UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The single-family house located at 57 Gainsboro, Irvine, California 92620	)	Case No. 8:22-MJ-00358

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028	Fraud in Connection with Identification Documents
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1341	Wire Fraud
18 U.S.C. § 1343	Mail Fraud
18 U.S.C. § 1956	Laundering of Monetary Instruments
18 U.S.C. § 1957	Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity
18 U.S.C. § 2314	Interstate or Foreign Transportation of Stolen Property
21 U.S.C. § 841	Controlled Substances
21 U.S.C. § 846	Attempt and conspiracy

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Christopher B. Doering

Applicant's signature

Christopher B. Doering, Special Agent (FBI)

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Santa Ana, CA

Autumn D. Spaeth, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Rabbani (714) 338-3499

AFFIDAVIT

I, Christopher B. Doering, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation and have been so employed since October 2005. I have been assigned to the FBI Dallas Violent Crimes Task Force since July 2016. I have extensive experience conducting analysis of pen registers and call detail records, electronic surveillance, surveillance techniques, recordings, the use of criminal informants, and debriefing of defendants. I have gained extensive experience conducting a device trafficking investigation since 2021. I have learned ways that device traffickers illicitly obtain devices, traffic devices overseas, and use different methods to conduct payments associated to devices.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a search warrant for a house located at 57 Gainsboro, Irvine, California 92620 (the "SUBJECT PREMISES"), described in Attachment A, for the items to be seized described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1028 (fraud in connection with identification documents), 1028A (aggravated identity theft), 18 U.S.C. § 1341 (wire fraud), 18 U.S.C. § 1343 (mail fraud), 18 U.S.C. § 1956 (laundering of monetary instruments), 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified

unlawful activity), 18 U.S.C. §2314 (interstate or foreign transportation of stolen property), 21 U.S.C. §841 (controlled substances), and 21 U.S.C. §846 (attempt and conspiracy) (the "Subject Offenses").

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

COOPERATING DEFENDANTS

4. Cooperating defendant (CD)-1 is cooperating with the government to receive a sentence reduction. CD-1 is currently facing federal charges in the Eastern District of Texas. Prior to being federally charged, CD-1 was a Confidential Human Source ("CHS") for the FBI and closed for cause because CD-1 engaged in criminal conduct while opened as an FBI CHS. After his/her arrest, CD-1 began cooperating with the government. Much of his/her information has been corroborated. CD-1 was recently approved for re-opening by the FBI as a CHS. CD-1 is considered reliable.

5. CD-2 is cooperating with the government to receive a sentence reduction. CD-1 is currently facing federal charges in the Eastern District of Texas. Much of his/her information has been corroborated. CD-2 is considered reliable.

6. CD-3 is cooperating with the government to receive a sentence reduction. CD-3 is currently facing federal charges in the Eastern District of Texas. Much of his/her information has been corroborated. CD-3 is considered reliable.

III. SUMMARY OF PROBABLE CAUSE

7. Naeem RAZZAK d/b/a Teleport International is a wholesaler of stolen devices that include cell phones, tablets, laptops, air pods, and other cellular devices. The devices are obtained through fraud, robbery, and theft, and are referred to as "street stock". RAZZAK collects the street stock and exports it to his Dubai-based company or to Hong Kong. RAZZAK is also involved in money laundering activities related to device trafficking. RAZZAK engaged in business with multiple cooperating defendants under Eastern District of Texas cause number 4:20-CR-382.

8. Based on records checks and physical surveillance, the SUBJECT PREMISES is believed to be RAZZAK's primary residence, and there is probable cause to believe that evidence of the Subject Offenses will be found at the SUBJECT PREMISES, including on any digital devices belonging to and/or used by RAZZAK.

IV. STATEMENT OF PROBABLE CAUSE

9. The FBI is investigating a device-trafficking scheme, in which individuals and businesses have conspired to purchase street stock (stolen devices), unlock IMEIs so that the devices can be used by anyone, and export the street stock to foreign businesses since 2016. A summary of the companies involved in the scheme, and additional details of the FBI's investigation, are provided below.

COMPANIES

10. Teleport International LLC is owned by Nargis Naeem[1] and operated by Naeem RAZZAK. On May 12, 2022, RAZZAK was indicted by an Eastern District of Texas federal grand jury for violations of 18 U.S.C. § 1343, 18 U.S.C. § 1956(h), and 18 U.S.C. §2314, related to device trafficking and money laundering.

11. Always Buy More LLC, Always Pay More LLC, and Always Sell More LLC are Houston companies owned and operated by Shamsuddin Dosani or Akber Jesani[2]. On May 12, 2022, Dosani was indicted by an Eastern District of Texas federal grand jury for violations of 18 U.S.C. § 1343, 18 U.S.C. § 1956(h), and 18 U.S.C. §2314, related to device trafficking and money laundering.

12. Unlockdon Distributor LLC is owned by Arif Shaikh. Shaikh uses websites to collect locked IMEIs and submits the

[1] CD-1 advised Nargis Naeem is the wife of RAZZAK.

[2] CD-1 provided information that Jesani is a partner with Dosani. Jesani and Dosani are listed together on other company filings.

locked IMEIs to a "source" to illegally unlock the IMEIs. On May 12, 2022, Shaikh was indicted by an Eastern District of Texas federal grand jury for violations of 18 U.S.C. § 1343, 18 U.S.C. § 1956(h), and 18 U.S.C. §2314, related to device trafficking and money laundering.

13. RJ Telecom is a Dallas-based company owned and operated by Arsalan Bhangda.[3]

14. M7 Group LLC is a Dallas-based wholesaler owned and operated by Awais Ahmed.

15. SCS Supply Chain is a Dallas-based company owned and operated by Saad Aziz.

BACKGROUND OF INVESTIGATION

16. The FBI in Dallas is investigating Always Pay More, M7 Group, RJ Telecom, SCS Supply Chain, Teleport International LLC, and other entities who have exported over $200 million worth of Apple, Samsung, and other electronic products into the United Arab Emirates ("U.A.E.") and Hong Kong grey markets. Most of these electronic products, also referred to as "street stock," were derived from acts of robbery, fraud, or theft. The street stock is generally purchased by companies from the individuals obtaining the street stock ("street traffickers") with U.S. currency.

17. The grey market avoids formal distribution channels. This allows companies like Always Pay More LLC, RJ Telecom, SCS

[3] Awais Ahmed, Saad Aziz, and Arsalan Bhangda were indicted under Eastern District of Texas cause number 4:20-CR-382, for charges related to device trafficking and money laundering.

Supply Chain, M7 Group LLC, and Teleport International LLC (also known as "aggregators" or "wholesalers") to sell stolen products abroad, namely to Dubai and Hong Kong based companies.

18. Often, trafficked devices include new Apple and Samsung devices, such as cell phones, tablets, laptops, watches, and other personal cellular or electronic devices ("devices"), as well as other electronics that are illicitly obtained in the United States and exported to foreign countries like the U.A.E. and Hong Kong. There, foreign entities sell these new devices in those and other countries to end consumers.

19. Payments from foreign entities to wholesalers like RJ Telecom can come in the form of wire transfer, cryptocurrency, or cash. Wholesalers need cash to pay mini wholesalers[4] or street traffickers for the street stock. If the wholesaler received payment by wire transfer, they then must withdraw those monies in the form of cash from their bank account. Frequent cash withdrawals can lead to scrutiny by the bank and lead to their account being closed. To circumvent the bank cash withdrawals and this scrutiny, wholesalers can accept payment in the form of cash from these U.A.E. and Hong Kong companies. The cash used to pay the wholesalers is typically derived from illegitimate sources such as drug proceeds, business proceeds avoiding tax, or gambling proceeds. Thus, these foreign entities enable cash proceeds to be laundered through the trade of devices.

[4] Mini wholesalers collect street stock from device traffickers and sell to wholesalers. They generally do not aggregate and ship overseas.

20. The investigation found one common way for street traffickers to illicitly obtain devices is through new line activation fraud. New line activation fraud entails utilizing stolen identities to obtain financed phones, which are carrier locked devices. The credit of the stolen identities is used to obtain new cellular devices through financing, leaving the suspects to pay only taxes or a small down payment at the time of the transaction. Once the devices are obtained, the suspects sell, or "cash out," the devices to entities who purchase street stock like RJ Telecom, SCS Supply Chain, M7 Group LLC, Always Pay More LLC, Teleport LLC, or smaller companies (often referred to as "mini-wholesalers") who in turn sell to big wholesalers or aggregators like Teleport International, RJ Telecom and others.

21. Mobile phone carriers typically offer subscribers a locked phone, essentially restricting the phone's use to specific carriers and/or countries when a phone is purchased through financing. Network providers can lock a phone from accepting any SIM cards that are not associated with a particular carrier. Once a financed cell phone ("financed phone") is paid off, or close to being paid off, the carrier will typically unlock the cell phone.

22. For carrier locked cellular phones to be used overseas, they must first be unlocked. The unlocking process allows a phone to work with any network service as well as be used overseas. Unlocking is accomplished by using the international mobile equipment identifier ("IMEI") number of a cellular device or mobile handset. These IMEI numbers are a

unique identifier for a device. The IMEI can be unlocked within a mobile phone carrier such as AT&T, T-Mobile, or Verizon.

23. To unlock these cell phones, wholesalers use individuals with access to unlock the IMEIs through their employment. These individuals can work for a carrier or contract with one and are often referred to as "sources". These sources charge a fee per IMEI to illegally unlock the IMEI associated with the cell phone. The sources will use individuals who communicate on their behalf and are referred to as "mediators".

24. Wholesalers use individuals or companies like Shaikh d/b/a Unlockdon Distributor LLC to unlock IMEIs.

25. Shaikh has been identified as running a business that provides illegal IMEI unlocking services for wholesalers who deal in street stock. Shaikh uses websites or e-mails to collect IMEIs from wholesalers or individuals. Shaikh then submits the IMEIs to mediators or direct sources to get the IMEIs unlocked. Shaikh collects payments from the wholesalers and remits a portion of the payment to the mediator or direct source.

26. There is a higher profit margin in selling unlocked cell phones overseas, particularly in the Dubai market versus selling locked cell phones. The locked cell phones typically go to the Hong Kong market where GV, or "magic", sim cards[5] are used. The FBI's investigation has found that AT&T devices are

[5] GV SIM cards have been explained as SIM cards that allow usage of a locked phone on a different network. The SIM card can stop working after a phone is restarted or other reasons causing the owner to purchase a new SIM card. The lack of dependability makes the purchase of a locked cell phone and the use of a magic SIM card less desirable than an unlocked cell phone.

commonly targeted through new line activation fraud and transit theft, and the IMEIs for this stolen stock are routinely submitted for unlocking by these inside AT&T sources.

INVESTIGATION

27. Naeem RAZZAK is a Pakistani citizen. He maintains a Pakistani passport. In January 2020, RAZZAK interviewed for his B1/B2 visa[6]. RAZZAK advised he was visiting his two sons, one that lived in Los Angeles and one in Houston. RAZZAK stated that he had lived in the U.A.E. for the past 11 years and provided an address there. RAZZAK stated he had family in Pakistan. CD-1 believed that RAZZAK's parents and one brother still lived in Pakistan. Department of Homeland Security advised that neither RAZZAK's wife nor his children were United States citizens.

28. RAZZAK advised the following: 1) RAZZAK has a Dubai based company Teleport LLC that has dealt in new cell phones since 2012; 2) the company had ten employees; 3) RAZZAK dealt with global customers of Teleport Trading to include customers in Hong Kong, U.A.E., Oman, Saudi Arabi, and Pakistan; and 4) RAZZAK earned $13,000 per month.

29. In July 2020, RAZZAK arrived in Chicago, Illinois from the United Arab Emirates (U.A.E.) on the B1 visa and currently holds that status. RAZZAK has applied for Legal Permanent

[6] The B1/B2 visa for RAZZAK was issued on January 30, 2020. RAZZAK's status is currently nonimmigrant overstay. RAZZAK entered as a B2, which is visitor for pleasure, and he is not allowed to work or enroll in a course for study. RAZZAK is prohibited from possessing a firearm because of his nonimmigrant overstay status.

Resident (LPR) status. As of March 14, 2022, that application was still pending.

RAZZAK's Travel

30. Department of Homeland Security provided the travel history related to RAZZAK and his Pakistan passport.

Name	DOB	Document	Status	Date (ET)	Conveyance	Cities
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	07/20/2020 15:20	EY 151 (AUH > ORD)	Abu Dabi, U.A.E to Chicago, IL
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	08/01/2019 19:55	EK 212 (IAH > DXB)	Houston, TX to Dubai, U.A.E.
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	06/28/2019 13:55	EK 215 (DXB > LAX)	Dubai, U.A.E. to Los Angeles, CA
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	05/28/2019 19:55	EK 212 (IAH > DXB)	Houston, TX to Dubai, U.A.E.
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	05/22/2019 16:50	EK 211 (DXB > IAH)	Dubai, U.A.E to Houston, TX
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	04/10/2019 22:55	EY 100 (JFK > AUH)	New York, NY to Abu Dabi, U.A.E.
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	03/26/2019 16:55	EY 101 (AUH > JFK)	Abu Dabi, U.A.E to New York, NY
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	08/04/2018 15:45	AF 639 (IAH > CDG)	Houston, TX to Paris, France
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	06/13/2018 12:50	AF 66 (CDG > LAX)	Paris, France to Los Angeles, CA
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	09/11/2015 16:45	EK 216 (LAX > DXB)	Los Angeles, CA to Dubai, U.A.E.
RAZZAK, Naeem	03/21/1971	P AD9864153 (PAK)	OBD	09/03/2015 11:40	EK 219 (DXB > MCO)	Dubai, U.A.E. to Orlando, Florida

31. RAZZAK also stated that he had traveled to the following countries in the last five years: Pakistan, Switzerland, Italy, Saudi Arabia, Turkey, Sri Lanka, Oman, Germany, Czech Republic, and Georgia.

Teleport Trading & Teleport International

32. In DHS records provided by RAZZAK, he lists the address for Teleport LLC as 101 Al Sabkha Building, Deira, U.A.E.

33. A review of e-mails for CD-2 in 2018 found nearly the same address listing in an e-mail from a Tele Port e-mail address as Office #101, Al Sabkha Building, Beside Gargash Centre Sabkha Bus Station, Deira, Dubai, U.A.E.

34. CD-1 provided information that RAZZAK has been in the cellphone business for approximately eight to nine years. RAZZAK has a business Teleport Trading LLC in Dubai that purchases and sells street stock. RAZZAK has laundered customers' money to other countries. RAZZAK charged customers based on the difficulty and risk associated with the money movement to the requested country, which generally averaged 2.5 percent to three percent of the transfer amount.

35. CD-1 stated that RAZZAK provided U.S. currency to Dosani (Always Pay More) for the purchase of street stock. A cash ledger for Dosani was obtained through the course of the investigation. A review found RAZZAK provided approximately $13,500,000 in U.S. currency to Dosani from October 2020 to August 2021.

36. In September 2020, Nargis RAZZAK formed Teleport International LLC in Texas.

37. In September 2020, RAZZAK opened a personal account, and RAZZAK and Nargis Naeem opened a corporate account for Teleport International, at Hanmi Bank. On the signature card for

the personal account, RAZZAK listed the address 201 Sawaira Excellency Bath Island Clifton, Karachi, Pakistan. Both accounts were closed in February 2022. Both Nargis Naeem and RAZZAK are listed on the signature card for the corporate account. Some of the account activity was as follows:

a. Deposits of $2,254,000:

i. $1,050,000 from U.S. based companies to include $50,000 from SCS Supply Chain (Saad Aziz).

ii. $901,000 from Dubai based companies to include $500,000 from Teleport Trading LLC (five deposits from November 2020 to April 2021).

iii. $146,000 from Hong Kong, specifically Hanggroup Telecom, a known importer of street stock and an IMEI unlocker.

iv. $135,000 incoming transfer from his wife Nargis Naeem's Bank of America account.

v. $21,000 of cash deposits

b. Disbursements:

i. $1,654,000 to companies for what appears to be electronics purchases.

ii. $404,000 to the purchase of a property under his children's names and which has since been sold.

38. The FBI does not have foreign accounts for Teleport Trading identified, as the wire transfers to RJ Telecom, M7 Group, and SCS Supply chain typically came through Dubai logistical companies like Action Logistics, or through companies

tied to Fakhruddin Gheewalla, a Houston based partner to RAZZAK, and described further below.

39. A review of telephone analysis, interviews, discussions with FBI personnel, and other investigative techniques found RAZZAK is associated with a Pakistani organized crime syndicate known as D-Company, led by Dawood Ibrahim[7], through device trafficking and money laundering.

RJ Telecom

40. A preliminary review of an e-mail account used by Arsalan Bhangda found e-mails between Bhangda and RAZZAK, from 2016 to 2018. Many of these e-mails were related to Bhangda sending invoices for the sale of devices to RAZZAK d/b/a Teleport Trading. CD-1 advised that nearly all stock sent to RAZZAK was street stock.

41. On or about April 16, 2016, RJ Telecom sent 12 Sprint (carrier locked) IMEIs to RAZZAK. The IMEIs were sent to RAZZAK to be unlocked. T-Mobile confirmed five of the devices were stolen and three devices were never activated or Boost devices. The value of the devices was over $4,000.

42. From 2017 to 2018, there were approximately 20 invoices or payments for devices sent from Bhangda to RAZZAK. Based on amounts associated with the invoices, the total dollar amount of devices sold from Bhangda to RAZZAK was approximately $3,519,169. For three of the invoices, IMEIs associated with the devices were located (referenced below). The invoices or

[7] Dawood Ibrahim has been designated as a global terrorist by the Department of Treasury.

payments were associated with FedEx shipments. Numerous shipments were sent by Bhangda from a FedEx station located at 1200 Capital Avenue, Plano, Texas, a location within the Eastern District of Texas, to various Dubai logistical companies in Dubai, U.A.E.

43. On or about March 21, 2018, an e-mail was sent from Bhangda to multiple parties, including RAZZAK. The e-mail asked APL Global Logistics, a Dubai logistical company, to release the shipment for Naeem RAZZAK from Teleport Trading LLC. It also listed three FedEx shipping tracking numbers. The invoice 03202018 listed various models of Apple cell phones (200 units) for a total of $185,530. Days later, Bhangda sent an e-mail to RAZZAK that had an attachment filename of "3 20 2018 IMEIS". The spreadsheet listed 200 IMEIs.

44. On or about May 8, 2018, an e-mail was sent from Bhangda to multiple parties, including RAZZAK. The e-mail asked APL Global Logistics, a Dubai logistical company, to release the 3 pcs for Naeem RAZZAK from Teleport Trading LLC. It also listed a FedEx shipping tracking number 772186167444 (the shipment was sent from 1200 Capital Avenue, Plano, Texas). The invoice 0508018 listed various models of Apple cell phones and iPads (192 units) for a total of $167,682. Bhangda later sent an e-mail to RAZZAK that had an attachment filename of "5 08 2018". The spreadsheet listed 192 IMEIs.

45. On or about May 12, 2018, an e-mail was sent from Bhangda to multiple parties, including RAZZAK. The e-mail asked APL Global Logistics, a Dubai logistical company, to release the

2 pcs for Naeem RAZZAK from Teleport Trading LLC. It also listed a FedEx shipping tracking number 772208491879 (the shipment was sent from 1200 Capital Avenue, Plano, Texas). The invoice 051018 listed various models of Apple cell phones (140 units) for a total of $142,225. Bhangda later sent an e-mail to RAZZAK that had an attachment filename of "5 10 2018". The spreadsheet had the invoice 051018 and a tab for that listed 140 IMEIs.

46. The IMEIs associated with the invoices in March and May 2018, referenced above, were sent to AT&T. Of the approximate 532 IMEIs related to cell phones, 304 devices resolved to a category of fraud or indicative of fraud[8], resulting in an approximate dollar loss of $309,000, 165 devices had no records at AT&T (likely another carrier), 49 were prepaid devices with no further information, five were classified as "legitimate," and two devices were under review. Seven devices were listed as "blacklisted" and were associated with other carriers (non-AT&T).

M7 Group

47. A preliminary review of an e-mail account for Awais Ahmed found e-mails between Ahmed and RAZZAK related to device trafficking. Ahmed sent street stock to RAZZAK's company in Dubai, U.A.E.

48. In 2018 and 2019, M7 Group sold over $1,400,000 in street stock to Tele Port Trading LLC in Dubai, U.A.E. There

[8] The classifications were fraud, various non-pay categories, or other categories indicative of fraud.

were numerous WhatsApp and e-mail communications with RAZZAK to conduct the below and other transactions. Included within these sales are the following shipments:

49. On or about December 26, 2018, a FedEx shipment of street stock from M7 Group consisting of approximately 91 stolen Apple iPhones was received by Action Logistics in Dubai, U.A.E. The stock was released to Naeem RAZZAK d/b/a Tele Port Trading.

50. On or about December 27, 2018, M7 Group received a wire transfer for approximately $62,815 related to the 91 stolen Apple iPhones.

51. On or about January 10, 2019, a FedEx shipment of street stock from M7 Group consisting of approximately 61 stolen Apple iPhones was received by Action Logistics in Dubai, U.A.E. The stock was released to Naeem RAZZAK d/b/a Tele port Trading.

52. On or about January 16, 2019, M7 Group received a wire transfer from Action Logistics in the amount of $47,393 that included a partial payment for the 61 stolen Apple iPhones.

53. CD-2 advised that devices sold to RAZZAK were street stock, or devices that were stolen.

54. CD-2 advised that RAZZAK offered cash as a form payment on multiple occasions, but CD-2 never accepted the offer.

SCS Supply Chain

55. From approximately 2018 to 2020, SCS Supply Chain sold street stock to **Teleport International**. Saad Aziz communicated with RAZZAK via WhatsApp. CD-3 advised street stock was sold to RAZZAK.

56. On or about December 3, 2018, SCS Supply Chain sold approximately $103,000 in street stock cell phones to **Teleport International.**

DEA, HONG KONG, AND MONEY LAUNDERING

57. During the investigation, LCD One Technology (LCD), Haowei and Hanggroup Telecom were identified as Hong Kong based companies purchasing and importing stolen devices from wholesalers like Dosani (Always Pay More) and RAZZAK (Teleport). They are also involved in money laundering activities. Each company uses cash from various sources to pay United States based wholesalers for the exported stolen devices to their companies. Those sources include drug proceeds, gambling proceeds, and business proceeds seeking tax avoidance.

58. These Hong Kong companies have been identified through cooperating defendant statements, bank statements, shipping records, or chat messages as international purchasers and importers of consumer electronic devices from United States based wholesalers.

59. CD-1 advised that LCD is currently one of the largest Hong Kong companies to purchase and import stolen cell phones from United States wholesalers. CD-1 further provided information that LCD uses cash rebates with wholesalers. Essentially, if wholesalers accept payment in U.S. currency versus wire transfer, they are provided a cash rebate anywhere from three to seven percent of the sale amount. CD-1 further advised that the cash provided to the wholesalers is "dirty" money that is being laundered through the international sale of

stolen consumer devices. The sources of laundered money can range from cash businesses seeking tax avoidance of their proceeds, which commonly include businesses involved in jewelry, game slots, and gas stations to drug proceeds.

60. In February 2022, CD-1 communicated via WhatsApp chats with WhatsApp number 85261942922 with Lai Yuk Hang (Hank). Hang told the CD that LC (LCD) was able to purchase at high prices because they were able to offer anywhere from four to six percent cash rebates. Hang further told the CD that LCD was able to offer these cash rebates because the "cash directly from mexican deliver," which CD-1 advised was Hang's way of saying the cash used to pay wholesalers was coming from drug proceeds in the form of cash. Hang advised LCD's 6% cashback used to payout suppliers was associated with Mexican drug money.

DEA and Drug Proceeds

61. A Drug Enforcement Agency ("DEA") investigation identified the WhatsApp number 8613040832203, believed to be used by a female known as Crystal. Crystal works for LCD. The investigation found through deconfliction that the DEA had initiated a pen register on Crystal's WhatsApp number. CD-1 has received WhatsApp messages from Crystal who is advertising the purchase of devices for cash.

62. On or about February 18, 2022, a pen register and trap and trace court order was signed in the Eastern District of Texas for telephone number 757-344-8684, associated with Dosani.

63. A pen register analysis associated with Dosani's telephone number found approximately 270 contacts between Dosani and Crystal (LCD) from January 25, 2022 to March 30, 2022.

64. A pen register analysis for Crystal's WhatsApp found Jesani's telephone number had approximately 119 contacts between Jesani and Crystal (LCD) from January 25, 2022 to March 3, 2022.

65. CD-1 advised that while he/she was conducting business in Houston, Texas, Dosani operated his business in large quantities of twenty-dollar bills. CD-1 stated it is common knowledge that drug proceeds are the source of cash when a wholesaler is using large quantities of $20 bills.

66. A pen register analysis for Crystal's WhatsApp found approximately 607 contacts between RAZZAK and Crystal (LCD) from February 9, 2022 to February 27, 2022.

Controlled IMEI Submissions – Shaikh and RAZZAK – March 2022

67. In March 2022, CD-1 conducted three controlled transactions involving locked IMEIs with RAZZAK. CD-1 brokered the purchase of approximately 546 AT&T locked IMEIs on three different occasions from RAZZAK for the purpose of unlocking the IMEIs. Under the direction of the FBI, CD-1 received invoices from RAZZAK via WhatsApp that listed the IMEIs and then submitted the IMEIs to Shaikh (Unlockdon). The FBI sent the list of IMEIs to AT&T to track how the IMEIs went through the unlocking process. AT&T found AT&T found that these IMEIs were illegally unlocked and the approximate loss of the devices was $611,000.

68. On or about March 17, 2022, a WhatsApp pen registers were obtained for Shaikh's cellular phone number 512-785-0444.

69. A review of the WhatsApp pen register data revealed approximately 336 contacts with RAZZAK from April 7, 2022 to May 8, 2022:

70. The WhatsApp pen register data shows Shaikh's continued contact with RAZZAK, who is actively involved in collecting street stock and unlocking carrier locked IMEIs. CD-1 advised that RAZZAK has continued to use Shaikh d/b/a Unlockdon Distributor to unlock IMEIs in 2022.

Controlled Money Pickup – May 6, 2022

71. On or about May 6, 2022, CD-1 conducted a money pickup from a Dallas, Texas based individual (Dallas IND) for $71,000. RAZZAK coordinated the money pickup with CD-1 and put CD-1 into contact with the Dallas IND to arrange the money pickup. After meeting with the Dallas IND and completing the transaction, CD-1 confirmed with RAZZAK that money had been picked up. Agents counted the money and approximately half the money was in denominations of $20s.

WhatsApp Pen Register – Naeem RAZZAK

72. On or about March 17, 2022, a WhatsApp pen register was obtained for a cellular phone number used by RAZZAK. An analysis of the pen register data from March 21, 2022 through May 10, 2022 showed the following:

73. Fakhruddin Gheewalla a.k.a. Dean: 804 contacts. The investigation identified Gheewalla as a partner of RAZZAK's who resides in Houston. CD-1 advised that Dean collects street stock

for RAZZAK in the Houston area. Two companies registered to Gheewalla are used to conduct financial payments to other wholesalers.

74. Kevin: 152 contacts. The investigation identified Kevin as an IMEI unlocker based in India, much like Shaikh.

75. The review identified numerous India, Pakistan, or U.A.E. based numbers that RAZZAK is in communication with. RAZZAK is also in contact with numerous United States based numbers.

Investigative Experience with Wholesalers and Records

76. Based on my experience with this investigation, I know that wholesalers like RAZZAK commonly use WhatsApp messaging, or other messaging services, on their cell phones to communicate and conduct device trafficking and money laundering activities. The WhatsApp messaging is a common way to send lists of IMEIs, invoices, voice recorded messages, and coordinate transactions. E-mail accounts are often associated with their cell phones thus storing e-mails related to device trafficking, i.e. coordinate the release of street stock overseas, send/receive invoices or ledgers, or other business records. Wholesalers and device traffickers often send screenshots, images, or videos of meet locations, "token bills"[9], cell phone boxes, IMEIs, large quantities of street stock, or other business records. Financial

[9] Token bills are used during money laundering activities. A photograph is taken of one bill of U.S. currency by one party and it is sent through the coordinator (like RAZZAK) to the third party. During the meet, the token bill is used to authenticate the transaction.

records are also sent through WhatsApp to include screenshots or photographs of bank transfers/activities.

77. The content of WhatsApp messages cannot be obtained through a third party and must be extracted from a cell phone or other device storing the WhatsApp messages and content. Therefore, the seizure of RAZZAK's cell phones is essential to capturing business communications and records related to device trafficking and money laundering activities.

78. Wholesalers are known to use laptops, tablets, and other devices to create, store, and transmit business records, or backup their cell phone data.

79. In this investigation, numerous search warrants have been conducted at the residences of wholesalers. The search warrants resulted in the seizure of personal cell phones used by wholesalers that contained WhatsApp messages with other wholesalers containing the above referenced business records. The investigation found wholesalers often maintain chats with other wholesalers or traffickers that date back several years. Other messages were also found with device traffickers, unlockers like Shaikh d/b/a Unlockdon, and other individuals involved in device trafficking. The search warrants also seized large amounts of U.S. currency and firearms.

SUBJECT PREMISES

80. A public records search found the current address for RAZZAK's wife Nargis Naeem and three relatives, who appear to be

children—Hunain, Zain and Zoya--was the SUBJECT PREMISES[10]. A 2017 Mercedes with license plate number NBD4334 is registered to Hunain Naeem at the SUBJECT PREMISES. A white Tesla with license plate number PNW-5265 is registered to Zain Naeem at the SUBJECT PREMISES.

81. On May 5, 2022, at 5:26 a.m., the FBI initiated physical surveillance at the SUBJECT PREMISES. Surveillance observed the white Tesla with license plate number PNW-5265 ("Tesla") at the SUBJECT PREMISES. At 8:20 a.m., surveillance observed RAZZAK depart the residence in the Tesla and drive a school-aged female to a high school. At 8:42 a.m., RAZZAK returned to the residence in the Tesla. A photograph was taken of RAZZAK at the SUBJECT PREMISES. CD-1 and CD-2 positively confirmed RAZZAK as the individual in the photograph.

82. Because the SUBJECT PREMISES appears to be RAZZAK's primary residence, I believe there is probable cause to believe that evidence of the Subject Offenses will be found at the SUBJECT PREMISES, including on any digital devices belonging to and/or used by RAZZAK that are likely to be found at the SUBJECT PREMISES.

SEARCH PROCEDURES RELATED TO PRIVILEGED COMMUNICATIONS

83. Naeem RAZZAK is involved with a registered business. With this, there is a possibility that privileged communications may be found at the SUBJECT PREMISES. Agents assigned to the search of the SUBJECT PREMISES are instructed to stop searching

[10] A search for RAZZAK through public databases found no results.

and not to read any document that appears to be potentially privileged, and to immediately contact the AUSA specifically assigned to review potentially privileged documents. Agents also anticipate seizing computers and other electronic storage devices. These devices could contain e-mails and other communications that could contain privileged communications. Where the likelihood of privileged communications exists, the electronic devices and storage mediums will be seized, forensically imaged off-site, and reviewed by a taint team prior to an investigative team review.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[11]

84. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur

[11] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain

"booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

85. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

86. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress RAZZAK's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of RAZZAK's face

with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

87. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

88. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found at the SUBJECT PREMISES, as described in Attachment A.

Chris Doering, Special Agent
Federal Bureau of
Investigation

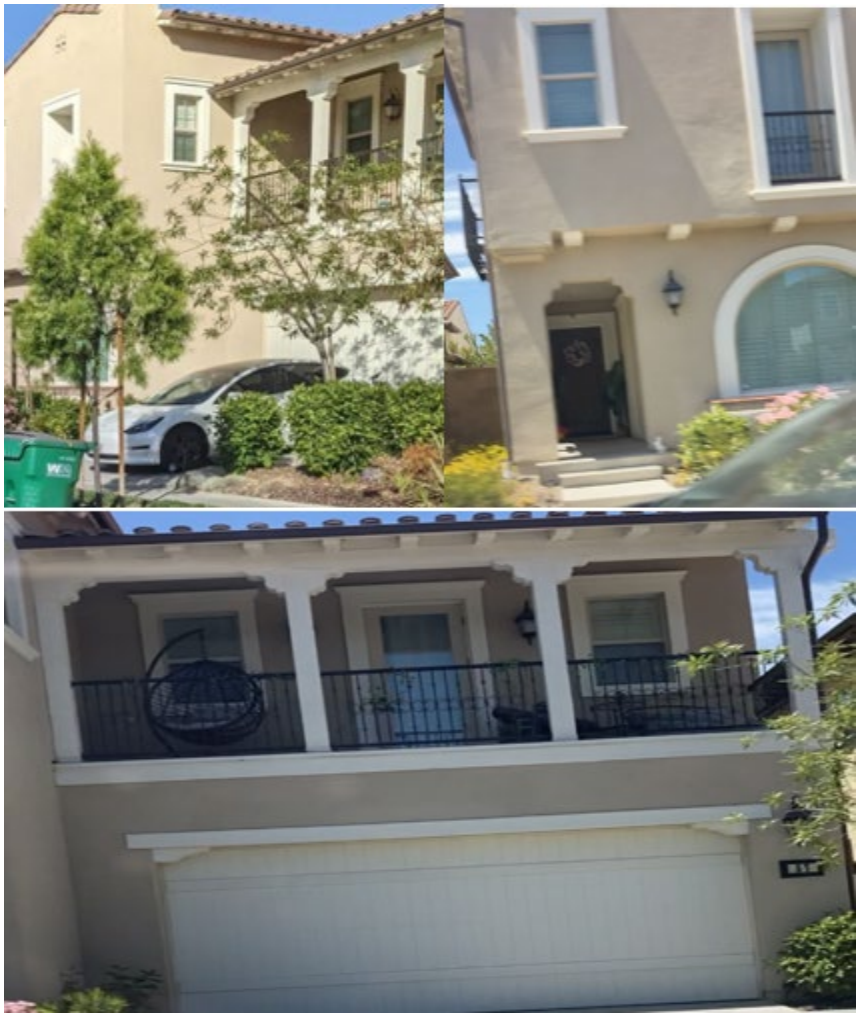
Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this __ day of May, 2022.

HONORABLE AUTUMN D. SPAETH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The single-family house located at 57 Gainsboro, Irvine, California 92620. The premises is described as a two-story residence with stucco construction and a red tile roof. The front door is to the left of the garage when facing the house. The numbers "57" are affixed to the right side of the two car garage. Photographs of the premises are below to include the numbers "57" to the right of the garage.



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1028 (fraud in connection with identification documents), 1028A (aggravated identity theft), 18 U.S.C. § 1341 (wire fraud), 18 U.S.C. § 1343 (mail fraud), 18 U.S.C. § 1956 (laundering of monetary instruments), 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity), 18 U.S.C. §2314 (interstate or foreign transportation of stolen property), 21 U.S.C. §841 (controlled substances), and 21 U.S.C. §846 (attempt and conspiracy) (the "Subject Offenses"), occurring after January 1, 2016, namely:

a. Computers and storage media, including the cellular phones for Naeem RAZZAK.

b. Internet-connected data storage or processing services, including Dropbox, Google, Apple, Adobe Sign, or DocuSign account information; data backups; passwords; connection logs; website cache; and software—and the associated data—designed to facilitate remote data storage or processing.

c. All virtual currency and related records of any kind, to include: any and all representations of virtual currency public keys or addresses, whether in electronic or physical format; any and all representations of virtual currency private keys, whether in electronic or physical format; any and all representations of virtual currency wallets or their

constitutive parts, whether in electronic or physical format, to include "root keys" which may be used to regenerate a wallet; and PGP keys and/or encryption passwords or keys of any kind;

d. Records evidencing occupancy or ownership of the subject premises described in Attachment A, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

e. Any and all notes, documents, records, tax returns, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the Subject Offenses.

f. Cell phones, cell phone boxes, watches, air buds, computers, tablets, and other electronic devices that match the description, either physically, by serial number or IMEI, consistent with obtaining new devices through illicit means.

g. Any electronic records, documents, or photographs of IMEI or serial numbers (bar codes) of cellular devices, boxes, watches, air buds, tablets, computers, or accessories of the aforementioned items, shipping labels, shipping receipts, return labels, return receipts, or any other evidence associated with the movement of stolen cell phones, watches, air buds, computers, tablets, or other items consistent with the conduct of obtaining new devices through illicit means.

h. Electronic or paper documents related to bank records, invoices, business correspondence to include electronic and written mail, and other business records that reflect business operations to include accounts payable, accounts receivable, daily transactions, customer databases, ledgers, inventory, and any other business function involved in the purchase or sale of electronic devices.

i. U.S. currency, electronics, valuables and safes designed to store U.S. currency, electronics, valuables, and other items.

j. Firearms and ammunition

k. Devices, documents, or information related to payments, finances, and digital or electronic currency.

l. Digital recorders and associated storage mediums used to record audio and/or visual surveillance footage.

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar

facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items

to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Naeem Ninit RAZZAK's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Naeem Ninit RAZZAK's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.