AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Jersey

United States of America
v.
Sercan Oyuntur

Case No. 19-MJ-1015 (AMD

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 6/2018 to 10/11/2018 in the county of Burlington in the _____ District of New Jersey, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 1349	Conspiracy to commit mail, wire and bank fraud

This criminal complaint is based on these facts:

See Attachment A

☑ Continued on the attached sheet.

Complainant's signature

Melissa Gibson, Special Agent, USAO-DNJ
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/01/2019

Judge's signature

City and state: Camden, New Jersey

Ann Marie Donio
Printed name and title

Attachment A

(Conspiracy to Commit Mail, Wire and Bank Fraud)

From on or about June 15, 2018 through in or about October 11, 2018, in Burlington County, in the District of New Jersey, and elsewhere, the defendant,

SERCAN OYUNTUR

did knowingly and intentionally conspire and agree with Co-Conspirators 1 through 4, and with others, known and unknown, to devise a scheme and artifice to defraud the Department of Defense ("DoD") and to obtain money and property from the DoD by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice: (1) to cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343; (2) to cause to be placed or cause to be deposited in a post office and authorized depository for mail to be delivered by the United States Postal Service and any private or commercial carrier certain mail matters, contrary to Title 18, United States Code, Section 1341; and (3) to defraud a financial institution, namely TD Bank, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of TD Bank, N.A. ("TD Bank"), by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344, as described in Attachment B.

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

ATTACHMENT B

I, Melissa Gibson, am a Special Agent with the United States Attorney's Office for the District of New Jersey. I have knowledge of the facts set forth below as a result of my participation in this investigation as well as from my review of reports from, and discussions with, other law enforcement personnel. Where statements of others are related herein, they are related in substance and in 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.

1. At all times relevant to this Affidavit:

Defendant and his co-conspirators and other entities

a. Defendant SERCAN OYUNTUR, is a native and citizen of Turkey and owned and operated an outdoor cell phone repair business at a mall in Santa Monica, California. OYUNTUR resided in Granada Hills, California. Per a review of commercial databases, OYUNTUR formed two businesses in the State of California, Fastfixphone LLC and IFIX, LLC. In September 2014, OYUNTUR was granted lawful permanent resident status in the United States.

b. Co-Conspirator 1 (hereinafter "CC1"), a resident of Willingboro, New Jersey, is a used car dealer in the State of New Jersey and operates a business named Deal Automotive Sales LLC (hereafter "Deal Automotive Sales"), also doing business as Car-S-Mart in Florence, New Jersey. CC1 is a native and citizen of Turkey. He first entered the United States in June 1999, when he was admitted as a B2 visitor. In May 2005, CC1 was granted lawful permanent resident status in the United States.

c. Co-Conspirator 2 (hereinafter "CC2") is a foreign national residing in Germany. CC2 was born in Turkey and holds citizenship in both Turkey and Germany.

d. Co-Conspirator 3 (hereinafter "CC3") is a foreign national believed to be residing in Turkey.

e. Co-Conspirator 4 (hereinafter "CC4") is a foreign national believed to be residing in Turkey.

f. Corporation 1 is an oil refining company. It produces lube-based oil and petro-chemical products, and it refines approximately 669,000 barrels of crude oil through its facilities daily. Corporation 1's headquarters is located in Seoul, South Korea.

g. WhatsApp is a free messaging and Voice over Internet Protocol (VoIP) service. Per its website, WhatsApp supports the sending and receiving of a variety of media, including text, photos, videos, documents, and location, as well as voice calls. These messages and calls are secured with end-to-end encryption, meaning that no third party, including WhatsApp, can read or listen to them.

Contracting with the U.S. Department of Defense

h. The United States Department of Defense ("DoD") is a department of the Executive Branch of the United States, that provided military forces to protect the security of the United States, and managed military installations and facilities on behalf of the United States.

i. The DoD contracts with private companies for a variety of equipment and supplies. The Defense Logistics Agency (hereinafter "DLA"), a component of the DoD, provides worldwide combat logistics support to DoD departments and agencies, including the Army, Navy, Air Force, and Marine Corps, by supplying the United States military with equipment, materials, and services. The departments and agencies under the DoD, also contract directly with vendors for equipment, materials, and services.

j. Defense items are put out to bid via a system known as the DLA Internet Bid Board System ("DIBBS"). DIBBS is a web-based application that provides contractors with the capability to search for, view, and submit secure bids regarding the United States government's requests for quotations ("RFQ's") from DLA.

k. In order to conduct business with the Federal Government, a vendor must have an active registration in the System for Award Management ("SAM") database, which is administered by the United States General Services Administration (hereafter "GSA"). SAM is a free United States government database through which government vendors, including DoD vendors, provide the Federal Government with corporate contact information, including financial information and corporate leadership information. This database, among other things, allows the Federal Government to route an electronic payment to the proper financial account.

l. The Enterprise Business System ("EBS") is a suite of computer applications that DLA relies upon to procure material, track inventory, and pay its vendors and contractors. The DoD relies on the information contained in EBS, including account information, when paying vendors and contractors. When vendors and contractors make changes to their SAM database profile, EBS is automatically updated to reflect the change. For example, when a vendor or contractor changes its bank account and routing number in the SAM database, that information is automatically updated in the EBS database.

m. Foreign vendors are able to provide domestic banking information (i.e., bank account and routing numbers) in SAM, but they are not able to provide foreign banking information in SAM. For the purposes of bidding on RFQs and receiving DLA awards, foreign vendors wishing to use a foreign bank account must instead provide their banking information to DLA on a separate form.

n. In order for any DLA vendor to change their banking information from a foreign bank account to a domestic bank account, the payment method in EBS must be changed manually. The payment method dictates the type of account to be paid (i.e., domestic or foreign) and the type of currency to be used (i.e., U.S. dollars or a foreign currency). If the payment

method in the SAM database does not match the banking information in the EBS database, then the DoD cannot make a payment.

o. For a vendor to do business with the DoD electronically, it must request and be assigned a Commercial and Government Entity (hereinafter referred to as "CAGE") code, which is a five-position unique identifier for entities doing business with the federal government. As part of the vendor's registration in the SAM database, the vendor receives a CAGE code.

p. To access SAM, a vendor or contractor must have a user account. To register or update a company's SAM entity account, a user must have a "role" in the SAM entity. The SAM user that initially registers a SAM entity is given a "role" in the entity. The users with roles can assign roles to other SAM users.

q. Prior to June 29, 2018, a user who wished to access SAM needed to enter a SAM-specific user name and password. On or about June 29, 2018, SAM began using a login.gov Internet portal to access its site. SAM users are required to create a login.gov account to gain access to their SAM account. During that registration, SAM users are required to provide a secondary device, such as a cell phone, to login and are given a "personal key." When a SAM user enters the user email address and password into the portal, the device the user provided during registration is sent a six-digit pin. The user then must enter the pin to complete access to SAM. The users are also given two other options to gain access to the SAM account, in the event that the user cannot enter the six-digit pin (1) the user can receive a phone call to the registered device or (2) the user can use a personal key. Each personal key may only be used one time. If a user decides to use a personal key for access, then a new personal key is generated and displayed on screen to the user that logged in.

r. The Defense Finance and Accounting Service (DFAS) is an agency of the DoD. DFAS makes payments to service-members, employees, contractors and vendors on behalf of the DoD. In addition to DFAS, the U.S. Department of the Treasury makes payments on behalf of the DoD, and its departments and agencies.

s. Once the DoD accepts the equipment, materials, or services from a contractor or vendor, the DoD authorizes payment to be sent to that contractor or vendor. In this case, the relevant payment was made by the U.S. Department of Treasury, to the contractor or vendor by electronic funds transfer (hereinafter "EFT"). The EFT was sent to the financial institution and account number that was registered by a person who impersonated the vendor in the SAM database.

Phishing Scam

t. t. In August of 2018, GSA OIG learned that phishing emails were being sent from dibbsbsm@dla-mil.com to DoD contractors. (Legitimate emails from the DLA originate from the domain name "@dla.mil." The domain name used by the conspirators in the phishing scheme, @dla-mil.com, is not a real DLA domain name and is a slight variation of DLA's legitimate domain name, likely used to deceive unsuspecting DoD vendors). Phishing emails were sent to SAM users with roles in SAM accounts. The emails provided a link to a

copy of a fictitious "login.gov" site and solicited the email address, password and personal key of users. When unsuspecting DoD vendors accessed the fictitious site, a bad actor would receive all the information necessary to login to a SAM user account. By accessing the fictitious site and provided the solicited information, a bad actor would have the information needed to login to a SAM user account..

Current Investigation

2. The Defense Criminal Investigative Service (hereafter "DCIS"), Homeland Security Investigations (hereafter "HSI"), and GSA Office of Inspector General (hereafter "GSA OIG"), are currently conducting an investigation of an illegal scheme being committed against several unsuspecting, legitimate DoD vendors, whose identities were hijacked by the conspirators in order to perpetrate the theft of millions of dollars. Specifically, the conspirators entered the SAM database in order to change the bank account and routing numbers associated with a DoD vendor, thereby diverting Government payments intended for the vendor, to bank accounts under the co-conspirators' control.

3. The DoD vendor in this case is Corporation 1. Victim 1 was the only United States-based representative of Corporation 1. Victim 1's office is located in Fort Lee, New Jersey. According to a review of the SAM database, there was only one SAM user with access to Corporation 1's SAM account. That user's name was Victim 1 with the email address lwpllc.ek@gmail.com. On November 25, 2013, Corporation 1 provided its banking information to DLA, directing their payments to a South Korean bank account. On November 26, 2013, DLA updated its EBS database to reflect the correct foreign banking information for Corporation 1.

4. A review of Corporation 1's procurement history with the DoD in 2018 revealed that Corporation 1 was awarded approximately 11 contracts to provide fuel for the United States military during fiscal year 2018. The total value of the 11 contracts awarded to Corporation 1 was approximately $175,496,276.00. In regards to this particular incident, on July 27, 2018, the DoD awarded Corporation 1 contract SPE602-18-D-0455 / Delivery Order SPE602-18-F-C143. The value of that contract was $23,453,350.90. The contract called for Corporation 1 to provide 10,080,000 gallons of Aviation JA1 Turbine Fuel ("Jet Fuel") to the United States military.

5. There is probable cause to believe that during the period of the conspiracy, from on or about June 15, 2018, to on or about October 11, 2018, CC1, OYUNTUR, and CC2 communicated about the fraudulent scheme using various cellular telephones, WhatsApp messenger and WhatsApp VoIP. On November 5, 2018, federal agents executed a search warrant at CC1's residence in Willingboro, New Jersey and seized CC1's cellphone. A subsequent search of CC1's cell phone pursuant to the search warrant revealed that CC1 communicated with both OYUNTUR and CC2 via WhatsApp. Most of the text and What's App communications were in Turkish. The text messages were translated into English and are summarized in substance and in part in this Complaint.

6. There is probable cause to believe that Victim 1, the sole Corporation 1 representative in the United States, was the victim of the phishing scheme described above.

From August 6, 2018 to September 7, 2018, Victim 1 received three phishing emails from dibbsbsm@dla-mil.com which, when considered together and with the other evidence in this case, were designed to obtain the SAM account login information from Victim 1.[1] These emails are as follows:

a. The first email, sent to Victim 1 on August 6, 2018, provided information about the login.gov process.

b. The second email, sent to Victim 1 on August 13, 2018, contained a link to confirm the login.gov personal key.

c. The third email, sent to Victim 1 on September 7, 2018, stated that Corporation 1's SAM registration had been successfully updated.

The metadata on the emails from dibbsbsm@dla-mil.com revealed they were sent from a Yandex email server.[2] By contrast, if the DoD had sent an automated email to Victim 1, that email would have been sent from the server associated with notification@sam.gov.

7. On August 17, 2018, CC2 sent CC1 several texts. CC2 instructed CC1 to form a company, open two bank accounts for the company, and obtain a phone number for the company. CC2 also instructed CC1 to ensure that one of the bank accounts was opened at Bank of America. CC2 told CC1 that he would receive $20,000, of which a couple thousand dollars would be paid in advance and the rest would be paid at the end. CC2 further told CC1 that if they did not succeed, CC1 would not be paid.

8. The following day, on August 18, 2018, CC1 responded to CC2 via text and requested an advance payment of $5,000. CC2 responded that CC1 originally requested $3,000 in advance and told CC1 that if CC2 now asked the men for $5,000 they would take it wrong. CC1 then provided CC2 with CC1's bank account information for the advance payment. Specifically, CC1 sent CC2 two pictures, which contained the bank account number and routing number for CC1's TD Bank account, ending in -8989 (hereafter "TD-8989"), held in CC1's company's name, Deal Automotive Sales. According to TD Bank records, CC1 was the sole signature on that account.

9. On Monday, August 20, 2018, CC2 and CC1 discussed via text whether to form a new company or use CC1's existing company (Deal Automotive Sales) for the job. CC1 said he was going to form a completely new company and was getting ready to meet with the accountant. CC1 asked CC2 whether there was a particular company name they should use for

[1] During his interview with law enforcement, Victim 1 consented to the search of his email account which allowed agents to obtain electronic copies of the emails he received from the phishing email account.

[2] Yandex is headquartered in Moscow, Russia. According to open source information, Yandex provides many internet-based services including search engines and email hosting. Yandex is commonly used in Turkey, Russia and surrounding countries.

the new company, to which CC2 responded that the company name was not important. CC2 asked CC1 whether CC1 could form a new company, open a bank account, and obtain a phone within a few days, adding that it would be quicker to use CC1's already-existing company. CC1 responded to CC2 that CC1's own name was associated with the existing company, so they could not use that company. CC1 assured CC2 that CC2 should not worry and that the new company would be ready in time.

10. On August 21, 2018, CC2 texted CC1 the name of an individual ("Individual 1") and an address on Morse Avenue, North Hollywood, California, 91606."[3] CC2 instructed CC1 to send the phone and bank account information to this California address. On the day of the search, CC1 told federal agents that CC2 had instructed CC1 to purchase a phone and mail the SIM card to the California address.[4]

11. On August 27, 2018, CC2 sent CC1 a picture of a wire transfer document indicating that a $3,000 advance payment had been sent to CC1. Per bank records, the TD-8989 account, held in the name Deal Automotive Sales and controlled by CC1, received the wire transfer on August 27, 2018. The wire originated from a bank account in Turkey held by a co-conspirator (hereafter referred to as "CC3").

12. On August 28, 2018, CC1 sent a text to CC2 acknowledging receipt of the wire. On the same date, CC2 resent CC1 the name Individual 1 and the California address where CC2 wanted CC1 to send the SIM card. CC1 responded that he was getting the card from T-Mobile and would send it via Federal Express (hereafter "FedEx"). CC1 also told CC2 that once the bank account was open, an online account would be established so that CC1 and CC2 could control the bank account via phone. CC1 then sent CC2 a picture of the T-Mobile receipt for the new SIM card and phone number, (609) 227-8576 (hereafter referred to as the "GLOBAL TRAC CELL"). The GLOBAL TRAC CELL number was circled in the picture that was sent to CC2.

13. On August 29, 2018, Global Trac World, LLC (hereafter "Global Trac World") was formed in the State of New Jersey. On the formation documents, Witness 1 was listed as the registered agent for Global Trac World. Per witness interviews, CC1 facilitated the formation of Global Trac World, paid cash to have the company formed, and paid Witness 1 in cash to use Witness 1's name on both the formation and bank account documents.

---

[3] Individual 1 is OYUNTUR's cousin. The North Hollywood address was OYUNTUR's previous address based on California Division of Motor Vehicle records. In March 2019, law enforcement officers interviewed OYUNTUR and confirmed that he previously lived at the address.

[4] A Subscriber Identification Module, widely known as a SIM card, is an integrated circuit that is intended to securely store the international mobile subscriber identity ("IMSI") number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices (such as mobile phones and computers).

14. On August 30, 2018, CC1 sent CC2 a picture of the completed FedEx Airbill for the SIM card that CC1 mailed to the California address on August 29, 2018.

15. On or about September 4, 2018, CC2 sent CC1 a picture of a wire transfer document indicating that an additional $1,000 advance payment was sent to CC1. Specifically, CC2 sent CC1 a picture of CC2's cell phone screen, which showed an image of wire transfer details. Based on a review of the picture sent to CC1, the wire transfer document was sent to CC2 from CC4 in Turkey. According to the bank records, CC1's TD-8989 account received the wire transfer on September 5, 2018. The wire originated from CC3's bank account in Turkey.[5]

16. On September 7, 2018, Witness 1, at CC1's direction, opened a business bank account for Global Trac World at Bank of America, account ending in 4015 (hereafter "BoA-4015"). Witness 1 was the sole authorized signature on the account. After opening the account, CC1 kept the account opening documents and paid Witness 1 approximately $250 cash for her work, which included having the Global Trac World formation documents notarized and opening the bank account at Bank of America.

17. On September 7, 2018, CC1 texted CC2 the account number and routing number for Global Trac World's BoA-4015. CC1 also sent CC2 pictures of the Global Trac World formation document, as well as correspondence from the Internal Revenue Service (hereafter "IRS") listing Global Trac's Employer Identification Number (hereafter "EIN").[6] CC1 also texted a picture of Witness 1's driver's license to CC2.

18. On September 7, 2018, unknown co-conspirators fraudulently accessed the DoD database and changed the name of Corporation 1's financial institution and bank account number to the Global Trac World bank account, BoA-4015, in Corporation 1's SAM account. The unknown co-conspirators logged into Corporation 1's SAM account, using Victim 1's login and personal key, which had been obtained via the phishing scheme. The originating internet protocol ("IP") address[7] for the SAM database login was 31.207.2.100. According to GSA

---

[5] CC3 was the originator for both advance payments to CC1.

[6] An EIN is a unique nine-digit number assigned by the IRS to business entities operating in the United States for the purposes of identification. Here, the IRS letter regarding the EIN was addressed to Global Trac, not Global Trac World. Per witness interviews, when CC1 was forming the new company, the name "Global Trac" was already in use, so CC1 (or someone at CC1's direction) added "World" to the company name.

[7] "Internet Protocol Address ("IP Address")" refers to the unique address assigned to every computer or device on the Internet, the same way that every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 69.116.211.141. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address.

records, this was the first time that this particular IP address accessed this account. This IP address was registered to Newark Cloud, a cloud computing and data storage company.[8]

19. Between September 11, 2018 and September 22, 2018, CC1 communicated via WhatsApp with an individual identified in CC1's phone as "CALI SERKAN," using telephone number (818) 433-5544. There is probable cause to believe that "CALI SERKAN" is SERCAN OYUNTUR, as follows:

a. Per phone records, the subscriber for this cellular number was IFIX LLC (hereafter "IFIX"). IFIX was formed in the State of California on July 8, 2015 by OYUNTUR.

b. On the IFIX formation documents, OYUNTUR was listed as the manager of IFIX and the business address was listed on Morse Avenue in North Hollywood, California.

c. Per phone records, IFIX was the subscriber for the phone from August 20, 2018 to September 3, 2018.[9]

d. Per California motor vehicle records and OYUNTUR's statements to agents, OYUNTUR resided at the Morse Avenue address in North Hollywood, California (the same California address that CC1 mailed the SIM card for the GLOBAL TRAC CELL).

Hereafter, "CALI SERKAN" and SERCAN OYUNTUR will be referred to as "OYUNTUR" and the phone corresponding to (818) 433-5544 will be referred to as "OYUNTUR CELL 1."

20. On September 11, 2018, CC1 sent a text to CC2 stating, "6092278576 [GLOBAL TRAC CELL] telephone is not working." CC2 responded, "I will get back you straight away." "The friend will have the telephone on in half an hour." "The telephone is on right now." CC1 responded, "The sim card must be placed into the smart phone." CC2 responded, "It is on the smart phone."

21. There is probable cause to believe that in addition to using OYUNTUR CELL 1, OYUNTUR was also using and in possession of the GLOBAL TRAC CELL. Per phone records, on September 11, 2018, the GLOBAL TRAC CELL was active in Granada Hills, California. Specifically, the GLOBAL TRAC CELL received two incoming calls from CC1's phone, during a time when the GLOBAL TRAC CELL was physically located in Granada Hills, California.

---

[8] According to GSA records, prior September 7, 2018, the IP address used to access Corporation 1's SAM account was issued by Verizon.

[9] The phone number was not reassigned to a new subscriber until November 2, 2018, which allowed OYUNTUR to continue using the phone number to correspond with CC1 via WhatsApp even after the phone service was terminated.

Per an interview with OYUNTUR, he moved to Granada Hills on July 12, 2018 and still lives there.

22. On September 11, 2018, OYUNTUR attempted to log into the Global Trac World bank account BoA-4015. According to Bank of America records, a device with cookie[10] ID "4894186243" attempted to login to that account from T-Mobile IP address 172.58.200.35. The same device with cookie ID "4894186243" was used to successfully log into OYUNTUR's personal Bank of America accounts on approximately 11 separate days between November 2017 and May 2018.

On September 12, 2018, at approximately 3:09pm UTC, OYUNTUR sent a text to CC1 from OYUNTUR CELL 1 stating that CC1 was going to switch on the "other" phone.[11] Per phone records, at 3:35pm UTC, about a half an hour after telling CC1 that he was switching on the "other" phone, CC1 attempted to call the GLOBAL TRAC CELL, but did not connect. A review of phone records for the GLOBAL TRAC CELL revealed that from September 5, 2018 to September 19, 2018, the phone was used in several areas of Los Angeles County, including Granada Hills, Sylmar, and Los Angeles. Per an interview conducted with OYUNTUR on March 21, 2019, OYUNTUR moved to Granada Hills on July 12, 2018, and still lived there as of mid-April 2019.

23. On September 12, 2018, CC1 notified OYUNTUR via text to OYUNTUR CELL 1 that CC1 was going to attempt to connect to the Bank of America account from the internet. About six minutes later, OYUNTUR sent CC1 a six-digit code. Two minutes later, CC1 sent OYUNTUR a screenshot of a Bank of America webpage that read, "You have successfully enrolled. Welcome to online banking." CC1 then sent OYUNTUR a picture of a hand written note with what appears to be an online user ID, password and answers to security questions. OYUNTUR asked CC1 for a picture of the BoA-4015 debit card, front and back. CC1 responded with pictures of the debit card. Bank of America records show that on September 12, 2018, the Global Trac World account, BoA-4015, was accessed from an IP address assigned to Comcast in New Jersey. The records show the "Enrolled" status for the first time during this login. During an interview, CC1 confirmed that Comcast was his internet service provider.

24. On September 12, 2018, at approximately 8:06pm UTC, 10 minutes after receiving the login information from CC1, OYUNTUR logged in to the Global Trac World bank account, BoA-4015. Per bank records, the device that logged into the Global Trac World bank account was known to Bank of America, in that the same device was previously used to login to

---

[10] Cookies are small files which are stored on a user's device. Cookies are unique to one particular device. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next.

[11] Universal Time Coordinated, also referred to as Coordinated Universal Time, is the time standard commonly used across the world.

OYUNTUR's bank accounts at Bank of America. The device already had Bank of America cookie ID "4953705261" on it and was used multiple times to login to Bank of America accounts held by OYUNTUR. In addition, the device used to login to the Global Trac World bank account originated from IP address 172.250.43.186. Per records obtained from the internet service provider, the subscriber for IP address 172.250.43.186 on September 12, 2018 was OYUNTUR and the originating location of the IP address was OYUNTUR's residence in Granada Hills, California.

25. On September 12, 2018, at approximately 8:32pm UTC, OYUNTUR asked CC1 to provide him with the "social insurance number" so his "friend" would not hesitant when they called the bank. In response, CC1 texted OYUNTUR a copy of Witness 1's driver's license. Several hours later, OYUNTUR sent CC1 a picture of the Bank of America SafePass security screen, which stated that in order to complete the enrollment process and add a mobile device to the account, they needed to call Bank of America to activate the service.[12]

26. Per phone records, on September 12, 2018, at approximately 10:31pm UTC, the GLOBAL TRAC CELL placed a call to the Bank of America. Per phone records, the call originated from Granada Hills, California, and lasted 454 seconds.[13]

27. On September 13, 2018, OYUNTUR texted CC1 the user name and password for the BoA-4015 account.

28. On September 14, 2018, OYUNTUR and CC1 communicated via text about Witness 1. CC1 stated that he was concerned that Witness 1 may have stolen the DLA payment that CC1 and CC2 were attempting to obtain. OYUNTUR texted CC1 that there was nothing to fear because the money had not yet been deposited.

29. On September 17, 2018, the BoA-4015 account was closed. Witness 1 advised agents that Witness 1 went to the bank with CC1 several times because CC1 had difficulty accessing the account online. Witness 1 further stated that on their last visit to the bank, the account was closed. A review of bank records revealed that on September 17, 2018, Witness 1 withdrew the entire balance from the account, which totaled $100.

30. On September 18, 2018, CC1 sent several texts to the GLOBAL TRAC CELL. Specifically, CC1 sent a picture of the bank account information for Deal Automotive Sales, TD-

[12] According to Bank of America, SafePass uses a 6-digit one-time code sent in a text message to your mobile phone to help verify your identity before authorizing the transfer of funds from your account.

[13] During law enforcement's interview with OYUNTUR, he admitted that since July 12, 2018, he lived in Granada Hills, California.

8989.[14] CC1 also sent instructions to the GLOBAL TRAC CELL requesting that the payment be sent to the TD-8989 account, which CC1 controlled.

31. A review of SAM database records for Corporation 1 revealed that on September 18, 2018, co-conspirators fraudulently accessed the DoD's database, using Victim 1's stolen identity, and changed the name of Corporation 1's financial institution and bank account number from the BoA-4015 to the TD-8989 bank account supplied by CC1, in Corporation 1's SAM account. The originating IP address for the SAM account login was 31.207.2.100, which was registered to Cogent Communications. A Cogent representative advised agents that the subject IP address was part of a block of IP's assigned by Cogent to their customer M247 Ltd, an Internet Service Provider in the United Kingdom. On October 18, 2018, M247 Ltd advised agents that they assigned the IP address to NordVPN. NordVPN is located in Panama and does not comply with U.S. subpoenas or warrants.

32. On September 20, 2018, OYUNTUR asked CC1, via text from OYUNTUR CELL 1, to provide OYUNTUR with CC1's company's email, telephone number and address. CC1 responded with the name "Deal Automotive Sales, LLC," on Route 130 South in Florence, New Jersey. CC1 also provided OYUNTUR with several phone numbers for Deal Automotive Sales and his personal email address.

33. On September 22, 2018, OYUNTUR sent several texts to CC1 from OYUNTUR CELL 1, telling CC1 that several contracts were sent to CC1's personal email account and that each contract was for two assault boats, for a total of six boats. CC1 responded and acknowledged receipt of the contracts.

34. On November 5, 2018, law enforcement officers executed a search warrant on Microsoft for CC1's emails. Per a review of search warrant records, on September 22, 2018, CC1 received an email from Victim1@gmail.com. The subject line of the email was "Government Contracts." Attached to the email was three documents purporting to be contracts between the DoD and Deal Automotive Sales, which law enforcement later learned were fictitious. The fictitious contracts showed that Deal Automotive Sales received contracts from the DoD in July and August of 2018. The fictitious contracts were dated July 11, 2018, July 27, 2018, and August 30, 2018, and were valued between approximately $17 million and $22 million dollars each.

35. CC1 then asked OYUNTUR via text who had financed the deal. OYUNTUR responded the deal had been financed by a man named "Erik" (Victim 1's first name). OYUNTUR then directed CC1 to go to the CC1's bank (TD Bank), show them the document and tell them that money would be deposited into his account that week and he would then have to transfer the money to other companies. CC1 responded "okay."

36. From September 24, 2018 to on or about October 11, 2018, CC1 communicated via WhatsApp with an individual identified in CC1's phone as "Secret Code." On September 24,

[14] TD-8989, held by Deal Automotive Sales, is the same account used by CC1 to receive the advance payments from Turkey.

2018, "Secret Code" sent a text to CC1 that stated, "It's me Serkan"…"You can reach me from here" (in Turkish). In addition, CC1 stopped communicating with OYUNTUR on the OYUNTUR CELL 1 on September 24, 2018, the same date he began communicating with OYUNTUR on this phone, hereafter referred to as SECRET CODE CELL.

37. Every night, the DoD's EBS servers compare its files to the SAM servers and download any bank account changes. In this instance, when the conspirators inputted their own domestic banking information into Corporation 1's SAM account on September 7, 2018, and September 18, 2018, Corporation 1's South Korean banking information in EBS was overwritten with the conspirators' domestic banking information, BoA-4015 (Global Trac World) and TD-8989 (Deal Automotive Sales). However, the computer system automatically prevented DLA from issuing a payment to the domestic account to satisfy Corporation 1's outstanding invoice because Corporation 1's payment method was set in EBS to a payment method that directed the system to pay in US dollars to a foreign, rather than domestic, bank account.

38. To trigger a payment to their domestic bank account, the conspirators had to contact DLA and have DLA manually change the payment method in EBS from foreign to domestic, which would direct the system to pay in U.S. dollars to a domestic account.

39. To accomplish this, on or about September 19, 2018, OYUNTUR or someone at OYUNTUR's direction, called DFAS and represented themselves to be Victim 1 from Corporation 1. The caller provided Corporation 1's unique CAGE code to DFAS. The call was placed from the GLOBAL TRAC CELL on September 19, 2018, at approximately 5:41pm UTC. The call was placed from Sylmar, California, which is located approximately five miles from OYUNTUR's residence in Granada Hills. The call was recorded. The caller advised DFAS that he had updated the bank information in the SAM database and wanted to make sure that the new information was reflected within the DFAS database as well. The caller advised that the account number should be the TD-8989 bank account (which account was held in the name of Deal Automotive). A DFAS representative confirmed that the bank account was updated in the SAM database to the TD-8989 account. A DFAS representative asked the caller if he was calling in regards to a particular contract. The caller stated that he was calling in reference to contract SPE602-18-D-0455 / Delivery Order SPE602-18-F-C143. The caller asked the DFAS representative if there had been any transactions with the company's old Bank of America account within the last 10 days. The caller stated that the company was not working with Bank of America anymore. The DFAS representative stated that that there were no transactions and that the old account was on file at DFAS, however the DFAS representative was updating their system to reflect the account information that was listed in the SAM database. The caller responded, "Thank God."

40. As a result of that phone call, on October 2, 2018, and again on October 4, 2018, a DFAS representative contacted a DLA Finance Business Process Analyst ("BPA") and explained that Corporation 1 was not being paid because the payment method was set to foreign, instead of domestic. At DFAS's urging, the DLA BPA changed Corporation 1's payment method in EBS from foreign to domestic, thus triggering a payment to the domestic bank account, which was scheduled to be paid on October 10th.

41. On October 9, 2018, OYUNTUR sent a text to CC1 from the SECRET CODE CELL advising CC1 that the payment would occur sometime between the "9th and the 13th." OYUNTUR told CC1 that documents would be sent to CC1 and asked CC1 to provide them with the exact amount deposited into the account so OYUNTUR could prepare the documents according to the incoming figures.

42. According to TD Bank, on October 9, 2018, the TD-8989 account had a balance of $12,297.30.

43. Per DFAS records, on October 10, 2018, a payment of $23,453,350.90, was paid via EFT to the TD-8989 bank account (Deal Automotive Sales).

44. On October 10, 2018, CC1 received another email from Victim1@gmail.com. The subject line of the email was "Contracts" and had two attachments. One of the attachments was a fictitious DoD purchase order (SPE602-18-D-0455) awarded to Deal Automotive Sales on August 17, 2018, valued at $23,000,036.61. The second attachment was a fictitious "Proforma Invoice," purportedly sent from Aydos Boats to Deal Automotive Sales, dated August 10, 2018 and valued at $21,411,079.25. Per the "Proforma Invoice," Deal Automotive Sales was in the process of purchasing boats from Aydos Boats for delivery to the U.S. Customs and Border Protection at the Newark/New York Port.

45. On October 10, 2018, OYUNTUR sent a text to CC1 from the SECRET CODE CELL telling him that if he did not go to the bank with the documents that he received the deposited money would remain pending. CC1 told OYUNTUR that he would go to the bank the following morning.

46. According to a TD Bank employee, about a week prior to October 10, 2018, CC1 told the employee that CC1 was expecting a large sum of money soon and that it related to the purchase of vehicles. CC1 said he would be receiving a 10 percent commission on the sales. The bank employee advised CC1 to be cautious of schemes and not to give out his account number to anyone. On October 10, 2018, when the employee arrived at the bank in the morning, CC1 was already inside the branch purchasing cashier's checks. After purchasing the cashier's checks, CC1 stopped by the employee's office to advise him that the large sum was deposited to his account. The bank employee reviewed CC1's account and saw the $23 million dollar deposit. The bank employee then told CC1 that because the transaction was so large he needed to provide the bank with supporting documentation. CC1 told the bank employee that people in Turkey picked him to purchase vehicles at an auction in Turkey. CC1 further stated that initially they wanted him to travel to Turkey with the money but later decided to have him wire the money to Turkey instead. During the meeting, CC1 provided the bank employee with the Aydos Boats Proforma Invoice he received via email. The TD bank employee told CC1 that the document alone was not enough and requested additional documentation related to the transaction. CC1 then used his cell phone to call an unknown co-conspirator to request additional supporting documentation. The call was placed on speakerphone. The unknown co-conspirator asked the bank employee for the bank employee's email address and stated that his "assistant" would send over additional documentation.

47. On October 11, 2018, the TD Bank employee received an email from the dibbsbsm@dla-mil.com email account. [15] The email was purportedly from an individual named Sameisha Wright, DLA-Energy, telephone (616) 692-2947, and had one attachment. The attachment was the DoD purchase order (SPE602-18-D-0455) dated August 17, 2018, indicating that DLA Energy/Bulk Petroleum Products issued an award to Deal Automotive Sales, LLC in the amount of $23,000,036.61.[16] CC1 was copied on the email.

48. I have been advised by Special Agents with DCIS that according to DLA, no "Sameisha Wright" is listed in DLA's global address book. However, I also learned that there was a DLA Energy employee with the first name of "Sameisha." Sameisha's job title is "Inventory Management Specialist." An inventory management specialist would not send out emails about DIBBS accounts or Secure.Login accounts to DoD vendors. I have also been advised that DLA employee email accounts do not come from or have "dibbs" in the address. DLA employees' e-mail addresses end with dla.mil and not "@dla-mil.com." In addition the area code of that phone number is an area code assigned to Michigan. DLA Energy is located in Fort Belvoir, Virginia with a satellite locations in nearby Lorton, Virgina, and the Aerospace Energy directorate in San Antonio, Texas

49. I have reviewed the actual purchase order (SPE602-18-D-0455) issued by DLA Energy/Bulk Petroleum Products and have determined the following. According to the actual purchase order, the contractor was Corporation 1. The date of order was August 18, 2018, the total was $22,289,998.50, date of delivery September 19, 2018 and it was signed by the contracting officer. I am aware that the DLA contracts and purchase orders are publicly available on the internet. Additionally, Deal Automotive Sales is not a government contractor, does not have a CAGE code, does not have a SAM or EBS account, and has never bid on or been awarded a DoD contract.

50. According to TD Bank, on October 10, 2018, prior to TD Bank placing a hold on the TD-8989 account, CC1 transferred $459,350 from the TD-8989 account to another TD bank account he controlled, ending in 7783 (hereafter "TD-7783"). TD-7783 was opened on May 9, 2018. The TD-7783 account was also held in the name of Deal Automotive Sales LLC in Willingboro, New Jersey, and CC1 was the sole signer on the account.

51. On October 15, 2018, Corporation 1 discovered the changes made to their SAM account banking information and corrected the information. On October 15, 2018, Victim 1 contacted GSA and advised that he was the "Entity Administrator" for Corporation 1 and that Corporation 1's banking information had been changed in the SAM database without the company's authorization.

---

[15] The dibbsbsm@dla-mil.com email account was the same email account used in the phishing scheme with Victim 1.

[16] The attachment was a copy of the same DoD purchase order emailed to CC1 on October 10, 2018.

52. On October 15, 2018, Victim 1 also contacted DFAS to report that the Corporation 1's bank account had been changed without the company's authorization. Victim 1 advised DFAS that the bank account that Corporation 1 actually uses is an international bank in South Korea, but Victim 1 noticed that Corporation 1's SAM account was now reflecting a bank account for Corporation 1 at TD Bank. Victim 1 asked DFAS if DFAS could confirm whether or not a payment related to contract SPE602-18-D-0455 /Delivery Order SPE602-18-F-C143 had issued. DFAS confirmed that a payment had been issued for that contract to an account at TD Bank. This payment had been issued via EFT on October 10, 2018, for approximately $23 million dollars.