much as approximately 60 to 88 percent off of Cisco’s MSRP for those products. AKSOY and the Pro Network Coconspirators would falsely represent the Counterfeit Cisco Products to buyers as new, genuine, high-quality, and factory-sealed Cisco products. AKSOY and the Pro Network Coconspirators made these false representations on a variety of platforms, including email, the

Pro Network website, and Amazon and eBay storefronts controlled by AKSOY.

i. End users of the Counterfeit Cisco Products imported and resold by AKSOY and the Pro Network Coconspirators included hospitals, schools, government agencies, and the military. In fact, the Pro Network website claimed that Pro Network offered “IT [information technology] Infrastructure Built for Rigors of Government & Education.” However, the performance, security, safety, and reliability defects in the Counterfeit Cisco Products harmed the users’ networks and operations, sometimes causing significant financial losses.

j. In all, AKSOY generated at least approximately \$100 million in gross revenue through the sale of Counterfeit Cisco Products during the conspiracy.

k. Through Amazon alone, for example, AKSOY and the Pro Network Coconspirators, operating through approximately 15 separate seller accounts associated with various front Pro Network Entities and under AKSOY’s full ownership and control (the “Pro Network Amazon Storefronts”), sold approximately 61,310 Counterfeit Cisco Products, generating total sales of nearly \$50 million. These Amazon storefronts included the following:

Pro Network Amazon Storefront	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

1. Similarly, through eBay, AKSOY and the Pro Network Coconspirators, operating through at least 10 separate seller accounts associated with various front Pro Network Entities and under AKSOY's full ownership and control (the "Pro Network eBay Storefronts"), sold thousands of Counterfeit Cisco Products, generating total sales in the millions of dollars. The Pro Network eBay Storefronts included at least the following:

Pro Network eBay Storefront	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

m. Throughout the conspiracy, AKSOY and the Pro Network

Coconspirators would receive frequent notifications that the purported Cisco products that AKSOY was importing and selling were counterfeits. For example:

i. Between in or about February 2014 and in or about April 2022, CBP officials seized approximately 180 shipments of Counterfeit Cisco Products, comprising approximately 860 counterfeit devices, from numerous Supplier Coconspirators to AKSOY and the Pro Network Entities. The total MSRP of genuine versions of these seized Counterfeit Cisco Products exceeded \$5 million. After each of these seizures, CBP sent a notice to the listed importer on the seized shipment—either AKSOY, a Pro Network Entity, or a Pro Network employee—notifying the listed importer that the underlying shipment had been seized as counterfeit (each a “CBP Seizure Notice” and collectively, the “CBP Seizure Notices”). AKSOY retained copies of the CBP Seizure Notices in his office at the Pro Network Warehouse, many of which he kept inside a binder in his office with a cover page that read:

Pro Network

U.S. Customs & Border Protection

“Unauthorized personnel is not allowed to access this binder”

Moreover, even after CBP had seized a shipment of Counterfeit Cisco

Products imported by Aksoy and the Pro Network Entities from a particular Supplier Coconspirator, Aksoy would often continue to order Counterfeit Cisco Products from the same Supplier Coconspirator.

ii. Between in or about June 2014 and in or about August 2019, Cisco sent at least seven cease-and-desist letters to AKSOY and the Pro Network Entities demanding that they stop trafficking in Counterfeit Cisco Products (the “Cisco Cease-and-Desist Letters”). Among other things, the Cisco Cease-and-Desist letters stated that “counterfeit technology products potentially pose serious health and safety risks to the end users of such products” and demanded that “you immediately cease and desist importing, marketing and/or distributing ... counterfeit or infringing goods.”

iii. AKSOY also received numerous complaints from Pro Network’s customers, in some cases from end users who purchased directly from the Pro Network Entities and in other cases from resellers who purchased from the Pro Network Entities, who passed on complaints that they had received from the end users. End users and resellers complained that the devices they had obtained from the Pro Network Entities were counterfeit, substandard, used, or broken; had missing parts; did not work; were either not covered or were not eligible for Smart Net coverage; and in some instances had caused significant damage to

the end users' networks and operations.

iv. In response to counterfeiting complaints received from customers and Cisco, Amazon routinely removed Cisco product listings posted by AKSOY's Pro Network Amazon Storefronts and, in some instances, suspended or terminated entire Pro Network Amazon Storefronts. In response, AKSOY and the Pro Network Coconspirators communicated regarding Amazon's anti-counterfeiting actions. For example, in one email sent from a Pro Network employee to AKSOY on or about December 27, 2017, the employee wrote (translated from Turkish):

TTG [referring to TeamTech Global, a Pro Network Amazon Storefront] – ***There is another return on a product because it is counterfeit.*** Amazon deleted the [Amazon product listing]. This is the 2nd time it happens in [TeamTech Global]. As you know, in Easy [referring to EasyNetworkUS, a Pro Network Amazon Storefront], they closed the account on the 3rd.

(emphasis added). Similarly, in or about August 2021, eBay blocked and took offline numerous Pro Network eBay Storefronts in response to a counterfeiting complaint received from Cisco.

n. At least as early as in or about October 2016, AKSOY hired an attorney to represent him, Pro Network, and the Pro Network Entities ("Attorney-1"). Among other things, Attorney-1 communicated with Cisco on behalf of AKSOY and Pro Network in response to certain of the Cisco Cease-and-Desist Letters, which demanded that Pro Network produce documentation

regarding the purchase of Counterfeit Cisco Products, including correspondence, invoices, purchase orders, and other commercial documents. AKSOY caused Attorney-1 to submit forged documents to Cisco in response to these Cisco Cease-and-Desist Letters, including forged supplier invoices and a forged wire receipt.

o. AKSOY and the Pro Network Coconspirators maintained a significant inventory of Counterfeit Cisco Products at the Pro Network Warehouse. For example, on or about July 21, 2021, AKSOY possessed at the Pro Network Warehouse approximately 1,156 Counterfeit Cisco Products. The total MSRP of these Counterfeit Cisco Products was approximately \$7,011,296.

p. AKSOY and the Pro Network Coconspirators routinely communicated with each other and with others regarding the Counterfeit Cisco Products. For example:

i. On or about October 25, 2020, a Pro Network email account under AKSOY's control sent an email to a Supplier Coconspirator that certain products that the Supplier Coconspirator had shipped were counterfeit, defective, and/or reported stolen. For one of these products, the email stated: "WS-C3850-24XS-S **Counterfeit unit, has a soldered chipset on motherboard.**" (Emphasis added.) Nevertheless, AKSOY continued to procure Counterfeit Cisco Products

from this particular Supplier Coconspirator after this email was sent, including a shipment sent in or about March 2021 that AKSOY attempted to have initially shipped to one of the Ohio Addresses and then diverted to the Pro Network Warehouse.

ii. On multiple occasions, AKSOY and the Pro Network Coconspirators discovered that Counterfeit Cisco Products they had obtained from the Supplier Coconspirators bore duplicate serial numbers—even though, as AKSOY well knew, a genuine Cisco product would never bear the same serial number as another genuine Cisco product. On or about August 14, 2019, for example, the following exchange took place within a group chat including AKSOY and three Pro Network Coconspirators (“PNCC-1,” “PNCC-2,” and “PNCC-3”):

Sender	Message
PNCC-1	Big problem
PNCC-1	[Attaching two photographs, the second photograph depicting two Cisco products with boxes bearing identical serial numbers]
PNCC-1	Same serials on second picture ^
PNCC-2	😬
PNCC-3	How the hell did we not catch that?
AKSOY	Can you email this.. I'll check tonight
PNCC-3	We should consider flagging duplication of serials in the system
AKSOY	Yes
PNCC-1	Yes 😬😬

iii. AKSOY and the Pro Network Coconspirators generated

and maintained inventory lists, which they at times transmitted through Pro Network email accounts under AKSOY's control and which AKSOY retained on his own computer. These inventory lists contained notations that the purported Cisco products in Pro Network's inventory were counterfeit, defective, and of low quality. For example, one inventory list contained notations for three separate Counterfeit Cisco Products—each shipped by the same Supplier Coconspirator to Pro Network in or about May 2020—that read: “[Serial number] shows as [different Cisco product ID] in Cisco system, **counterfeit.**” (Emphasis added.) Other notations included:

- “Issues with the [serial number]. [Serial number] shows as stolen in Cisco system. [Return to vendor]”
- “Sealed box. Wrong [serial number]”
- “Unit doesn't power on”
- “Defective RAM module, embedded on motherboard”
- “Unit works for a while and then suddenly freezes.”

iv. On or about November 14, 2014, AKSOY exchanged the following messages, translated from Turkish, with another Pro Network Coconspirator (“PNCC-4”), in which AKSOY and PNCC-4 referenced two other individuals (“Individual-1” and “Individual-2”):

Sender	Message
AKSOY	[Individual-1] called yesterday.
PNCC-4	What does he say, [Individual-2]?
PNCC-4	You should have told him, "I am opening an office in Turkey."
AKSOY	Well, the same old stuff. He tells me, "You are selling counterfeit, you might go to jail".
AKSOY	The Chinese built a factory and directly started manufacturing counterfeit CISCO.
PNCC-4	Bro, they haven't put you in jail in the last 5 years.
AKSOY	Yeah, exactly.

v. On or about May 26, 2015, AKSOY and PNCC-4 exchanged the following messages, translated from Turkish except where noted:

Sender	Message
AKSOY	In the meantime, another document came from Customs. The papers that you sent are not in order. We will give the products to CISCO, they say.
PNCC-4	Whatever that company is, move the sales to the other one, and I think you should decrease your stock.
PNCC-4	In 3-4 months, CISCO...
PNCC-4	...will come to you.
AKSOY	Yes.
PNCC-4	Do you still continue to buy products from that supplier?
AKSOY	[In English] Main supplier
PNCC-4	[In English] Ok good luck than..

q. AKSOY and the Pro Network Coconspirators used Cisco's Device Coverage Checker to ensure that the Counterfeit Cisco Products that were either offered for sale or shipped to them by the Supplier Coconspirators

did not bear serial numbers already covered by Smart Net, which would signal to AKSOY's customers that the devices he was selling to them were counterfeit. To evade detection by Cisco and their customers, AKSOY and the Pro Network Coconspirators accessed the Device Coverage Checker to check serial numbers of Counterfeit Cisco Products using a Cisco account registered under the name of an individual and business entity purportedly located in Bolivia (the "Bolivian Cisco Account").

r. To further conceal his conduct and evade detection by CBP and law enforcement, AKSOY would at times use the alias "Dave Durden" to conduct Pro Network business, including communicating with the Supplier Coconspirators and receiving shipments of Counterfeit Cisco Products from the Supplier Coconspirators. However, no actual person named "Dave Durden" was ever associated with Pro Network.

s. In some instances, AKSOY submitted completed written response forms to CBP Seizure Notices—notwithstanding a warning on those forms that false statements and claims could result in criminal prosecution and imprisonment for obstruction of justice and perjury—falsely claiming to be "Dave Durden" or simply "Dave" and signing that name. AKSOY retained copies of these false response forms in his Pro Network Warehouse office.

t. AKSOY derived millions of dollars for his personal gain through the conspiracy.

Overt Acts

6. In furtherance of the conspiracy and to effect the conspiracy's objects, AKSOY and the Coconspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

- a. On or about August 15, 2013, AKSOY formed and caused to be formed Pro Network LLC, a New Jersey business entity.
- b. On or about March 28, 2017, in response to a CBP Seizure Notice to "Dave Durden" regarding the seizure of three counterfeit Cisco switches valued at \$6,294, AKSOY filed a form to abandon the property on which he falsely claimed to be "Dave Durden" and signed that name.
- c. On or about April 4, 2017, AKSOY formed and caused to be formed Easy Network LLC, a New Jersey business entity.
- d. On or about April 27, 2017, AKSOY formed and caused to be formed ACE NETUS LLC (a/k/a "Ace Network"), a New Jersey business entity.
- e. On or about April 27, 2017, AKSOY formed and caused to be formed My Network Dealer LLC, a New Jersey business entity.
- f. On or about June 12, 2017, in response to a CBP Seizure Notice to "Dave Durden" regarding the seizure of five counterfeit Cisco switches valued at \$2,091, AKSOY filed a form to abandon the property on which he falsely claimed to be "Dave Durden" and signed that name.

g. On or about January 1, 2018, AKSOY formed and caused to be formed Team Tech Global LLC, a New Jersey business entity.

h. On or about February 2, 2018, AKSOY caused one purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-2960S-48FPD-L, to be shipped by UPS to a location in Red Bank, New Jersey.

i. On or about February 2, 2018, AKSOY caused one purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-C2960X-48FPS-L, to be shipped by UPS to a location in Red Bank, New Jersey.

j. On or about April 13, 2018, AKSOY caused \$74,200 to be transferred by wire from a U.S. bank account under his ownership and control to a bank account in Hong Kong under the control of a Supplier Coconspirator.

k. On or about April 8, 2019, AKSOY caused \$185,623 to be transferred by wire from a U.S. bank account under his ownership and control to a bank account in Hong Kong under the control of a Supplier Coconspirator.

l. On or about July 1, 2019, AKSOY caused \$154,571 to be transferred by wire from a U.S. bank account under his ownership and control to a bank account in Hong Kong under the control of a Supplier Coconspirator.

m. On or about August 9, 2019, AKSOY and the Pro Network Coconspirators registered the Bolivian Cisco Account with Cisco.

n. On or about August 17, 2019, AKSOY caused Attorney-1 to transmit a forged supplier invoice to Cisco in response to a Cisco Cease-and-Desist Letter.

o. On or about August 26, 2019, AKSOY caused Attorney-1 to transmit a forged supplier invoice and a forged wire receipt to Cisco in response to a Cisco Cease-and-Desist Letter.

p. On or about December 16, 2019, AKSOY caused \$13,264 to be transferred by wire from a U.S. bank account under his ownership and control to a bank account in Hong Kong under the control of a Supplier Coconspirator.

q. On or about December 18, 2019, AKSOY caused one purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-C2960S-48FPD-L, to be shipped by UPS to a location in Red Bank, New Jersey.

All in violation of Title 18, United States Code, Section 371.

COUNTS 2 THROUGH 4
(Mail Fraud – 18 U.S.C. §§ 1341 and 2)

1. Paragraphs 1, 2, 4, 5, and 6 of Count 1 of this Indictment are realleged here.

2. From at least as early as in or about August 2013 through at least as recently as in or about April 2022, in Monmouth County, in the District of New Jersey, and elsewhere, the defendant,

ONUR AKSOY,
a/k/a “Ron Aksoy,”
a/k/a “Dave Durden,”

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud victims of money and property, namely the scheme and artifice to defraud described in Count 1 of this Indictment, and on or about the dates listed below, in the District of New Jersey and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, did knowingly cause to be delivered by private and commercial interstate carriers according to the direction thereon the shipments listed below, each shipment constituting a separate Count of this Indictment:

Count	Approximate Date Shipment Received	City and State Shipment Received	Carrier	Shipment
2	February 2, 2018	Red Bank, New Jersey	UPS	One purportedly new, genuine, and high-quality boxed Cisco

				switch, product ID WS-2960S-48FPD-L
3	February 2, 2018	Red Bank, New Jersey	UPS	One purportedly new, genuine, and high-quality boxed Cisco switch, product ID WS-C2960X-48FPS-L
4	December 18, 2019	Red Bank, New Jersey	UPS	One purportedly new, genuine, and high-quality boxed Cisco switch, product ID WS-C2960S-48FPD-L

In violation of Title 18, United States Code, Section 1341 and Section 2.

COUNTS 5 THROUGH 8
(Wire Fraud – 18 U.S.C. §§ 1343 and 2)

1. Paragraphs 1, 2, 4, 5, and 6 of Count 1 of this Indictment are realleged here.

2. From at least as early as in or about August 2013 through at least as recently as in or about April 2022, in Bergen County, in the District of New Jersey and elsewhere, the defendant,

ONUR AKSOY,
a/k/a “Ron Aksoy,”
a/k/a “Dave Durden,”

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud victims of money and property, namely the scheme and artifice to defraud described in Count 1 of this Indictment, and on or about the dates listed below, in the District of New Jersey and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, did knowingly and intentionally transmit and cause to be transmitted by means of wire, radio and television communications in interstate and foreign commerce, certain writings, signs, signals, pictures and sounds, as listed below, each transmission constituting a separate Count of this Indictment:

Count	Approximate Date of Transmission	Wire Transmission
5	April 13, 2018	Transfer of \$74,200 from a U.S. bank account ownership and control to a bank account in Hong Kong controlled by a Supplier Coconspirator, by an

		interstate and foreign wire that traveled through New Jersey via Fedwire
6	April 8, 2019	Transfer of \$185,623 from a U.S. bank account under AKSOY's ownership and control to a bank account in Hong Kong controlled by a Supplier Coconspirator, by an interstate and foreign wire that traveled through New Jersey via Fedwire
7	July 1, 2019	Transfer of \$154,571 from a U.S. bank account under AKSOY's ownership and control to a bank account in Hong Kong controlled by a Supplier Coconspirator, by an interstate and foreign wire that traveled through New Jersey via Fedwire
8	December 16, 2019	Transfer of \$13,264 from a U.S. bank account under AKSOY's ownership and control to a bank account in Hong Kong controlled by a Supplier Coconspirator, by an interstate and foreign wire that traveled through New Jersey via Fedwire

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNTS 9 THROUGH 11
(Trafficking in Counterfeit Goods – 18 U.S.C. §§ 2320(a)(1) and 2)

1. Paragraphs 1, 2, 4, 5, and 6 of Count 1 of this Indictment are realleged here.

2. On or about the dates listed below, in Monmouth County, in the District of New Jersey, and elsewhere, the defendant,

ONUR AKSOY,
a/k/a “Ron Aksoy,”
a/k/a “Dave Durden,”

did intentionally traffic and attempt to traffic in goods, namely the goods listed below, while knowingly using on and in connection with such goods counterfeit marks, namely spurious marks that were identical to and substantially indistinguishable from marks that were in use and registered by Cisco on the principal register of the United States Patent and Trademark Office for those goods, the use of which counterfeit marks was likely to cause confusion, to cause mistake, and to deceive, each instance of trafficking constituting a separate Count of this Indictment:

Count	Approximate Date of Trafficking	Goods
9	February 2, 2018	One purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-2960S-48FPD-L
10	February 2, 2018	One purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-C2960X-48FPS-L

11	December 18, 2019	One purportedly new, genuine, and high-quality boxed Cisco switch with counterfeit Cisco marks, product ID WS-C2960S-48FPD-L
----	-------------------	--

In violation of Title 18, United States Code, Section 2320(a)(1) and Section 2.

FORFEITURE ALLEGATIONS

Count 1

1. Upon conviction of one or more objects of the conspiracy offense charged in Count 1 of this Indictment, the defendant,

ONUR AKSOY,
a/k/a "Ron Aksoy,"
a/k/a "Dave Durden,"

shall forfeit to the United States:

- a. Pursuant to 18 U.S.C. § 2323(b),
 - i. Any and all articles, the making or trafficking of which is prohibited under 18 U.S.C. § 2320;
 - ii. Any and all property used, or intended to be used, in any manner or part to commit or facilitate the conspiracy to violate 18 U.S.C. § 2320(a)(1) as charged in Count 1 of this Indictment; and
 - iii. Any and all property, real and personal, constituting or derived from proceeds the defendant obtained directly or indirectly as a result of the conspiracy to violate 18 U.S.C. § 2320(a)(1) as charged in Count 1 of this Indictment; and
- b. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), all property, real and personal, the defendant obtained that constitutes or is derived from proceeds traceable to the conspiracy to violate 18 U.S.C. § 1341 or 1343 as charged in Count 1 of this Indictment;

and all property traceable to such property.

2. The property subject to forfeiture includes, but is not limited to, all right, title, and interest of defendant ONUR AKSOY in the real property and appurtenances known as 6783 SW 104 Street, Pinecrest, Miami-Dade County, Florida 33156, Folio: 20-5002-000-1100.

Counts 2 Through 8

3. Upon conviction of one or more of the offenses charged in Counts 2 through 8 of this Indictment, the defendant,

ONUR AKSOY,
a/k/a "Ron Aksoy,"
a/k/a "Dave Durden,"

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), all property, real and personal, the defendant obtained that constitutes or is derived from proceeds traceable to the commission of each such offense.

4. The property subject to forfeiture includes, but is not limited to, all right, title, and interest of defendant ONUR AKSOY in the real property and appurtenances known as 6783 SW 104 Street, Pinecrest, Miami-Dade County, Florida 33156, Folio: 20-5002-000-1100.

Counts 9 Through 11

5. Upon conviction of one or more of the offenses charged in Counts 9 through 11 of this Indictment, the defendant,

ONUR AKSOY,
a/k/a "Ron Aksoy,"
a/k/a "Dave Durden,"

shall forfeit to the United States, pursuant to 18 U.S.C. § 2323(b):

- a. Any and all articles, the making or trafficking of which is prohibited under 18 U.S.C. § 2320;
- b. Any and all property used, or intended to be used, in any manner or part to commit or facilitate the commission of each violation of 18 U.S.C. § 2320(a)(1); and
- c. Any and all property, real and personal, constituting or derived from proceeds the defendant obtained directly or indirectly as a result of the commission of each violation of 18 U.S.C. § 2320(a)(1), and all property traceable to such property.

6. The property subject to forfeiture includes, but is not limited to, all right, title, and interest of defendant ONUR AKSOY in the real property and appurtenances known as 6783 SW 104 Street, Pinecrest, Miami-Dade County, Florida 33156, Folio: 20-5002-000-1100.


SUBSTITUTE ASSETS PROVISION

7. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described above.

A True Bill,


Foreperson



VIKAS KHANNA
Attorney for the United States
Acting Under the Authority of 28 U.S.C. § 515

CASE NUMBER: 22-

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

ONUR AKSOY, a/k/a "Ron Aksoy" and "Dave Durden"

INDICTMENT FOR

18 U.S.C. § 371; 18 U.S.C. § 1341; 18 U.S.C. § 1343;
18 U.S.C. § 2320(a)(1); 18 U.S.C. § 2

A True Bill,
Foreperson

VIKAS KHANNA

ATTORNEY FOR THE UNITED STATES
ACTING UNDER AUTHORITY CONFERRED BY 28 U.S.C. § 515
NEWARK, NEW JERSEY

ANDREW M. TROMBLY
ASSISTANT UNITED STATES ATTORNEY
NEWARK, NEW JERSEY
973-645-2847

MATTHEW A. LAMBERTI
SENIOR COUNSEL, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
WASHINGTON, DISTRICT OF COLUMBIA
202-353-0381