UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA

v.

[1] HGLOBAL,
[2] CALL MANTRA,
d.b.a. Robust Inc., Raytheon International,
[3] WORLDWIDE SOLUTION,
[4] ZORIION COMMUNICATIONS PVT. LTD.,
[5] SHARMA BPO SERVICES,
[6] HITESH MADHUBHAI PATEL,
a.k.a. Hitesh Hinglaj,
[7] HARDIK ARVINDBHAI PATEL,
[8] JANAK GANGARAM SHARMA,
[9] TILAK SANJAYBHAI JOSHI,
[10] SAURIN JAYESHKUMAR RATHOD,
[11] TARANG RANCHHODBHAI PATEL,
[12] KUSHAL NIKHILBHAI SHAH,
[13] KARAN JANAKBHAI THAKKAR,
[14] MANISH BALKRISHNA BHARAJ,
[15] RAJPAL VASTUPAL SHAH,
[16] SAGAR THAKAR,
a.k.a. Shaggy, Shahagir Thakkar,
[17] CYRIL JHON DANIEL,
[18] JATIN VIJAYBHAI SOLANKI,
[19] JERRY NORRIS,
a.k.a. James Norris, IV,
[20] NISARG PATEL,
[21] MITESHKUMAR PATEL,
a.k.a. Mitesh,
[22] RAJUBHAI BHOLABHAI PATEL,
[23] ASHVINBHAI CHAUDHARI,
[24] FAHAD ALI,
[25] JAGDISHKUMAR CHAUDHARI,
a.k.a. Jagdish,
[26] BHARATKUMAR PATEL,
a.k.a. Bharat,
[27] ASMITABEN PATEL,
[28] VIJAYKUMAR PATEL,
[29] MONTU BAROT,
a.k.a. Monty Barot,
[30] PRAFUL PATEL,
[31] ASHWINBHAI KABARIA,
[32] DILIPKUMAR RAMANLAL PATEL,

SEALED

CRIMINAL NO. 4:16-cr-385-S

18 U.S.C. § 371
Conspiracy
(Count 1)

18 U.S.C. § 1349
Wire Fraud Conspiracy
(Count 2)

18 U.S.C. § 1956(h)
Money Laundering Conspiracy
(Count 3)

18 U.S.C. § 1952
False Statement in Application for Passport
(Counts 4 & 5)

18 U.S.C. § 981
18 U.S.C. § 982
28 U.S.C. § 2461
Forfeiture Allegations

TRUE COPY I CERTIFY
ATTEST:
DAVID J. BRADLEY, Clerk of Court
By Kathleen Murphy
Deputy Clerk

[33] NILAM PARIKH,
[34] DILIPKUMAR AMBAL PATEL,
a.k.a. Don Patel,
[35] VIRAJ PATEL,
[36] ABHISHEK RAJDEV TRIVEDI,
[37] SAMARTH KAMLESHBHAI PATEL,
[38] HARSH PATEL,
[39] AALAMKHAN SIKANDERKHAN PATHAN,
[40] JAYKUMAR RAJANIKANT JOSHI,
[41] ANJANEE PRADEEPKUMAR SHETH,
[42] KUNAL CHATRABHUJ NAGRANI,
[43] SUBISH SURENRAN EZHAVA,
a.k.a. Chris Woods,
[44] SUNNY TARUNKUMAR SUREJA,
a.k.a. Khavya Sureja,
[45] SUNNY JOSHI,
a.k.a. Sharad Ishwarlal Joshi, Sunny Mahashanker Joshi,
[46] RAJESH BHATT,
a.k.a. Manoj Joshi, Mike Joshi,
[47] NILESH PANDYA,
[48] TARUN DEEPAKBHAI SADHU,
[49] VISHALKUMAR RAVI GOUNDER,
a.k.a. Vishal Gounder,
[50] BHAVESH PATEL,
[51] RAMAN PATEL,
[52] RAJESH KUMAR UN,
[53] ANIRUDDH RAJESHKUMAR CHAUHAN,
[54] RAHUL TILAK VIJAY DOGRA,
[55] VICKY RAJKAMAL BHARDWAJ,
[56] CLINTWIN JACOB CHRISSTIAN,
a.k.a. Clintwin Jacob, Clintwin Jacob Christian,
[57] ANEESH ANTONY PADIPURIKAL,
a.k.a. Aneesh Anthony,
[58] JATANKUMAR HARESHKUMAR OZA,
a.k.a. Jatan Oza,
[59] RAJKAMAL OMPRAKASH SHARMA,
[60] VINEET DHARMENDRA VASISHTHA,
a.k.a. Vineet Sharma, Vineet Vashistha, and
[61] GOPAL VENKATESAN PILLAI,

Defendants.

SUPERSEDING INDICTMENT

THE GRAND JURY CHARGES:

General Allegations

"Telefraud"[1] Scam

1. As used in this Indictment, a "call center" was an organization or group of organizations that defendants used in connection with a scheme to defraud U.S. residents by misleading U.S. residents into sending money utilizing a number of different confidence scams, to include:

a. IRS scam: India-based call centers impersonated U.S. Internal Revenue Service (IRS) officers and defrauded U.S. residents by misleading them into believing that they owed money to the IRS and would be arrested and fined if they did not pay their alleged back taxes immediately.

b. USCIS scam: India-based call centers impersonated U.S. Citizen and Immigration Services (USCIS) officers and defrauded U.S. residents by misleading them into believing that they would be deported unless they paid a fine immediately for alleged issues with their USCIS paperwork.

c. Payday loan scam: India-based call centers defrauded U.S. residents by misleading them into believing that the callers were loan officers and that the U.S. residents were eligible for a fictitious "payday loan" (small, short-term, unsecured loan in which repayment is

[1] Telefraud is a term describing fraud activity via telephonic means.

generally linked to a borrower's next paycheck or regular income payment, such as a social security check). The India-based callers directed the U.S. residents to pay an upfront "worthiness fee" to demonstrate an ability to repay the loan. The victims received nothing in return.

d. Government grant scam: India-based call centers defrauded U.S. residents by misleading them into believing that they were eligible for a fictitious government grant. Callers directed the U.S. residents to pay an upfront IRS tax or processing fee. The victims received nothing in return.

Roles in the Operation

2. The defendants held one or more of the following roles in furtherance of the conspiracy:

a. Runner: The defendants referred to below as "Runners" were located in the United States and typically operated regionally. Runners purchased temporary general purpose reloadable ("GPR") cards; forwarded the unique GPR card numbers to the Payment Processors located in India so the cards could be registered; purchased money orders using GPR cards funded with fraud proceeds; retrieved cash payments of scammed funds via money transmitters such as Western Union and MoneyGram using fake identification documents; and deposited scammed funds into bank accounts. Runners were often directed by Domestic Managers.

b. Domestic Manager: The defendants referred to below as "Domestic Managers" were located in the United States and directed runners' activities and at times provided runners with resources and supplies, such as vehicles and credit cards for travel expenses. Domestic

Managers were often the direct points of contact with the Call Center Operators and Payment Processors in India, including to negotiate their crew's payout of scammed funds.

c. Call Center Operator: The defendants referred to below as "Call Center Operators" were located in India and oversaw and managed the day-to-day operations of the call centers, such as keeping time and attendance; maintaining the facilities, to include acquiring telephone numbers from which scam calls would be made; maintaining expense sheets for respective call centers; obtaining and distributing "lead lists";[2] and creating monthly invoices for Payment Processors regarding how much was owed to the call centers based on the amount of scam funds the call centers accrued. In some cases, the Call Center Operators had equity shares in the call centers.

d. Caller: The individuals referred to as "Callers" received lead list information and call scripts. Callers made fraudulent and extortionate calls to victims in the U.S. and elsewhere, purporting to be U.S. government officials or money lenders in order to extract scammed funds from victims.

e. Payment Processor: The defendants referred to below as "Payment Processors" were located in India, were often affiliated with particular call centers, and were the intermediaries between the call centers and the Runners. For example, they facilitated overseas payments for hawaladars, activated (or managed individuals who activated) GPR cards with

---

[2] A short-form "lead list" contained personally identifiable information such as name, address, and telephone numbers. A long-form "lead list" contained personally identifiable information such as name, address, telephone numbers, dates of birth, and social security numbers, among other pieces of identifying information.

unwitting U.S. citizens' personally identifiable information ("PII"), communicated with and instructed Runners to liquidate GPR cards, transferred scammed funds from prepaid stored value cards to GPR cards, and liaised with call centers that made the scam calls.

f. Data Broker: The defendants referred to below as "Data Brokers" identified and contacted U.S. and foreign lead generators and marketing companies to purchase names and PII for registering GPR cards and targeting potential victims. Data Brokers also facilitated payment for PII through domestic Runners.

g. Hawaladar: The defendant referred to below as a "Hawaladar" was located in India and liaised between hawaladars in cities outside India and the India-based call centers to obtain requests for funds which would be fulfilled by the call centers. Hawaladar is a person who operates a "hawala". A hawala is an underground banking system based on trust through which money can be made available internationally without actually moving it or leaving a record of the transaction. In a hawala system, a person wanting to send money abroad contacts a broker (the hawaladar), and gives him money, a fee, name, and location of the person to whom he wants the money delivered. The hawaladar contacts another hawaladar in the recipient's country, and the second hawaladar delivers the money to the recipient. The first hawaladar then owes the transferred amount to the second, and the debt is frequently repaid by transactions conducted in the reverse direction.

Call Centers

3. In this Indictment, there are five major conglomerates of call centers, all located in Ahmedabad, Gujarat, India: HGlobal, Call Mantra, Worldwide Solution, Zoriion

Communications, and Sharma BPO (Business Process Outsourcing). During the course of the conspiracy, the call center conglomerates often acted together to effect the scheme, to include: sharing call scripts and lists of potential victims, processing payments for each other, and liquidating victim scammed funds.

HGLOBAL		
DEFENDANTS	**PRIMARY ROLE**	**LOCATION**
HITESH PATEL (a.k.a. HITESH HINGLAJ)	Call Center Operator	India
HARDIK PATEL	Call Center Operator	India
JANAK SHARMA	Payment Processor	India
TILAK JOSHI	Call Center Operator & Payment Processor	India
SAURIN RATHOD	Data Broker	India
TARANG PATEL	Data Broker	India
KUSHAL SHAH	Payment Processor	India
KARAN THAKKAR	Payment Processor	India
MANISH BHARAJ	Call Center Operator	India
RAJPAL SHAH	Call Center Operator & Runner	India
SAGAR THAKAR	Call Center Operator & Payment Processor	India
CYRIL JHON DANIEL	Payment Processor	India
JATIN SOLANKI	Payment Processor	India
JERRY NORRIS	Runner	Oakland, CA
NISARG PATEL	Runner	Warner Robbins, GA

MITESHKUMAR PATEL	Domestic Manager	Willowbrook, IL
RAJUBHAI PATEL	Domestic Manager	Willowbrook, IL
ASHVINBHAI CHAUDHARI	Runner	Louisiana and Texas
FAHAD ALI	Runner	Dyer, IN
JAGDISH CHAUDHARI	Runner	Sarasota, FL
BHARATKUMAR PATEL	Runner	Midlothian, IL
ASMITABEN PATEL	Runner	Willowbrook, IL
VIJAYKUMAR PATEL	Runner	Schiller Park, IL
MONTU BAROT	Runner	Glendale Heights, IL
PRAFUL PATEL	Runner	Fort Meyers, FL
ASHWIN KABARIA	Runner	Bradenton, FL
DILIPKUMAR RAMANLAL PATEL	Runner	Ocala, Florida
NILAM PARIKH	Runner	Pelham, AL
DILIPKUMAR AMBAL PATEL	Runner	Corona, CA
VIRAJ PATEL	Payment Processor	Anaheim, CA
ABHISHEK TRIVEDI	Payment Processor	India
SAMARTH PATEL	Payment Processor	India
HARSH PATEL	Runner	New Jersey
AALAMKHAN SIKANDERKHAN PATHAN	Call Center Operator	India
JAYKUMAR RAJANIKANT JOSHI	Call Center Operator	India
ANJANEE PRADEEPKUMAR SHETH	Call Center Operator	India

CALL MANTRA		
TARGET	**PRIMARY ROLE**	**LOCATION**
KUNAL NAGRANI	Call Center Operator	India
SUBISH EZHAVA	Call Center Operator	India
SUNNY SUREJA	Call Center Operator	India
SUNNY JOSHI	Domestic Manager	Sugar Land, TX
RAJESH BHATT (a.k.a. MANOJ JOSHI)	Domestic Manager	Sugar Land, TX
NILESH PANDYA	Runner	Stafford, TX

WORLDWIDE SOLUTION		
TARGET	**PRIMARY ROLE**	**LOCATION**
TARUN SADHU	Call Center Operator	India
VISHAL GOUNDER	Payment Processor	India
BHAVESH PATEL	Domestic Manager	Phoenix, AZ
RAMAN PATEL	Runner	Phoenix, AZ
RAJESH KUMAR UN	Runner	Phoenix, AZ

ZORIION		
TARGET	**PRIMARY ROLE**	**LOCATION**
ANIRUDDH CHAUHAN	Call Center Operator	India
RAHUL DOGRA	Call Center Operator & Payment Processor	India

VICKY BHARDWAJ (a.k.a. VICKY SHARMA)	Call Center Operator	India
CLINTWIN JACOB	Call Center Operator	India
ANEESH ANTHONY	Call Center Operator	India
JATAN OZA	Payment Processor	India
RAJKAMAL SHARMA	Hawaladar	India

SHARMA BPO SERVICES		
TARGET	**PRIMARY ROLE**	**LOCATION**
VINEET VASISHTHA	Call Center Operator	India
GOPAL PILLAI	Call Center Operator	India

Definitions

4. At all times relevant to this Indictment:

a. "Prepaid stored value cards" were cards that had monetary value placed onto them by purchasers and could be used to fund GPR cards. They were also called "MoneyPaks", "Reloadit", etc., depending on the brand.

b. "GPR cards" or general purpose reloadable cards were cards that had monetary value and could be used like a debit without being associated with a personal bank account. GPR cards were funded and can be reloaded using prepaid stored value cards.

c. Green Dot Corporation ("Green Dot") was an entity that, among other things, sold GPR cards ("Green Dot cards"). Green Dot cards, once funded, could be used to make purchases.

i. In order to fund a Green Dot card, individuals using the cards were first required to register the card telephonically or online by providing, among other things, a name, address, telephone number, date of birth, and social security number.

ii. There were several ways to fund a Green Dot card. One involved the purchase of a MoneyPak card from retail stores such as CVS and Walgreens in amounts from $20 to $500. Once purchased, the customer could, using a code (PIN or personal identification number) on the back of the MoneyPak card, authorize a transfer of funds from the MoneyPak card to a GPR card. For instance, a customer that purchased a $500 MoneyPak could provide the PIN code associated with their MoneyPak to an individual who had a Green Dot card. The Green Dot card holder could then effect the transfer through Green Dot's website or by calling Green Dot's toll free number and providing both the Green Dot card number and the MoneyPak PIN code.

d. Blackhawk Network Holdings ("Blackhawk") was an entity that, among other things, sold "Reloadit" prepaid stored value cards which operated similarly to Green Dot MoneyPaks.

e. Personally identifiable information ("PII") or sensitive personal information is information that can be used on its own or with other information to identify, contact, or locate a person.

f. The terms "accessing" and "accessed" refer to 1) electronically or telephonically registering GPR cards with misappropriated PII; 2) electronically or telephonically transferring victim scammed funds from stored value cards to GPRs; or 3) electronically or telephonically

checking balances of GPR cards.

g. A "money services business" transferred funds on behalf of the public to other locations within the U.S. or to locations abroad by means of wire transfers, such as Western Union or MoneyGram. These businesses also sell money orders.

h. Voice-over Internet Protocol (VoIP) was a telephone connection over the internet; the data was sent digitally using the internet protocol instead of analog telephone lines.

i. "Spoofing" was a mechanism whereby callers could deliberately falsify the information transmitted to a victim's caller ID and thereby disguise their identity or location.

j. YMax Corporation or "Magic Jack" phone numbers utilized physical devices which employed VoIP to allow users to make unlimited local or long distance phone calls to U.S. and Canadian telephone numbers using an existing internet connection; users could make and receive calls using a computer or phone. No additional telephone service was required. A Magic Jack application (or computer program) could substitute as the physical device. Users were permitted to choose the phone number associated with the Magic Jack.

k. A lead generator was an individual or company which used proprietary methods to produce leads usually in mass quantities to sell to other businesses.

Pertinent Phone Numbers

5. During the course of the investigation, the conspirators used approximately 1,500 Magic Jack numbers to defraud victims and to facilitate the transfer of victim funds. The Magic Jack numbers below were some of the most active numbers used to perpetrate the scheme.

6. Targets of the investigation were involved in the bulk purchasing of Magic Jack

devices. On November 18, 2011, ASVHWIN KABARIA using acs.wun@gmail.com emailed HITESH PATEL and JANAK SHARMA at acsglobal3@gmail.com. The email and attached shipping label indicated that ASHWIN KABARIA shipped via UPS 20 Magic Jack devices to an HGLOBAL conspirator in India. On March 7, 2012, ASHWIN KABARIA using acs.wun@gmail.com emailed HITESH PATEL at hitesh.hinglaj@gmail.com indicating that 41 Magic Jack devices had been shipped via UPS to TILAK JOSHI in India. On September 25, 2012, ASHWIN KABARIA using acs.wun@gmail.com emailed HITESH PATEL and JANAK SHARMA who operated email address acsglobal3@gmail.com. The email indicated that ASHWIN shipped 40 Magic Jack devices using UPS to a conspirator in Hoffman Estates, IL.

7. (713) 370-3224 Magic Jack: (713) 370-3224 was a YMax Communications VoIP telephone number ("713 Magic Jack") registered in the name of an individual at an address in Waco, TX, by individuals in Ahmedabad, Gujarat, India. This phone number accessed more than 4,000 Green Dot GPR cards that were registered in more than 1,200 different misappropriated identities in the year 2013. (713) 370-3224 was controlled by HITESH PATEL and other HGLOBAL associates. The subscriber information associated with 713 Magic Jack included the email address JHS.Hinglaj24@yahoo.com. In a Google chat on March 12, 2013 (saved as an email in the acsglobal3@gmail.com account) between HITESH PATEL and ASHWIN KABARIA, HITESH provided the 713 Magic Jack phone number during a conversation about transferring money. The subscriber information for acsglobal3@gmail.com lists the recovery email account as hitesh.hinglaj@gmail.com and HITESH's Indian phone number 9879090909, which HITESH listed on his U.S. visa application.

8. (630) 974-1367 Magic Jack: (630) 974-1367 was a YMax Communications VoIP telephone number ("630 Magic Jack") registered to a person at an address in Aurora, Illinois by individuals in Ahmedabad, Gujarat, India. This phone number accessed more than 990 Green Dot GPR cards that were registered in more than 776 different misappropriated identities from December 28, 2013 through December 23, 2014. The 630 Magic Jack was controlled by HITESH PATEL, JANAK SHARMA, and other HGLOBAL associates. The 630 Magic Jack replaced the 713 Magic Jack and accessed the same IP address. The 630 Magic Jack was registered on January 13, 2014 using IP address 216.169.138.203. On the same day, the 713 Magic Jack placed a phone call to a Green Dot customer service telephone number from IP address 216.169.138.203. The subscriber information associated with 630 Magic Jack listed the password for the Magic Jack account as "DIPESH2008". Between March 18, 2013 and November 7, 2013, email account hglobal01@gmail.com sent at least five (5) emails containing GPR cards that utilized the password "DIPESH2008" or "DIPESH@2008".

9. (785) 340-9064 Magic Jack: (785) 340-9064 was a YMax Communications VoIP telephone number ("785 Magic Jack") registered to a person at an address in Columbus, KS by individuals in Ahmedabad, Gujarat, India. This phone number accessed at least 4,163 Green Dot GPR cards that were registered in at least 1,903 different misappropriated identities from September 23, 2013 through October 18, 2014. The 785 Magic Jack was controlled by JATAN OZA. On or about October 15, 2013, JATAN OZA using jatan_oza@rocketmail.com drafted an email in which the body contained the email address that was used to register the 785 Magic Jack. The 785 Magic Jack subscriber records show that its Magic Jack application was