UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	Honorable Cathy L. Waldor
	:	
MUSA KARAMAN	:	Mag. No. 22-9206
	:	
	:	**FILED UNDER SEAL**

I, Robert S. Pinches, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations, and that this complaint is based on the following facts:

SEE ATTACHMENT B

/s/ Robert S. Pinches/AMT

Robert S. Pinches, Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations
Special Agent Robert S. Pinches attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on May 18, 2022

Honorable Cathy L. Waldor
United States Magistrate Judge

/s/ Cathy L. Waldor/AMT
Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Mail and Wire Fraud)

From at least as early as in or around September 2017 through at least as recently as in or around May 2021, in Passaic County, in the District of New Jersey, and elsewhere, the defendant,

MUSA KARAMAN,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to cause to be delivered by mail according to the directions thereon matters and things to be sent and delivered by a private and commercial interstate carrier, and to transmit and cause to be transmitted by means of wire, radio, and television communications in interstate and foreign commerce certain writings, signs, signals, and sounds, contrary to Title 18, United States Code, Sections 1341 and 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Robert S. Pinches, am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background

1. At times relevant to this Complaint:

a. Business-1 was a New Jersey limited liability company incorporated in 2014. Business-1 maintained a warehouse in Woodland Park, New Jersey, which served as Business-1's primary place of business (the "Business-1 Warehouse").

b. The defendant, Musa Karaman ("KARAMAN"), resided in North Arlington, New Jersey. Karaman was a principal and partial owner of Business-1 and its associated entities.

c. Israfil "David" Demir, a co-conspirator previously charged in this matter, resided in Secaucus, New Jersey. Demir was a principal and partial owner of Business-1 and its associated entities. Demir's legal name was Israfil, but he also used the name "David," including in correspondence relating to Business-1 and it associated entities.

d. CC-1, a presently uncharged co-conspirator, resided in Hawthorne, New Jersey. CC-1 was a principal and partial owner of Business-1 and its associated entities.

e. Cisco Systems, Inc. ("Cisco") was a major U.S. technology conglomerate headquartered in San Jose, California. Among other services and products, Cisco designed, manufactured, and sold networking devices, *i.e.*, computer hardware that allowed computers connected by a network to communicate with each other. The networking devices relevant to this Complaint included "switches" and "transceivers," which are devices used to facilitate the transmission of signals between computers on a computer network. In essential terms, a switch connects multiple computers within a network, and a computer connects a device to a network. Relevant Cisco devices also included power supply devices.

f. I know, from training, experience, and investigation, that Cisco's networking devices are used in information networks in the United States and across the world. Many of these devices are purchased and used by U.S. government and military entities, hospitals, schools, and other critical sectors, and are used in sensitive and essential applications. A wide variety of critical infrastructure relies on such networking equipment to maintain the security and integrity of government, medical, and business data storage, transfer, and communications. Sensitive and important functions performed by the government, as well as both public- and private-sector entities, rely on the performance of high-quality networking products. These functions are endangered by lower quality counterfeits.

g. Cisco owned numerous registered trademarks, including word and design trademarks.

h. I also know, from training, experience, and investigation that counterfeit products that bear Cisco trademarks without permission provide customers with the false assurance that those products are reliable and conform with Cisco's standards, come with applicable Cisco warranties, can be immediately placed under a Cisco service support contract, and have been produced in accordance with Cisco's quality assurance standards.

i. I also know, from training, experience, and investigation, that counterfeit Cisco products often use pirated versions of Cisco software—in many cases, older and outdated software that does not necessarily operate correctly—leaving users exposed to security vulnerabilities that Cisco had detected and fixed in current and genuine software versions. For this reason, using counterfeit Cisco products can expose a user's network to security or intrusion vulnerabilities.

j. Supplier-1 was a supplier of counterfeit Cisco devices headquartered in Beijing, China. Supplier-1 was not affiliated with Cisco in any way and was not an authorized reseller or distributor of Cisco products.

k. CC-2, a presently uncharged co-conspirator, was a sales representative for Supplier-1.

l. Supplier-2 was another supplier of counterfeit Cisco devices headquartered in Beijing, China. Supplier-2 was not affiliated with Cisco in any way and was not an authorized reseller or distributor of Cisco products.

m. CC-3, a presently uncharged co-conspirator, was a sales representative for Supplier-2.

n. Supplier-3 was another supplier of counterfeit Cisco devices headquartered in China. Supplier-3 was not affiliated with Cisco in any way and was not an authorized reseller or distributor of Cisco products.

o. Supplier-4 was another supplier of counterfeit Cisco devices headquartered in China. Supplier-4 was not affiliated with Cisco in any way and was not an authorized reseller or distributor of Cisco products.

p. Distributor-1 was a company based in Pennsylvania. Distributor-1 was a major authorized distributor and reseller of genuine Cisco products.

Overview of the Conspiracy

2. An investigation conducted by HSI and the U.S. Department of Defense, Office of Inspector General has shown that KARAMAN, Demir, CC-1, and others (the "Conspirators") have, from at least as early as September 2017 through at least as recently as May 2021, executed a scheme to knowingly import counterfeit Cisco networking devices from various illicit overseas suppliers, including suppliers based in China and Hong Kong (such as Supplier-1, Supplier-2, Supplier-3, and Supplier-4), and to then sell those counterfeit Cisco devices to U.S. customers as genuine Cisco products (the "Conspiracy").

3. During this time, KARAMAN, Demir, and CC-1 used various business entities that they either owned and/or controlled, including Business-1 (the "Trafficking Business Entities"), to sell products that were packaged and built to appear like genuine Cisco networking devices. But in fact, virtually all of the Cisco products sold by the Conspirators through the Trafficking Business Entities were counterfeits (the "Counterfeit Cisco Products"). In other words, the Counterfeit Cisco Products were devices that Cisco did not authorize and that bore Cisco trademarks and/or were packaged with counterfeit labels bearing Cisco trademarks without Cisco's permission.

4. The numerosity of the Trafficking Business Entities appears to serve no legitimate business purpose. To the contrary, I know from training and experience that counterfeit traffickers frequently form and conduct transactions through multiple business entities to evade detection, identification, and enforcement by either intellectual-property owners (like Cisco), marketplaces (like Amazon), and law enforcement.

5. Evidence obtained by law enforcement, including bank records, records of deliveries by interstate carriers, and emails sent and received by the Conspirators from Business-1 email accounts, show that the Conspirators have acquired Counterfeit Cisco Products from multiple overseas suppliers. Many of these suppliers, including Suppliers-1, -2, -3, -4, and -5, are situated in China. I know from training, experience, and investigation that many suppliers and manufacturers of counterfeit Cisco products operate in China, at least in part

because of China's comparatively lax enforcement of U.S. intellectual property rights.

6. The Conspirators have sold the Counterfeit Cisco Products through multiple channels, including online marketplaces like Amazon, where the Conspirators have operated multiple online storefronts associated with the Trafficking Business Entities. The Conspirators also have sold Counterfeit Cisco Products directly from their own websites, also associated with various Trafficking Business Entities, many of which falsely touted the authenticity of the Cisco products for sale. For example, one such website claimed, falsely, that "[a]ll of [its] products are factory new sealed and clean serial."

Seized Shipments and Notifications to the Conspirators

7. Between in or around September 2017 and in or around May 2021, U.S. Customs officials seized more than 20 shipments of purported Cisco networking devices, including switches and transceivers, from various suppliers in China and other overseas locations that were destined for various locations controlled by the Conspirators. The majority of these seized shipments were addressed to the Business-1 Warehouse. At least two of these seized shipments listed Supplier-1 as the named exporter. Many of the shipments listed bogus names for the importer, which I know, based on training and experience, to be a tactic used by counterfeit traffickers to evade detection.

8. Cisco has analyzed the supposed Cisco networking devices contained in these seized shipments. These products bore Cisco trademarks and were clearly designed and intended to mimic actual Cisco networking devices. Cisco has verified to law enforcement, however, that the supposed Cisco networking devices in the seized shipments were actually Counterfeit Cisco Products based on, among other indications, packaging irregularities and internal circuitry within these products.

9. The total manufacturer's suggested retail price ("MSRP") of the genuine analogues of the seized Counterfeit Cisco Products totals at least approximately $3.8 million.

10. It is standard procedure for U.S. Customs, after an international shipment is seized, to send a seizure notice to the listed importer on that shipment that articulates the basis for the seizure. In this matter, law enforcement has verified that such seizure notices were sent by U.S. Customs to the listed importer on each of the seized shipments of Counterfeit Cisco Products, and that these seizure notices advised that the shipments contained Counterfeit Cisco Products. The identifying information listed for the importer on these seized shipments included, in each instance, either: (i) a Conspirator name, (ii) a Trafficking Business Entity name, and/or (iii) physical addresses known to be controlled by the Conspirators, such as the Business-1 Warehouse.

11. In addition, Cisco sent multiple cease-and-desist letters to the Conspirators and to the Trafficking Business Entities, including letters sent in or around April 2019 and in or around August 2019, advising that the products included in the seized shipments were counterfeits and directing the Conspirators and Trafficking Business Entities to cease selling counterfeit Cisco products.

12. Notwithstanding these U.S. Customs seizure notices and Cisco cease-and-desist letters, the Conspirators continued to import Counterfeit Cisco Products—frequently from many of the same suppliers that shipped the Counterfeit Cisco Products seized by U.S. Customs as described above.

The August 2020 Controlled Purchase

13. In or about August 2020, law enforcement visited the Amazon online storefront of a particular Trafficking Business Entity ("TBE-1") (the "TBE-1 Storefront"). At that time, the TBE-1 Storefront advertised a particular model of a Cisco switch in "new" condition. The listed price was $1,455.52. By contrast, the MSRP of a genuine, new model of that switch is, according to Cisco, $12,793.30.

14. Law enforcement ordered the switch from the TBE-1 Storefront. The ordered switch was delivered in or about September 2020. The return address on the switch was "SHIPPING DEPARTMENT" at the Business-1 Warehouse address. Subsequent analysis of the switch conducted by Cisco found the switch to be a Counterfeit Cisco product.

15. Records obtained in this investigation show that the counterfeit switch was procured by the Conspirators from Supplier-1 earlier in or around August 2020.

The May 2021 Search of the Business-1 Warehouse and Arrest of Demir

16. On or about May 26, 2021, law enforcement executed a lawfully obtained search warrant for the Business-1 Warehouse. During this search, law enforcement discovered thousands of purported Cisco devices, nearly all of which were found during later analysis by Cisco to be Counterfeit Cisco Products. Specifically, law enforcement seized around 7,260 transceivers, which bore a total MSRP of around $13,774,576. Law enforcement also seized around 15 switches, which bore a total MSRP of around $241,000. Law enforcement also discovered a number of purported Cisco power supply devices to which counterfeit labels bearing Cisco trademarks were affixed.

17. According to Cisco, this was one of the largest volumes of counterfeit transceivers ever seized in the United States, and the value of this seizure was unprecedented.

18. Also on or about May 26, 2021, a criminal complaint against Demir in this matter was unsealed, and law enforcement executed a lawfully obtained arrest warrant for Demir based on that complaint.

Shipments to Home Addresses of KARAMAN and Other Conspirators Under Bogus Names

19. KARAMAN and the Conspirators would routinely have purported Cisco products—presumably Counterfeit Cisco Products—shipped to their own home addresses, frequently directed to bogus recipient names. I know, based on training, experience, and investigation, that traffickers of counterfeit goods frequently use multiple shipment addresses under multiple and often bogus names to evade detection by U.S. Customs and law enforcement. Law enforcement is aware of no legitimate business purpose served by listing bogus names on these shipments—or, indeed, by having the shipments shipped to residential addresses at all rather than to the Business-1 Warehouse.

20. For example, at times relevant to this Complaint, KARAMAN resided at a residential address in North Arlington, New Jersey (the "KARAMAN Address"). A shipment of purported Cisco products, which Cisco later confirmed to be Counterfeit Cisco Products, was seized by U.S. Customs on or about August 29, 2018. That seized shipment was directed to "SAM KAR" at the KARAMAN Address. Law enforcement is unaware of any actual individual named "Sam Kar" relevant to this matter.

21. Records obtained in this investigation show that the Conspirators placed the following purchase orders for purported Cisco devices from the following China-based suppliers, all to be shipped to the KARAMAN Address. Law enforcement is unaware of any actual people with the listed names who are relevant to this matter.[1]

Approximate Date of Purchase Order	Supplier	Listed Recipient Name
July 17, 2018	Supplier-3	Sam Kar
October 4, 2018[2]	Supplier-2	Emily Solmaz
October 16, 2018	Supplier-2	Edward Solmaz
February 26, 2019	Supplier-2	Jesse Jordan
March 6, 2019	Supplier-2	James Jordan
March 12, 2019	Supplier-2	Alex Jay
March 15, 2019	Supplier-2	Jesse Jay

[1] On or about August 4, 2020, a purchase order for Cisco devices was sent to Supplier-1 directing shipment to KARAMAN's wife at the KARAMAN Address.

[2] In his email to CC-3 transmitting this purchase order to Supplier-2, Demir wrote: "You can make 3 shipment for custom issue."

March 25, 2019	Supplier-2	Samantha Gul
April 4, 2019	Supplier-2	Sam Gul
April 12, 2019	Supplier-2	Sam Gul
June 29, 2020	Supplier-4	Enes Kar

The Demir Email Account

22. Law enforcement has obtained by lawful search warrant and reviewed the contents of a Google-hosted email account used by Demir to conduct Business-1 business (the "Demir Email Account"). The email address of the Demir Email Account was "david@[Business-1][.]com."

23. Emails from the Demir Email Account show that Demir would regularly procure Counterfeit Cisco Products from overseas suppliers, including primarily Supplier-1 and Supplier-2, but also Suppliers-3, and -4, as well as other suppliers. CC-2 was Demir's regular point of contact at Supplier-1, and CC-3 was Demir's regular point of contact at Supplier-2. Demir would frequently email both CC-2 and CC-3 to, among other things, inquire about inventory and pricing and to place orders.

24. In one such email exchange in November and December 2019:

a. A Business-1 customer ("Customer-1") had ordered and taken shipment of Cisco networking devices from Business-1 in Fall 2019 (the "Fall 2019 Devices") and found during testing that those devices were Counterfeit Cisco Products. Specifically, Cisco devices contained codes, called "organizationally unique identifier" ("OUI") codes, that relate to where a given product was manufactured. In an email to the Demir Email Account sent in or around November 2019, Customer-1 explained that the Fall 2019 Devices contained OUI codes that pointed to a manufacturing location where genuine versions of those devices were never actually manufactured. I know from training, experience, and investigation that this type of mismatch in the OUI codes of Cisco devices is an indicator of counterfeiting. Customer-1 also told Demir that it would quarantine the Fall 2019 Devices to avoid liability for trafficking in counterfeit products.

b. In response, Demir repeatedly emailed Customer-1 in or around November-December 2019, falsely claiming that the Fall 2019 Devices had been procured from an authorized Cisco channel. As support for this false claim, Demir attached partially redacted invoices for the Fall 2019 Devices bearing Cisco logos and trademarks, which I believe were intended to make these documents appear like authentic invoices of either Cisco itself or an authorized Cisco reseller.

c. In fact, however, emails and records in the Demir Email Account show that Demir had procured the Fall 2019 Devices from

Supplier-1, not from either Cisco or an authorized Cisco reseller. Moreover, Cisco has confirmed to law enforcement that the purported Cisco invoice sent by Demir to Customer-1 was a forgery.

d. After being alerted by the customer of the counterfeit issue, Demir emailed CC-2 not to ask whether Fall 2019 Devices were in fact genuine—but rather to ask CC-2 for "replacement parts" from Supplier-1 for the Fall 2019 Devices.

e. Later in or around December 2019, Demir emailed CC-2 again. Demir wrote:

> One of the engineer said [manufacturing location] [Cisco] modules never use [different manufacturing location] OUI and china still don't know that. If they find out following instruction they will increase their ability and nobody can understand they are fake or not. 😊
>
> These are the issue. Copy that to your customer. They will understand.

Beneath this text, Demir then provided the list of OUI codes that he had received from Customer-1 indicating that the Fall 2019 Devices were Counterfeit Cisco Products.

f. Similarly, in or around January 2020, Demir emailed CC-3, the Business-1 Conspirators' point of contact for Supplier-2. In that email, Demir wrote:

> One of the customers complaint little bit. They sent me some information. If you share with your supplier they can be careful about counterfeit issue. Here is the American engineers test result:

As with the December 2019 email to CC-2, beneath this text, Demir then provided the list of OUI codes he had received from Customer-1 indicating that the Fall 2019 Devices were Counterfeit Cisco Products.

25. In or around January 2020, after Customer-1 had requested to purchase more Cisco devices from Business-1, both KARAMAN and Customer-1 exchanged the following emails (copying Demir) related to the Fall 2019 Devices:

Sender	Email Message
KARAMAN	Hello [Customer-1], This is Musa from MIS Enterprise LLC. We will not fulfill any orders from you until we get our money from previous orders. I really appreciate your business but this is not something we can continue doing it.
Customer-1	Musa Which orders are you talking about, are you talking about the counterfeit product that we had to quarantine? Please be specific? Best Regards, [Customer-1]
KARAMAN	Yes the products that you quarantine, I paid for those items and I cannot get my money back, I lost money. Best regards

26. The "counterfeit product[s]" discussed in this exchange appear to have included the Fall 2019 Devices.

KARAMAN and Demir Wires of Money to Counterfeit Suppliers

27. Law enforcement has also obtained and reviewed records for a bank account under the name of one of the Trafficking Business Entities, for which KARAMAN and Demir were signatories at various times. Those records show that the Conspirators, and in particular KARAMAN and Demir, have wired significant amounts of money to multiple overseas suppliers of Counterfeit Cisco Products during the Conspiracy. All told, the Conspirators have wired over $1.2 million to bank accounts in China and Hong Kong, which law enforcement believes to be owned or controlled by the counterfeit suppliers used by the Conspirators. The Conspirators have wired over $178,000 to Supplier-1 alone.

The Bosses Group Chat

28. On or about January 3, 2018, Demir, KARAMAN, and CC-1 began a group chat on WhatsApp. Demir named this group chat "Patrons-ozel," which, translated from Turkish, means "Bosses-private" (the "Bosses Group Chat").

29. On or about November 28, 2019, CC-2 sent an email to Demir at the Demir Email Account, which read in part:

> David,
>
> I heared [CC-3] was taken away by policeman for several weeks due to illegal business which is violate Cisco brand policy.Cisco and police went together to DHL and got all information from her shipping records,I think you certainly will be in the list,on the other side I heard some transceiver suppliers are stopped business these days [. . .] if the issue happened as I guess,the result will be very bad.
>
> Best Regards
>
> [CC-2]

30. On or around the same date, at around 10:50 p.m. EST, Demir copied and pasted this email into the Bosses Group Chat. The following exchange then took place on the Bosses Group Chat between around 10:52 p.m. EST and 11:56 p.m. EST (translated from Turkish):

Sender	Message
CC-1	I think we should stop purchasing products from China.
KARAMAN	If we go to China, they will arrest us too.
KARAMAN	[Message deleted by sender]
CC-1	It will be dangerous in here too.
KARAMAN	Chinese are remorseless.
KARAMAN	Unmerciful too.
KARAMAN	Exactly. There is danger in here as well.
CC-1	The product got stuck many times. If we continue to purchase, the guys will ask, why are you purchasing?
KARAMAN	From now on, we should definitely not use any company names and our names.
CC-1	Bro, we shouldn't purchase from now on.

KARAMAN	I agree, we should not.
Demir	Well if we do not purchase, we will be doomed.
Demir	All the money that we make comes from Cisco.
CC-1	If we purchase and we are doomed, that would be worse.
Demir	Yes, that too.
Demir	It will be a disaster.
Demir	We need to talk in the morning, in detail.
KARAMAN	Let's talk tomorrow.
KARAMAN	This woman, maybe she is trying to scare us to buy from her?
KARAMAN	Why does she continue?
Demir	I am not getting purchase orders from [CC-3] though.
Demir	She knows I am not.

31. KARAMAN, Demir, and CC-1 would also regularly discuss in the Bosses Group Chat fabricating invoices from legitimate Cisco distributors to provide to Amazon in response to complaints of suspected counterfeit trafficking received from Amazon. For example:

a. On or around July 4, 2020, Demir sent to the Bosses Group Chat a screenshot of an email received from Amazon indicating that an Amazon product listing offered by TBE-1 had been removed "because of a buyer complaint about . . . authenticity." The product offered by this listing was a Cisco power supply device.

b. After that, the following exchange took place (translated from Turkish):

Sender	Message
KARAMAN	To which ASIN [a unique Amazon product identification number] did it come?
KARAMAN	For this, we need to create an invoice from [Distributor-1] and send.
[…]	
Demir	Came in [TBE-1].
KARAMAN	We need to find the product and create an invoice from [Distributor-1].
Demir	Yes. We sold [Cisco power supply device] to this customer.

c. Records obtained from Amazon show that on or about July 6, 2020—two days after the above exchange took place—the Conspirators replied to the email from Amazon with the message:

> Hello Team,
>
> I hope you are doing well. We attached invoices from Cisco Distributor. We are Cisco partner and we sell authentic Cisco products. Please reinstate our listing.

d. As indicated, a document purporting to be an invoice from Distributor-1 was attached to the July 6, 2020 email to Amazon. The invoice purports to document the sale from Distributor-1 to TBE-1 of 20 units of the Cisco power supply device at issue. Distributor-1 has reviewed this invoice, however, and has informed law enforcement that it is a forgery. Distributor-1 has informed law enforcement that in fact, although TBE-1 does have a Distributor-1 account, TBE-1 has never purchased anything from Distributor-1.

e. Records obtained through this investigation show that the Conspirators did, however, procure significant volumes of the Cisco power supply device from various China-based suppliers of Counterfeit Cisco Products, including Supplier-2. Moreover, law enforcement discovered several of these purported Cisco power supply devices in the Business-1 Warehouse during the May 2021 Search that were either counterfeit devices or bore counterfeit labels.