2015R00692/LJW

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 15-
	:	
MUHAMMAD SOHAIL QASMANI, a/k/a "Sam Jee," a/k/a "Alvi Khan"	:	18 U.S.C. § 1349

INFORMATION

The defendant having waived in court prosecution by indictment, the United States Attorney for the District of New Jersey charges:

COUNT ONE
(Wire Fraud Conspiracy)

Relevant Individuals and Companies

1. At all times relevant to this Information:

The Defendant

a. Defendant MUHAMMAD SOHAIL QASMANI, a/k/a "Sam Jee," a/k/a "Alvi Khan," was a national of Pakistan who resided in Thailand where he operated Qasmani Trading Company Ltd. ("QTC").

Coconspirators

b. Coconspirator 1, an individual not named as a defendant herein ("CC-1"), was a national of Pakistan who resided in Saudi Arabia, and later in Pakistan, and operated businesses purporting to provide premium telephone services.

c. Coconspirator 2, an individual not named as a defendant herein ("CC-2"), was a national of Pakistan and served as CC-1's business manager at one of his companies.

d. Coconspirator 3, an individual not named as a defendant herein ("CC-3"), was a citizen of Germany who resided in Switzerland. CC-3 operated companies in Germany and Switzerland, both of which advertised themselves on the Internet as telecommunications companies.

A Victim of the Scheme

e. Victim 1 was an international telephone company with major operating centers and a fraud detection center located in New Jersey.

Background Regarding the Scheme

f. *PBX Systems.* Large businesses and organizations commonly used private computer systems to operate their internal telephone networks. Such internal telephone networks were referred to as Private Branch exchanges, or "PBX." The primary functions of PBX systems included making connections for internal calls placed within the system (*i.e.*, when one employee called another employee) and connecting internal users of the system to public telephone networks, very often for the purpose of making long distance telephone calls which were then charged to the business. PBX systems also directed calls made to a business' main number to the desired extension.

g. *PBX Hacking.* Since approximately 1999, there has been an ongoing scheme to gain unauthorized access (hereafter referred to as "hacking") into PBX systems of large corporations in the United States. As part of the scheme, hackers target the PBX systems of certain corporations and place calls

to those systems in an attempt to identify telephone extensions that are not in use. Once an unused extension is identified, the hackers reprogram the telephone system. The hacked telephone system can then be used by the hackers and others to make telephone calls that are charged back to the victim corporation. In short, the hackers take control of existing telephone lines through which they and their coconspirators can make calls at no cost to the hackers. Of course, the calls are not really free because the corporations that own and operate the PBX systems are charged for the calls from the telephone companies.

h. *Revenue Share Numbers* ("RSNs" or "Premium Numbers") are special high-rate numbers that typically host content that callers seek to access (*e.g.*, adult entertainment, chat lines, and psychic lines) on a cost-per-minute basis.

i. *Revenue Share Providers* ("RSPs" or the "Providers") are companies that lease telephone numbers from overseas telephone companies that the Providers use to host Premium Numbers. When a person places a call to a Premium Number, the Provider earns a portion of the per-minute revenue generated by the call. For example, if a Provider named "Provider A" leased a telephone number from a telephone company in Austria and set up a Premium Number on that telephone line, Provider A would receive a percentage of the rate that the Austrian telephone company charged for every minute of calls placed to that number. As part of the contractual arrangement between telephone companies and the Providers, the telephone companies (*e.g.*, Victim 1) pay the Providers for the calls made to the Premium Numbers and the

telephone companies are then left to collect their revenues from subscribers of numbers used to initiate the calls. Providers of Premium Numbers can sublease them to individuals and entities. In that case, the Providers pass on the proceeds they receive from telephone companies to the customers who leased out the Premium Numbers from the Providers.

The Conspiracy

2. From in or about November 2008 through on or about December 31, 2012, in the District of New Jersey, and elsewhere, defendant

MUHAMMAD SOHAIL QASMANI,
a/k/a "Sam Jee,"
a/k/a "Alvi Khan,"

did knowingly and intentionally conspire and agree with CC-1, CC-2, CC-3, and 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 transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce certain writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

Object of the Conspiracy

3. It was the object of the conspiracy for defendant QASMANI, CC-1, CC-2, CC-3, and others to fraudulently obtain money from telephone companies by causing unauthorized telephone calls to be made to Premium Numbers that were controlled by members of the conspiracy.

Manner and Means of the Conspiracy

The Fraudulent Revenue Share Numbers

4. It was part of the conspiracy that CC-1, CC-2, and CC-3 falsely represented to Providers and telephone companies that they were providing legitimate Premium Numbers when, in fact, they never intended to have legitimate calls placed to their Premium Numbers.

5. It was further part of the conspiracy that CC-1, CC-2, and CC-3 entered into contracts and agreements with Providers and telephone companies for the use of Premium Numbers. The contracts contained specific provisions regarding fraudulent activity, including provisions relating to unauthorized telephone calls. CC-1, CC-2, and CC-3 signed such contracts and represented that they would meet common carrier industry standards despite knowing that there would be no legitimate calls made to their Premium Numbers.

6. It was further part of the conspiracy that the Premium Numbers offered by CC-1 and CC-2 frequently contained no actual content (*i.e.*, did not have adult entertainment, chat rooms, or psychic lines) ("the Fraudulent Premium Numbers") and could, therefore, never generate legitimate fee revenue for the Providers or telephone companies. Telephone company representatives who dialed the Fraudulent Premium Numbers upon suspecting them of fraud have advised the FBI that the Fraudulent Premium Numbers frequently had recordings of fake rings, fake password prompts, fake voicemail messages, music, or dead air. When CC-1 and CC-2 did provide content, it was done in order to disguise the fraudulent nature of the Premium Numbers from victim telephone companies. In some cases, the Fraudulent Premium Numbers would

play fake audio files (such as instructions to enter a pin code or introductory instructions) that mimicked legitimate Premium Numbers. As a result, when fraud investigators dialed suspected Fraudulent Premium Numbers, they could be deceived into believing that the Fraudulent Premium Numbers were in fact legitimate.

7. It was further part of the conspiracy that CC-1 and CC-3 limited the frequency and duration of fraudulent call traffic to the Premium Numbers they controlled in order to minimize the risk that the unauthorized call traffic would be identified as fraudulent by interconnection carries, such as Victim 1. There is no legitimate reason for an RSP to limit the frequency or duration of calls to an RSN from a single phone number. To the contrary, a legitimate RSP would prefer frequent and long-duration calls because the frequency and duration of the calls is what drives the revenue and, therefore, the profits of RSPs.

Generating Fraud Proceeds By Using Compromised PBX Systems

8. It was further part of the conspiracy that CC-1 procured the services of individuals who gained unauthorized access to PBX systems ("Hackers") and individuals who generated unauthorized telephone calls from those systems to Premium Numbers that CC-1 and his coconspirators had leased ("Dialers"). Many of the compromised PBX systems were in the United States, including those in New Jersey, while the Hackers and Dialers typically were located abroad. As fraudulent call traffic to CC-1's Premium Numbers increased, so too did the illicit gains to CC-1 and the corresponding losses to the victims from these "stolen" calls.

Receiving Fraud Proceeds and Paying the Haçkers and Dialers

9. It was further part of the conspiracy that defendant QASMANI helped CC-1 to operate the scheme and avoid detection by (1) providing numerous bank accounts to receive the proceeds of the fraud; and (2) making money transfers from those accounts to the Hackers and Dialers at CC-1's direction.

10. It was further part of the conspiracy that defendant QASMANI provided CC-1 ten different bank accounts between the charged dates of the conspiracy to receive the fraud proceeds and paid the Hackers and Dialers from those accounts at CC-1's direction. None of those ten accounts were in the name of CC-1 or his companies. The account names for eight of the accounts had no apparent connection to defendant QASMANI or QTC. Defendant QASMANI kept CC-1 updated regarding money movements from the accounts by sending e-mails from Thailand to Saudi Arabia, and later to Pakistan, reflecting confirmations regarding the payments.

11. It was further part of the conspiracy that on March 11, 2009, defendant QASMANI created a new e-mail account with username "sam.1786" and registered it under the false name "Sam Jee." Defendant QASMANI thereafter used that account for the majority of his e-mail communications with CC-1 concerning receiving fraud proceeds and making payments to the Hackers and Dialers.

12. It was further part of the conspiracy that CC-1 forwarded defendant QASMANI e-mails from RSPs advising that payment of revenue otherwise owed to CC-1 had been withheld based on suspicion of fraudulent

activity. Several of those e-mails included invoices from the RSPs showing a breakdown of the revenue that had been blocked based on suspicion of fraudulent activity.

13. It was further part of the conspiracy that, despite being arrested CC-1 continued to the operate the scheme. Specifically, on May 21, 2012, Malaysian authorities took CC-1 into custody based on charges that CC-1 conspired with others to hack into PBX systems and generate unauthorized calls to Premium Numbers controlled by CC-1 and members of the conspiracy. Thereafter, on July 25, 2012, CC-1 was released from custody and was deported to Pakistan. Shortly after arriving in Pakistan, CC-1 created a new e-mail account with username "bluechiptelecoms," which he began using to continue the PBX hacking and fraud scheme.

14. It was further part of the conspiracy that, following CC-1's arrest and deportation to Pakistan, on August 8, 2012 defendant QASMANI created a new e-mail account with username "alvikhan1786" and registered it under the false name "Alvi Khan." Defendant QASMANI thereafter used that account for the sole and exclusive purpose of communicating with CC-1 about receiving fraud proceeds and making payments to Hackers and Dialers just as he had done so before CC-1's arrest.

15. It was further part of the conspiracy that defendant QASMANI transferred approximately $19 million to more than 650 transferees at CC-1's direction from the illicit proceeds generated by this scheme.

Losses to Victim 1 from the Scheme

16. The money transferred out of bank accounts by defendant QASMANI reflects a portion of the actual losses to Victim 1 and other telephone companies that paid overseas telephone companies internationally regulated fees to carry telephone traffic to overseas Premium Numbers that turned out to be vehicles for fraud. Victim 1 and other telephone companies could not recover their losses because the call traffic was fraudulent.

Fraudulent Activity

17. To further the conspiracy, defendant QASMANI, CC-1, CC-2, CC-3 and others engaged in the following conduct:

Managing the Tradecraft of the Hackers and Dialers to Avoid Detection

a. On August 19, 2009, CC-1 was negotiating a deal and asked the other party to the deal for information about the destination of the telephone calls. The other party asked CC-1 if he could work with "hacked" calls, to which CC-1 replied "YES, NO PROBLEM" (emphasis in the original).

b. CC-1 routinely received notice that call traffic to his Premium Numbers was generated through hacked PBX systems. For example, on August 16, 2010, September 2, 2010, October 30, 2010, April 12, 2011 and May 18, 2011, CC-1 received notices from different RSPs that his Premium Numbers were receiving calls from hacked PBX systems.

c. In March 2011, CC-1 received another report from an RSP concerning fraudulent call traffic to his Premium Numbers coming from a hacked PBX system. Instead of stopping calls from the hacked PBX system, on March 27, 2011, CC-1 contacted his Dialer responsible for the fraudulent call

traffic and instructed him to either make the calls appear legitimate or stop the calls. Specifically, CC-1 wrote: "[E]ither rotate the CLIs or send [call] traffic by hide CLI or stop further [call] traffic." CC-1's reference to "CLIs" referred to Call Line Identification number, which identify the telephone number calling the Premium Number. Furthermore, CC-1's instruction to "rotate" and/or "hide" CLIs was intended to decrease the risk that the call traffic would be identified as fraudulent by interconnection carries, such as Victim 1. This is because, in a scheme like this one, the CLI points back to a hacked PBX system.

Standing Up Bank Accounts to Receive the Fraud Proceeds

d. On the dates listed in the table below, defendant QASMANI sent e-mails to CC-1 providing the details of bank accounts that CC-1, in turn, provided to RSPs for the purpose of having the RSPs remit payments to CC-1 As noted above, the names of the accounts had no apparent connection to CC-1 or his businesses, and eight of the ten accounts had no apparent connection to defendant QASMANI or QTC.

Date	**Acct. No.**
08/17/2008	xxxxxxxx4838
11/07/2008	xxxxxxxx8833
08/17/2009	xxxxxxxx0838
03/30/2010	xxxxxxxx7838
08/09/2010	xxxxxxxx9833
12/17/2010	xxxxxxxxxx2225
10/20/2011	xxxxxxxx4838
02/22/2012	xxxxxxxx0168

02/22/2012	xxxxxxxx1883
11/28/2012	xxxxxxxxxx5069

e. In two of the e-mails referred to in the preceding subparagraph, defendant QASMANI wrote: "PLZ DO FORWARD THIS NEW ACCOUNT BANK DETAIL WHICH I AM GIVEN U BELOW FOR TRANSFERS TO YOUR CO-WORKERS" (emphasis in the original).

Directing Payments to Hackers and Dialers

f. Between August 14, 2008, and May 21, 2012 (*i.e.*, the date of CC-1's arrest in Malaysia), CC-1 sent more than one thousand e-mails to defendant QASMANI directing him to make more than three thousand transfers from the bank accounts that defendant QASMANI had provided to receive the fraud proceeds. Those e-mails revealed approximately 650 unique transferees, located in at least 10 countries, including the Philippines, India, Pakistan, Malaysia, China, the United Arab Emirates, Saudi Arabia, Indonesia, Thailand, and Italy. The total amount that defendant QASMANI transferred as of May 21, 2012 was approximately $19 million.

Continuing the Fraudulent Activity Even After CC-1's Arrest

g. Within weeks of his release from custody, on August 31, 2012, CC-1 began sending e-mails from the newly-created CC-1 Account 2 to defendant QASMANI at the newly-created MSQ Account 3 notifying him of incoming proceeds from RSPs, just as he had before his arrest.

h. On the same day, defendant QASAMNI began sending e-mails from MSQ Account 3 to CC-1 at CC-1 Account 2 confirming the details of

the money transfers that he had made during the period of CC-1's incarceration, just as he had before CC-1's arrest.

i. On September 11, 2012, CC-1 began sending e-mails from CC-1 Account 2 to defendant QASMANI at MSQ Account 3 directing defendant QASMANI to make money transfers, just as he had before his arrest.

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

Forfeiture Allegation

1. The allegations contained in this Information are incorporated by reference as though set forth in full herein for the purpose of noticing forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c).

2. The United States hereby gives notice to the defendant, that upon his conviction of the offense charged in this Information, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c), which requires any person convicted of such offenses to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offenses. The forfeiture shall be the following:

(a) A Money Judgment in the amount of $25,000.

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

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section

2461(c), to seek forfeiture of any other property of such defendants up to the value of the forfeitable property described above.

Paul J. Fishman

PAUL J. FISHMAN
United States Attorney

CASE NUMBER: 2015R00692

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

MUHAMMAD SOHAIL QASMANI

INFORMATION FOR

18 U.S.C. § 1349

PAUL J. FISHMAN
UNITED STATES ATTORNEY
NEWARK, NEW JERSEY

L. JUDSON WELLE
ASSISTANT U.S. ATTORNEY
(973) 645-2700

USA-48AD 8
(Ed. 1/97)