UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

GHALEB ALAUMARY,
aka "G,"
aka "Backwood,"
aka "Big Boss,"

Defendant.

CR No. 2:20-cr-00576 -MCS

I N F O R M A T I O N

[18 U.S.C. § 1956(h): Conspiracy to Engage in Money Laundering; 18 U.S.C. § 982 and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The United States Attorney charges:

COUNT ONE

[18 U.S.C. § 1956(h)]

A. INTRODUCTORY ALLEGATIONS AND DEFINITIONS

1. At times relevant to this Information:

Defendant

a. Defendant GHALEB ALAUMARY, also known as ("aka") "G," aka "Backwood," aka "Big Boss" ("ALAUMARY"), was a resident of Canada.

Bank Accounts

a. "US Bank Account 1" was a bank account at U.S. Bank, N.A., with the account number ending in 6155, which was held in Woodland Hills, California.

b. "US Bank Account 2" was a bank account at U.S. Bank, N.A., with the account number ending in 7096, which was held in Inglewood, California.

c. The "CIBC Account" was a bank account held at Canadian Imperial Bank of Commerce, with the account number ending in 1716, which was held in Ontario, Canada.

d. The "Chase Account" was a bank account held at JP Morgan Chase Bank, N.A. ("Chase"), with the account number ending in 6628, which was held in Pearland, Texas.

Victims

e. The "Victim Indian Bank" was a bank headquartered in India.

f. BankIslami Pakistan Limited ("BankIslami") was a bank headquartered in Pakistan.

g. The "Victim Maltese Bank" was a bank headquartered in Malta.

h. The "Victim English Premier League Club" was a professional soccer club located in the United Kingdom.

i. The "Victim U.K. Company" was a company located in the United Kingdom.

j. The "Victim Federal Contractor" was a federal contracting business in the State of North Dakota.

k. The "Victim Consumer Products Company" was a consumer products company in the State of North Carolina.

l. The "Victim Law Firm" was a law firm in the State of New York.

Definitions

m. An Automated Teller Machine ("ATM") cash-out occurs where a hacker gains unauthorized access to the computer(s) of a bank, intercepts ATM transaction data, and causes fraudulent ATM withdrawal requests to be approved, thereby causing a requesting ATM to dispense cash to coconspirators.

n. A cyber-heist occurs where a hacker gains access to the computer(s) of a bank without authorization and sends messages through the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") communication system from the victim bank's computer system, authorizing and causing fraudulent wire transfers to bank accounts used and controlled by coconspirators.

o. A business email compromise ("BEC") fraud occurs where a hacker tricks personnel of a victim company into making unauthorized wire transfers by (a) gaining unauthorized access to an email account used by a business; (b) blocking or redirecting communications to and/or from the email account; (c) and using the compromised email account or a separate fraudulent email account to communicate with personnel from a victim company (which may be the company to which the compromised account belongs, or another company doing business with that company).

p. "Cryptocurrency" or "virtual currency" is a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units of the currency, and to verify and transfer assets. Cryptocurrency is typically accessed using secret or private

encryption "keys" which are commonly stored using a software "wallet."

B. OBJECTS OF THE CONSPIRACY

2. Beginning on an unknown date, but no later than on or about August 7, 2018, and continuing until on or about October 17, 2019, in Los Angeles County, within the Central District of California, and elsewhere, defendant ALAUMARY, and unindicted coconspirator #1 ("UICC 1"), unindicted coconspirator Ramon Olorunwa Abbas ("Abbas"), unindicted coconspirator #2 ("UICC 2"), unindicted coconspirator #3 ("UICC 3"), unindicted coconspirator #4 ("UICC 4"), and unindicted coconspirator #5 ("UICC 5"), together with others known and unknown to the United States Attorney, knowingly conspired:

a. to conduct and attempt to conduct financial transactions, affecting interstate and foreign commerce, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, which, in fact, involved the proceeds of specified unlawful activity -- namely, obtaining information from a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2)(C); accessing a protected computer to defraud and obtain value, in violation of Title 18, United States Code, Section 1030(a)(4); and wire fraud, in violation of Title 18, United States Code, Section 1343 -- and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i);

b. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer, a monetary instrument and funds

from a place in the United States to a place outside of the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity, and knowing that the transportation, transmission, and transfer were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity -- namely, obtaining information from a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2)(C); accessing a protected computer to defraud and obtain value, in violation of Title 18, United States Code, Section 1030(a)(4); and wire fraud, in violation of Title 18, United States Code, Section 1343 -- in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i); and

c. to knowingly engage and attempt to engage in monetary transactions affecting interstate and foreign commerce involving criminally derived property of a value greater than $10,000, which property was derived from specified unlawful activity -- namely, obtaining information from a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2)(C); accessing a protected computer to defraud and obtain value, in violation of Title 18, United States Code, Section 1030(a)(4); and wire fraud, in violation of Title 18, United States Code, Section 1343 -- in violation of Title 18, United States Code, Section 1957.

C. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

3. The objects of the conspiracy were to be accomplished, in substance, as follows:

ATM Cash-Outs

a. In an ATM cash-out scheme, after UICC 1 or another coconspirator had gained unauthorized access to the computer(s) of a bank, UICC 1 or another coconspirator would ask defendant ALAUMARY to recruit and organize coconspirators to withdraw cash from ATMs ("runners").

b. At times, defendant ALAUMARY would provide UICC 1 or another coconspirator with debit card account numbers to which they could credit funds.

c. UICC 1 or another coconspirator would provide defendant ALAUMARY with debit card account numbers and pin numbers that were to be used in the ATM cash-out scheme.

d. Defendant ALAUMARY or a coconspirator would code blank debit cards with the debit card account information provided by UICC or another coconspirator.

e. UICC 1 or another coconspirator would cause fraudulent ATM withdrawal requests to be approved, which would cause a requesting ATM to dispense cash to runners who possessed the debit cards.

f. Defendant ALAUMARY would correspond with runners, and other coconspirators who assisted defendant ALAUMARY in organizing the runners, including UICC 3 and UICC 4, to coordinate the withdrawal of cash from ATMs in the United States and Canada.

Bank Cyber-Heists

g. In a bank cyber-heist scheme, after UICC 1 or another coconspirator had gained unauthorized access to the computer(s) of a bank, UICC 1 or another coconspirator would ask defendant ALAUMARY

for bank accounts that could be used to receive funds that would be fraudulently obtained by hackers through a bank cyber-heist.

h. Defendant ALAUMARY would ask unindicted coconspirator Abbas and other coconspirators for bank accounts that could be used to receive the funds.

i. Unindicted coconspirator Abbas and other coconspirators would provide account information for a bank account or bank accounts that could be used to receive fraudulently obtained funds, including the bank account number and the SWIFT code, or the international bank account number ("IBAN"), and defendant ALAUMARY would provide this information to UICC 1 or another coconspirator.

j. UICC 1 or another coconspirator would, after hacking into the computer network of a victim bank, send a fraudulent message through the SWIFT system of the victim bank, directing a wire transfer from the victim bank to the bank account(s) identified to receive fraudulently obtained funds.

k. Defendant ALAUMARY would correspond with unindicted coconspirator Abbas and other coconspirators to coordinate the receipt, and subsequent withdrawal, of cash from the bank accounts.

BEC Schemes

l. In a BEC scheme, defendant ALAUMARY, on the one hand, and unindicted coconspirator Abbas, UICC 2, UICC 5, and other coconspirators, on the other hand, would request from each other a bank account that could be used to receive funds from a BEC scheme.

m. Defendant ALAUMARY, on the one hand, and unindicted coconspirator Abbas, UICC 2, and UICC 5, on the other hand, would send each other account information for a bank account that could be used to receive fraudulently obtained funds, including the bank

account number and the SWIFT code, or the IBAN. Such a bank account would be opened by UICC 3 or UICC 4, or another coconspirator, to conceal the fraudulent nature of the transaction and the involvement of defendant ALAUMARY, unindicted coconspirator Abbas, UICC 2, UICC 5, and other coconspirators.

n. Unindicted coconspirator Abbas, UICC 2, and UICC 5, or other coconspirators would communicate with a victim-company -- fraudulently pretending to be a company doing business with the victim-company -- and would provide the victim-company with instructions to wire transfer a payment to the bank account.

o. After the victim-company had been fraudulently induced to wire transfer funds into the bank account, defendant ALAUMARY would correspond with unindicted coconspirator Abbas, UICC 2, UICC 3, UICC 4, and UICC 5 to coordinate the receipt, and subsequent withdrawal or transfer of those funds from the bank account.

Further Money Laundering

p. After obtaining funds through an ATM cash-out, bank cyber-heist, or BEC scheme, defendant ALAUMARY, and UICC 1, unindicted coconspirator Abbas, UICC 2, UICC 3, UICC 4, and UICC 5, and other coconspirators, would further launder the funds through a variety of means, including wire transfer(s) to a bank account in the name of UICC 3 or additional bank accounts in the names of persons other than defendant ALAUMARY, UICC 1, unindicted coconspirator Abbas, UICC 2, UICC 4, and UICC 5; cash withdrawals and transfers; or exchanging the funds for cryptocurrency -- sometimes with the assistance of additional coconspirators. This money laundering activity would include transfers of funds into, from, and through the United States.

q. Defendant ALAUMARY and his coconspirators attempted to fraudulently obtain and launder hundreds of millions of dollars in this manner.

D. OVERT ACTS

4. In furtherance of the conspiracy, and to accomplish its objects, defendant ALAUMARY, and UICC 1, unindicted coconspirator Abbas, UICC 2, UICC 3, UICC 4, and UICC 5, together with others known and unknown to the United States Attorney, on or about the dates set forth below, committed and caused to be committed various overt acts, in the Central District of California and elsewhere, including, but not limited to, the following:

ATM Cash-Outs

Overt Act No. 1: On August 11, 2018, and in the days following, defendant ALAUMARY communicated with UICC 1 and coordinated with runners to conduct withdrawals from ATMs and further launder funds, after hackers gained unauthorized access to the computer network of the Victim Indian Bank and caused ATMs to dispense approximately $16.3 million to coconspirators, including within the Central District of California.

Overt Act No. 2: On October 27, 2018, and in the days following, defendant ALAUMARY communicated with UICC 1 and coordinated with runners to conduct withdrawals from ATMs and further launder funds, after hackers gained unauthorized access to the computer network of BankIslami and caused ATMs to dispense approximately $6.1 million to coconspirators, including within the Central District of California.

Bank Cyber-Heists

Overt Act No. 3: On January 16, 2019, defendant ALAUMARY sent electronic messages to unindicted coconspirator Abbas requesting two bank accounts that could each receive €5 million wire transfers from the Victim Maltese Bank.

Overt Act No. 4: On January 16, 2019, unindicted coconspirator Abbas responded with electronic messages providing the account information for a bank account in Romania (the "Romanian bank account"), including the IBAN.

Overt Act No. 5: On January 18, 2019, after defendant ALAUMARY sent an electronic message to unindicted coconspirator Abbas asking about the "maximum amount" the Romanian bank account could "handle in 24hr," unindicted coconspirator Abbas responded "It's for large amounts[.]"

Overt Act No. 6: On January 18, 2019, defendant ALAUMARY sent electronic messages to unindicted coconspirator Abbas saying, "[m]y associates want u to clear as soon it hits . . . Cuz a recall can be," and, "if they don't notice we keep pumping."

Overt Act No. 7: From February 7, 2019 through February 11, 2019, defendant ALAUMARY sent electronic messages to other coconspirators, requesting bank accounts that could be used to receive funds from the cyber-heist from the Victim Maltese Bank.

Overt Act No. 8: On February 10, 2019, after defendant ALAUMARY sent electronic messages to unindicted coconspirator Abbas saying that he had "6 slots in total [¶] all 5m euro," and needed additional bank accounts to receive "big hit in 12th feb" that would "all credit same time," unindicted coconspirator Abbas provided the

account information for a bank account in Bulgaria, including the IBAN.

Overt Act No. 9: On February 12, 2019, defendant ALAUMARY sent an electronic message to UICC 1 stating that defendant ALAUMARY could provide four bank accounts that could be used to receive funds from the cyber-heist of the Victim Maltese Bank -- three that could receive wire transfers in euros and one that could receive wire transfers in United States dollars.

Overt Act No. 10: On February 12, 2019, defendant ALAUMARY sent an electronic message to unindicted coconspirator Abbas stating that €500,000 had been wired to the Romanian bank account that unindicted coconspirator Abbas had provided.

Overt Act No. 11: On February 12, 2019, defendant ALAUMARY sent electronic messages to unindicted coconspirator Abbas stating that the fraudulent wire transfer of €500,000 had come from the Victim Maltese Bank, and that "we still have access and they didn't realize , we gonna shoot again tomoro am."

Overt Act No. 12: On February 12, 2019, UICC 1 sent an electronic message to defendant ALAUMARY stating that the Victim Maltese Bank had discovered the fraudulent euro transfer, but that defendant ALAUMARY should check the United States bank account to see if that transfer was successful.

BEC Schemes

Overt Act No. 13: On May 8, 2019, after defendant ALAUMARY sent electronic messages to unindicted coconspirator Abbas asking for a bank account that could be used in a scheme to "swap" the account on file and that the account be able to "handle millions and not block," unindicted coconspirator Abbas sent defendant ALAUMARY the

account information for a bank account in Mexico, including the account number and IBAN.

Overt Act No. 14: On May 13, 2019, defendant ALAUMARY told unindicted coconspirator Abbas that the bank account in Mexico would be used to receive payments of £3-6 million per week, up to £100 million from the Victim English Premier League Club and £200 million from the Victim U.K. Company, and requested another bank account that could be used to receive fraudulent wire transfers.

Overt Act No. 15: On August 14, 2019, defendant ALAUMARY instructed a coconspirator to open a business bank account in the name of a specific business ("Company A").

Overt Act No. 16: On August 14, 2019, at the direction of defendant ALAUMARY, a coconspirator filed a fictitious business name statement with the Los Angeles County Registrar-Recorder/County Clerk ("LACRRCC") in the name of Company A.

Overt Act No. 17: On August 14, 2019, at the direction of defendant ALAUMARY, a coconspirator opened US Bank Account 1 in Woodland Hills, California, in the name of Company A.

Overt Act No. 18: On August 16, 2019, UICC 2 or a coconspirator fraudulently induced the Victim Federal Contractor through a BEC scheme to wire transfer approximately $13,966.00 to US Bank Account 1.

Overt Act No. 19: On August 19, 2019, after defendant ALAUMARY sent UICC 3 an electronic message asking which bank account they would be using for "the big one tomorrow," defendant ALAUMARY and UICC 3 exchanged electronic messages and agreed to use the CIBC Account, which was opened in the name of UICC 3, to receive the fraudulent payment.

Overt Act No. 20: On August 19, 2019, defendant ALAUMARY sent UICC 2 an electronic message containing the name, address, and social security number of the account holder of US Bank Account 1, as well as the bank account number, and the bank account username and password, for US Bank Account 1.

Overt Act No. 21: On August 19, 2019, after receiving an electronic message from UICC 3 containing the business name, account number, SWIFT code, and business address for the CIBC Account, defendant ALAUMARY sent that information to UICC 2.

Overt Act No. 22: On August 19, 2019, UICC 2 or a coconspirator fraudulently induced the Victim Federal Contractor through a BEC scheme to wire transfer approximately $538,781.66 to US Bank Account 1.

Overt Act No. 23: On August 20, 2019, at the direction of defendant ALAUMARY, a coconspirator attempted a wire transfer of approximately $509,880 from US Bank Account 1 to the CIBC Account.

Overt Act No. 24: On September 13, 2019, defendant ALAUMARY instructed UICC 4 to open a business bank account in the name of a specific business ("Company B").

Overt Act No. 25: On September 17, 2019, at the direction of defendant ALAUMARY, UICC 4 and another coconspirator filed a fictitious business name statement with the LACRRCC in the name of Company B.

Overt Act No. 26: On September 17, 2019, at the direction of defendant ALAUMARY, UICC 4 and another coconspirator opened US Bank Account 2 in Inglewood, California, in the name of Company B.

Overt Act No. 27: On September 17, 2019, defendant ALAUMARY sent UICC 5 an electronic message containing the name of the account

holder of US Bank Account 1, as well as the bank account number and routing number for US Bank Account 2.

Overt Act No. 28: On September 19, 2019, UICC 5 or a coconspirator induced the Victim Consumer Products Company to wire transfer approximately $1,170,175.21 to US Bank Account 2.

Overt Act No. 29: On September 19, 2019, defendant ALAUMARY sent electronic messages to UICC 4 saying "His doing t now," and "[c]heck the us bank 1.1."

Overt Act No. 30: On September 19, 2019, defendant ALAUMARY communicated by video chat with UICC 4, and thereafter sent an electronic message to UICC 5 containing a mobile device screenshot of an ATM receipt for US Bank Account 2 showing a balance of $1,169,775.21.

Overt Act No. 31: On September 19, 2019, defendant ALAUMARY exchanged electronic messages with UICC 5 about a check, and defendant ALAUMARY caused a coconspirator to send by FedEx -- to a California address provided by UICC 5 -- a check of approximately $772,000 drawn from US Bank Account 2.

Overt Act No. 32: On October 15, 2019, unindicted coconspirator Abbas or a coconspirator fraudulently induced the Victim Law Firm to wire transfer approximately $922,857.76 from its account at Quontic Bank, held in the State of New York, to the Chase Account.

Overt Act No. 33: On October 17, 2019, unindicted coconspirator Abbas sent defendant ALAUMARY an electronic message containing a photograph of a wire transfer confirmation relating to a wire transfer of approximately $396,050 from the Chase Account to the CIBC Account.

Overt Act No. 34: On October 17, 2019, defendant ALAUMARY informed UICC 3, through an electronic message, to look for a wire transfer of approximately $396,050 to the CIBC Account.

Overt Act No. 35: On October 17, 2019, while within the Central District of California, UICC 3 informed defendant ALAUMARY, through an electronic message, that the sum of approximately $396,050 had been credited to the CIBC Account.

Overt Act No. 36: On October 17, 2019, defendant ALAUMARY told unindicted coconspirator Abbas, through an electronic message, that the wire transfer of approximately $396,050 from the Chase Account to the CIBC Account had been completed.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 982 and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 982(a)(1) and Title 28, United States Code, Section 2461(c), in the event of defendant's conviction of the offense set forth in Count One of this Information.

2. Defendant, if so convicted, shall forfeit to the United States of America the following:

(a) Any property, real or personal, involved in such offense, and any property traceable to such property; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 982(b)(2), defendant, if so convicted, shall forfeit substitute property, if, by any act or omission of defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, 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 that cannot be divided without difficulty. Substitution of assets shall not be ordered, however, where the convicted defendant acted merely as an intermediary who handled but did not retain the property in the

course of the money laundering offense unless defendant, in committing the offense or offenses giving rise to the forfeiture, conducted three or more separate transactions involving a total of $100,000.00 or more in any twelve-month period.

NICOLA T. HANNA
United States Attorney

CHRISTOPHER D. GRIGG
Assistant United States Attorney
Chief, National Security Division

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

ANIL J. ANTONY
Assistant United States Attorney
Deputy Chief, Cyber & Intellectual Property Crimes Section

KHALDOUN SHOBAKI
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section