

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

IN RE: CRIMINAL COMPLAINT

)
)
)

Misc. No. 1:20-MJ-09 LDA

MOTION TO SEAL

The Government moves to have this Motion to Seal, along with the attached Criminal Complaint, Affidavit, Cover Sheet and Arrest Warrant, sealed until further Order of this Court. Disclosures may impede investigation and effectuation of an arrest warrant. The Government is permitted to share the attached Criminal Complaint, Affidavit, Cover Sheet and Arrest Warrant with law enforcements agents, as necessary for the effectuation of arrest and with the Court and probation officials in any arresting district, as necessary for initial appearance and detention proceedings.

Respectfully submitted,
UNITED STATES OF AMERICA

By its attorneys,

AARON L. WEISMAN
United States Attorney



MILIND S. SHAH
Assistant United States Attorney
U.S. Attorney's Office
50 Kennedy Plaza, 8th Floor
Providence, RI 02903
(401) 709-5000
(401) 709-5001 (fax)

FILED
JAN 23 2020
U.S. DISTRICT COURT
DISTRICT OF RHODE ISLAND

SO ORDERED:



LINCOLN D. ALMOND
UNITED STATES MAGISTRATE JUDGE

1/23/2020

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

United States of America
v.

Case No.

1:20-MJ-09 LDA

Abrar Anjum (YOB: 1986)

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

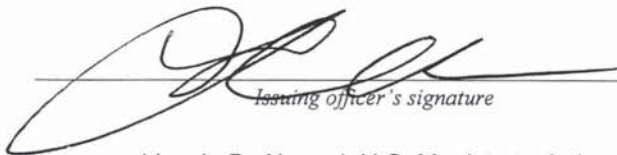
YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) Abrar Anjum,
who is accused of an offense or violation based on the following document filed with the court:

- Indictment Superseding Indictment Information Superseding Information Complaint
- Probation Violation Petition Supervised Release Violation Petition Violation Notice Order of the Court

This offense is briefly described as follows:

Wire fraud: 18 U.S.C. §§ 1343,
Conspiracy to commit wire fraud: 18 U.S.C. § 1349, and
Telemarketing or email marketing fraud: 18 U.S.C. § 2326.

Date: 1/23/2020


Issuing officer's signature

City and state: Providence, RI

Lincoln D. Almond, U.S. Magistrate Judge
Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____

Arresting officer's signature

Printed name and title

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Rhode Island

United States of America

v.

Abrar Anjum

Defendant(s)

Case No. 1:20-MJ-09 LDA

CRIMINAL COMPLAINT

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

On or about the date(s) of May, 2019 in the county of in the District of Rhode Island, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 1343; 18 U.S.C. § 1349; and 18 U.S.C. § 2326. Offense descriptions include Wire fraud; Conspiracy to commit wire fraud; and Telemarketing or email marketing fraud.

This criminal complaint is based on these facts:

See the attached Affidavit of Special Agent, Craig A. Graham, of the Federal Bureau of Investigation ("FBI").

Continued on the attached sheet.

Signature of Special Agent, Craig A. Graham ~ FBI. Printed name and title.

Sworn to before me and signed in my presence.

Date: 1/23/2020

Signature of Lincoln D. Almond, U.S. Magistrate Judge. Printed name and title.

City and state: Providence, Rhode Island

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: INFORMATION INDICTMENT COMPLAINT

CASE NO. _____

Matter Sealed: Juvenile Other than Juvenile

Pre-Indictment Plea Superseding Defendant Added
 Indictment Charges/Counts Added
 Information

Name of District Court, and/or Judge/Magistrate Location (City)

UNITED STATES DISTRICT COURT RHODE ISLAND
 DISTRICT OF RHODE ISLAND Divisional Office

Name and Office of Person Furnishing Information on THIS FORM AARON WEISMAN
 U.S. Atty Other U.S. Agency
 Phone No. (401) 709-5000

Name of Asst. U.S. Attorney (if assigned) Milind M. Shah

USA vs. 1:20-MJ-09 LDA

Defendant: Abrar Anjum

Address: Unknown India

Interpreter Required Dialect: _____

Birth Date 7/23/1986 Male Alien
 Female (if applicable)

Social Security Number _____

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)
Craig A. Graham, Special Agent ~ FBI

person is awaiting trial in another Federal or State Court (give name of court)

this person/proceeding transferred from another district per (circle one) FRCrP 20, 21 or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of:

U.S. Atty Defense

this prosecution relates to a pending case involving this same defendant. (Notice of Related Case must still be filed with the Clerk.)

prior proceedings or appearance(s) before U.S. Magistrate Judge regarding this defendant were recorded under

SHOW DOCKET NO.

MAG. JUDGE CASE NO.

Place of offense RHODE ISLAND County

DEFENDANT

Issue: Warrant Summons

Location Status:

Arrest Date _____ or Date Transferred to Federal Custody _____

Currently in Federal Custody

Currently in State Custody

Writ Required

Currently on bond

Fugitive

Defense Counsel (if any): _____

FPD CJA RET'D

Appointed on Target Letter

This report amends AO 257 previously submitted

OFFENSE CHARGED - U.S.C. CITATION - STATUTORY MAXIMUM PENALTIES - ADDITIONAL INFORMATION OR COMMENTS

Total # of Counts 3

Set	Title & Section/Offense Level (Petty = 1 / Misdemeanor = 3 / Felony = 4)	Description of Offense Charged	Felony/Misd.
	See Attachment		<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
		Estimated Trial Days: 5	<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor

**ATTACHMENT TO DEFENDANT COMPLAINT RELATIVE TO A CRIMINAL
ACTION - IN U.S. DISTRICT COURT**

DEFENDANT: Abrar Anjum

COUNT I: 18 U.S.C. § 1343: Wire Fraud - Felony.

MAXIMUM PENALTIES: Imprisonment: 20 years; Supervised release: 3 years; Fine: \$250,000; and Special assessment: \$100.

COUNT II: 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud - Felony.

MAXIMUM PENALTIES: Imprisonment: 20 years; Supervised release: 3 years; Fine: \$250,000; and Special assessment: \$100.

COUNT III: 18 U.S.C. § 2326: Telemarketing or email marketing fraud - Felony.

MAXIMUM PENALTIES: Imprisonment: 5 years; Supervised release: 3 years; Fine: \$250,000; and Special assessment: \$100.

AFFIDAVIT OF FBI SPECIAL AGENT CRAIG A. GRAHAM

I. INTRODUCTION

I, Craig A. Graham, having been duly sworn, state as follows:

1. Since 2010, I have been a special agent with the Federal Bureau of Investigation ("FBI"). Early in my career, I focused on counterintelligence investigation. Starting in 2015, my responsibilities expanded to include the investigation of wire fraud, mail fraud, and other white collar offenses, and since July 2018, when I was assigned to the FBI's Providence Resident Agency, I have focused primarily on white collar investigation. I have experience in the investigation of telemarketing fraud, and through that work have gained a familiarity with computer or smartphone based communication applications such as WhatsApp, Snapchat, and Skype.

2. I submit this affidavit in support of criminal complaints and arrest warrants charging ██████████ (born ██████████ ██████████ ("██████████"), ██████████ (born ██████████ ██████████ ("██████████")), and Abrar Anjum (born July 1986) ("Anjum"), all Indian residents, with the following offenses:

- (i) wire fraud, in violation of 18 U.S.C. §§ 1343,
- (ii) conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and
- (iii) telemarketing or email marketing fraud, in violation of 18 U.S.C. § 2326.

3. The information in this affidavit comes from my personal observations and investigation, my training and experience, other law enforcement agents, an FBI source of information, and other sources as specified in the body of this affidavit. This affidavit is intended to show that there is sufficient cause for the requested warrant and does not set forth all of my knowledge about this matter or investigation.

4. Based on my investigation, I believe that there is probable cause to believe that

a. ██████████ and others conspired to and did defraud or attempt to defraud multiple victims by misleading them into believing that their computers had been attacked by

malware, by obtaining remote access to the victims computers, and by extracting money from the victims;

b. [REDACTED] and others conspired to and did defraud or attempt to defraud multiple victims by misleading them into believing that their computers had been attacked by malware, by obtaining remote access to the victims' computers, and by extracting money from the victims;

c. [REDACTED] Anjum, and [REDACTED] and others conspired to and did defraud or attempt to defraud multiple victims by misleading them into believing that their computers had been attacked by malware, by obtaining remote access to the victims' computers, and by using that remote access or some other means to extract money from the victims' accounts;

d. [REDACTED], Abrar, and [REDACTED] on one occasion conspired to and did defraud or attempt to defraud a victim, PH, by misleading her into believing that her computer had been attacked by malware, by obtaining remote access to her computer, and by using that remote access or some other means to extract money from her accounts.

II. INVESTIGATION

Summary of Investigation

5. The investigation described below involved two phases. The first involved a review of records and recordings that indicated that [REDACTED] and [REDACTED] engaged in tech support fraud with others.

6. The second phase of this investigation involved using a cooperating informant who at the FBI's direction offered to provide [REDACTED] a bank account through which to funnel money obtained from victims. In communications with [REDACTED] that were roughly contemporaneous to money transfers to the account, the informant was able to obtain evidence of how the money had been obtained from the victims. Those communications also revealed that [REDACTED] and Anjum were acting in concert with or assisting [REDACTED] in obtaining that victim money, and ultimately the informant was able to communicate directly with both [REDACTED] and Anjum and further establish the nature of their actions.

Initial Information Provided by Informant

7. In May 2019, the FBI arrested a male in the United States on charges that included conspiracy to defraud and multiple instances of wire fraud and bank fraud. The male shortly after his arrest began cooperating with the FBI in the hope of receiving leniency in the disposition of the pending charges. The male is hereinafter referred to as the "Informant."

8. The Informant, an Indian citizen and resident, has not previously been convicted of any crimes in the United States. The FBI is not aware of whether the Cooperator has ever been convicted of crimes in India, but the Cooperator reports that he has never been jailed in India.

9. In May 2019, after his arrest, the Informant told me that an acquaintance who resided in India, [REDACTED] was involved in telemarketing scams that defrauded people residing in the United States. The Informant referred to these specific types of scams or schemes as "tech support fraud."

10. The Informant described himself and [REDACTED] as brokers engaged in tech support fraud. He explained that they bought telephone call traffic, specifically calls placed by people who, based on advertising that they had seen on their computers, believed that their computers had been or were being attacked by malware. The Informant explained that such advertising was not based on any information indicating that the callers' computers had malware problems and also explained that the advertising was often targeted toward those likely to lack computer or software expertise.

11. The Informant explained that he had sold such call traffic to [REDACTED] and had per [REDACTED] instructions directed that call traffic to call center operators who solicited the callers to purchase purported computer assistance services.

12. In December 2019, the Informant told me that another acquaintance who resided in India, [REDACTED], was also separately involved in tech support fraud. The Informant also told me [REDACTED] used to work at a call center and then later started his own call center in India and began buying calls from the Informant.

13. The Informant described the role of “publishers” in the tech support fraud. He explained that publishers created various forms of online advertising, including pop-up ads,¹ designed to mislead viewers into believing that malicious software or malware was attacking their computers. For example, the Informant suggested that a publisher could place ads on Facebook offering travel agent services for retirees interested in cruise vacations. A viewer who clicked on the ads would be directed to a page that would state that the viewer’s computer had been infected by a virus or was being attacked by malware and advise the viewer to call a particular telephone number.

14. The Informant explained that brokers could purchase from a publisher the calls generated by such advertising. Using call routing technologies, the publisher would route incoming calls to the broker. The broker in turn could sell the calls by re-routing them directly to call centers or to other brokers who ultimately had the calls routed to call centers.

15. The Informant explained that call centers, specifically those involved in telemarketing fraud, were facilities designed to accept incoming calls and extract money from the callers. Typically, call centers were comprised of multiple operators, each of whom would be familiar with the sort of advertising that had been seen by the callers. The operators would accept the calls generated by the publishers’ advertising and seek to extract money from the callers by purporting to provide computer protection services.

16. The Informant said that prior to his arrest by FBI and prior to becoming a source of information for the FBI, he had routed call traffic to [REDACTED] and [REDACTED] knowing that the callers would be defrauded or that there would be attempts to defraud the callers, and that call traffic routed by the Informant to [REDACTED] and separately to [REDACTED] included many calls from U.S. telephone numbers. The Informant also explained that the informant sold and directed call

¹ The Cooperator explained, and I know from my training and experience, that pop-up ads are a particular form of online advertising. While one is browsing internet sites, a separate browser window pops up, and that new window must be closed or disabled in order to continue browsing activities.

traffic to buyers, including [REDACTED] and other call centers by utilizing at least two, third party call-tracking and call routing software platforms. For convenience, I refer to these call routing software platforms as "CRS1" and "CRS2."

Identification of [REDACTED]

17. The Informant identified a particular WhatsApp account² as belonging to [REDACTED]. The telephone number associated with that account was [REDACTED], an Indian telephone number. The account's profile picture shows an individual who the Informant identified as [REDACTED]. An enlarged copy of the profile picture is attached as Exhibit 1.

18. The Informant also identified a particular Skype account³ as belonging to [REDACTED]. That account listed the vanity name, a user selected name, "[REDACTED]" and a Skype account name of "techs247." The account also indicated that the account holder's date of birth was "11/26."

19. Visa application records obtained from the Department of State show that [REDACTED] visa application listed a birthdate of November 26, 1987 and a home telephone number of "[REDACTED]," the same number that is associated with the WhatsApp account identified by the Informant. The visa application included a photograph of the applicant, which the Informant identified as a photograph of [REDACTED]. The visa photograph is attached as Exhibit 2, and the person pictured in it is visually similar to the male pictured in [REDACTED] WhatsApp profile photograph, Exhibit 1.

² WhatsApp is a communications applications for mobile devices and desktop computers that allows users to send and receive text and voice messages, make and receive voice and video calls, and share images, documents, user location, and other media. All users of the application must have an account or access to an account. In the account creation process, users provide a cellular mobile number. WhatsApp is owned by Facebook, Inc.

³ Skype is a communications application for mobile devices and desktop computers that allows users to send and receive text and voice messages, make and receive voice and video calls, and share images and other media. All users of the application must have an account or access to an account. Skype is owned by Microsoft Corporation.

Identification of Mishra

20. The Informant identified a particular WhatsApp account as belonging to [REDACTED]. The telephone number associated with that account was [REDACTED], an Indian telephone number. The account's profile picture shows an individual who the Informant identified as [REDACTED]. An enlarged copy of the profile picture is attached as Exhibit 3.

21. The Informant also identified a particular Skype account as belonging to [REDACTED]. The account listed the vanity name "[REDACTED]" and Skype account name "[REDACTED]." The account listed the holder's location as "new delhi, IN." (The account listed the holder's birthdate as "11/7.") On the Skype profile page, there is account holder entered text that reads "Zelle and Wire Accounts available."

22. Visa application records obtained from the Department of State show that [REDACTED]'s visa application listed a home telephone number of "[REDACTED]," the same number that is associated with the WhatsApp account identified by the Informant. (The "91" that begins the number sequence in the WhatsApp account is the country code for India.) The visa application included a photograph of the applicant, which the Informant identified as a photograph of [REDACTED]. (The application listed [REDACTED]'s date of birth as [REDACTED]) The visa photograph is attached as Exhibit 4, and the person pictured in it is visually similar to the male pictured in [REDACTED]'s WhatsApp profile photograph, Exhibit 3.

23. On January 14, 2020, [REDACTED] arrived at the Miami International Airport. A photograph of [REDACTED] was taken upon his entry into the United States. That photograph is included as Exhibit 5 and is visually similar to both [REDACTED]'s Visa application photo and his WhatsApp profile picture, respectively Exhibits 3 and 4.

Identification of Anjum

24. The Informant communicated with Anjum through two separate WhatsApp accounts, one of which was associated with U.S. telephone number [REDACTED] and the other was associated with Indian telephone number [REDACTED]. An enlarged copy of the profile picture for each account is attached as Exhibit 6.

25. Visa application records obtained from the Department of State show that Anjum's visa application listed a date of birth of July 23, 1986 and a home telephone number of "[REDACTED]," the same number associated with one of the aforementioned WhatsApp accounts. The visa application included a photograph of the applicant, and that photograph is attached as Exhibit 7. The person pictured in it is visually similar to the person pictured in Anjum's WhatsApp profile photographs.

*Call Traffic Sold to [REDACTED] Using CRS1 and
Call Center Operators' Attempts to Scam the Callers*

26. A review of records, including recorded calls, indicates that the Informant directed call traffic to a telephone number associated with [REDACTED] and that calls forwarded to that number resulted in the call recipients attempting to exact money from the callers by posing as providers of computer protection services. Efforts were made to suggest that Microsoft was involved in detecting viruses on the callers' computers or that the call recipients were affiliated with Microsoft. However, Microsoft policy makes plain that it would not have been involved in those purported instances of virus detection and was not affiliated with the call recipients.

27. The Informant provided access to his current CRS1 account, and from the account records, I was able to isolate, as further described below, calls that had been directed from the Informant to [REDACTED] and was able to determine that the Informant sold those calls to [REDACTED]. CRS1 has multiple features to aid account holders in managing and tracking calls which are routed through the account. These features included the ability to create a "Target" name for the person to whom the Informant was selling call traffic. CRS1 then monitored and tracked, among other information, how many calls were sent from the Informant to the buyer, whether the call was connected, and whether or not the call was a duplicate call. The Informant provided agents with a user ID and password for his CRS1 account. The user ID was in the form of the Informant's email which had previously been identified and associated with the Informant independently.

28. According to CRS1, in 2019, the Informant sold approximately eight calls to [REDACTED] on January 29, 2019, and approximately five calls on February 4, 2019. Within the Informant's CRS1 account, the Informant identified the Target name "[REDACTED] [REDACTED] [REDACTED]" The Informant said that that he assigned that Target name to [REDACTED] using [REDACTED] first name. The Informant explained that by setting up a Target name for [REDACTED] the Informant could track the number of calls he sold to [REDACTED]

29. FBI agents reviewed CRS1 records for all thirteen calls, each from a unique telephone number, that were sold by the Informant to [REDACTED] Twelve of the thirteen calls were dialed from U.S. telephone numbers; one call was dialed from a Canadian number. CRS1 generally preserves recordings of the sold calls. Agents were able to locate and review recordings for ten of the calls made from U.S. telephone numbers. Review of those calls revealed the following:

- In conversation with call center operators, the ten callers each said that they had received computer error messages that appeared to have locked or frozen their computers and that the messages indicated that their computers had been infected by a virus.
- In two calls, the callers stated that they were calling because messages on their computers, which appeared to have become frozen or blocked, directed them to call the particular telephone number.
- Five of the callers told the operators that the error message they received were from Microsoft.
- The call center operators identified themselves as "technical support" or "support."
- A call center operator told one caller that the toll free number that the caller had dialed was for "Microsoft Security Toll Free." Other call center operators said that the callers had reached "Global Windows Support," "Windows Support," and a "Windows Technician."
- The call center operators said that they needed to connect remotely to the callers' computers and directed the callers to

www.supremocontrol.com, to enable the operators to obtain a remote connection.

- After obtaining remote access, the call center operators attempted to sell the callers computer service packages.

30. One of those calls from early 2019 originated from a telephone number with the area code of 561, which is assigned to the area of Palm Beach County, Florida. In conversation with the operator who received the call, the caller can be heard reporting that he received a pop-up on his computer and that his computer was making an audible sound. The operator can be heard directing the caller to use a screen sharing service called "Supremo Control" to enable the operator to access remotely the caller's computer. The operator indicates that remote access has been obtained and then reports to the caller that "bad guys" were accessing the caller's network and that his computer was not secured. The operator then said that he for \$200 could connect the caller to a network engineer who would fix the computer in two hours. The caller stated that he did not have \$200. The caller ended the call after the operator suggested that the caller postdate a check.

31. Through publicly available information and the inbound telephone number captured by CRS1, the FBI was able to identify the caller, who is for convenience referred to as PK.

32. On September 30, 2019, FBI agents spoke to PK via phone while PK was traveling outside of the United States. He identified himself as PK and further identified himself through his address, phone number, and date of birth. PK relayed the following concerning the aforementioned call:

- PK received a pop-up on his computer while trying to access an online university.
- The pop-up stated that it was from Microsoft and provided a 1-800 number to fix the virus on his computer.
- PK dialed the number and spoke to a representative.
- The representative remotely connected to his computer using "Supremo Control."
- PK saw the representative moving around on his desktop.

- The representative asked PK to pay an amount of money, over \$500, to fix his computer.
- PK did not pay the representative and bought a new computer.

33. In relation to the calls described above, Microsoft policy indicates that the call centers had no relationship with the call center operators and that the messages appearing on the victims' computers did not come from Microsoft. Microsoft policy, as set forth on its publically accessible website, www.microsoft.com, in the section entitled "Protect yourself from tech support scams," specifies that "Microsoft error and warning messages never include a telephone number."

██████████ *Buying Call Traffic from the Informant*

34. Records of communications between ██████████ and the Informant indicate that ██████████ bought call traffic from the Informant, and that those purchases occurred during time periods that included January and February 2019, when as described above the Informant's CRS account showed calls being routed to ██████████

35. The Informant, after he was arrested in May 2019, allowed investigators to extract electronic records from his cellular telephone. The extraction revealed WhatsApp and Skype text communications between the Informant's WhatsApp and Skype accounts and ██████████ WhatsApp and Skype accounts. In the text messages set forth below, which fall between August 2018 and February 2019, ██████████ and the Informant negotiate the purchase of call traffic and ██████████ commits to the purchase of call traffic.

36. In the following Skype exchange between the Informant and ██████████ asked about the price for calls, advised about his call center's "cc" capacity (which means, as the Informant explained, the concurrent call capacity of the call center or the number of simultaneous calls that the call center could handle), indicated that money would be sent for 100 calls, and sought to provide the Informant with a toll free number (referred to as "TFN" according to the Informant) to which to direct the calls. The Informant directed ██████████ to share the "TFN" via "group chat."

Date	From	Body
08/28/2018	██████████	So what's the price you can offer ??
08/28/2018	Informant	how many cc ?
08/28/2018	██████████	7cc
08/28/2018	Informant	\$14
08/28/2018	██████████	Ok, should I transfer...
08/28/2018	Informant	you can if you want i dont have issues
08/28/2018	██████████	Ok Will transfer for 100 calls 2moro Let's test
08/28/2018	██████████	Can you send calls today ???
08/28/2018	Informant	yeah i can
08/28/2018	██████████	should i share TFN???
08/28/2018	Informant	group chat
08/28/2018	██████████	Ok

37. The Informant told FBI agents that he had an office manager (hereinafter, "Manager") who assisted him and that he had had that person create a chat group to facilitate communications between the Informant, the Manager, and ██████████.

38. In the following Skype exchange between the Informant, the Manager, and ██████████ the Informant instructed ██████████ to share the "TFN," toll free number, with the group, and ██████████ provided it. Information about the Informant's U.S. bank account was also shared, which would have enabled ██████████ to direct payment for the purchase of calls.

Date	From	Body
08/28/2018	Informant	please share TFN here & [Manager] US bank details
08/28/2018	Manager	[Informant's US bank account details]
08/28/2018	Informant	sir here ?
08/28/2018	██████████	Yes ██████████

39. In the following Skype exchange between the Informant, the Manager, and [REDACTED], the Manager described to [REDACTED] that the calls have a "RPC" of \$70 - \$100, and [REDACTED] agreed to pre-pay and asked to test 50 calls. The Informant explained that RPC stood for "return per call," the likely amount of money that could be extracted from the callers.

Date	From	Body
01/10/2019	Manager	High quality calls with guaranteed RPC over \$70-100 any cc doable .. if you dont get the RPC then dont pay
01/25/2019	[REDACTED]	Post pay or prepay
01/25/2019	Informant	Pre pay
01/25/2019	[REDACTED]	Can we test with 50 calls
01/25/2019	Informant	Yes when ever you want
01/25/2019	[REDACTED]	Share your details Please I will get the wire done , let's test from Monday -
01/25/2019	Informant	Ok let me send you sir
01/28/2019	[REDACTED]	[Informant] Still waiting for details
01/28/2019	Manager	do u know the pricing?
01/28/2019	Informant	[Manager] send us bank details
01/28/2019	Manager	[Informant's US bank account details]
01/28/2019	[REDACTED]	[Informant] do you know me ???
01/28/2019	Manager	Regarding
01/28/2019	[REDACTED]	We have taken calls from you earlier , was just checking if you can send few calls for now - I will wire today -
01/28/2019	Manager	no sir sorry onlt prepay if u want u can make payment in indian account for some calls
01/28/2019	[REDACTED]	Send me Indian account details
01/28/2019	Manager	[Informant's Indian account details]
01/29/2019	[REDACTED]	M sending \$700
01/29/2019	Manager	Ok
01/29/2019	[REDACTED]	Will we get calls today

01/29/2019	Manager	Yes u want calls?
01/29/2019	Informant	Yes sir you will
01/29/2019	██████████	Yeahv I m waiting for USA guy to send me SS Meanwhile I can transfer in India for few calls if you say ██████████ Toll free ???
01/29/2019	Manager	yes payment then we start
01/29/2019	██████████	Doing 20k Now [screen shot showing twenty thousand rupees transferred to the Informant]
01/29/2019	Manager	K
01/29/2019	██████████	Transferred
01/29/2019	Manager	its not showing amount
01/29/2019	██████████	It should be with you ,you can check too
01/29/2019	Manager	Ok
01/29/2019	██████████	Please start 3cc
01/29/2019	Manager	Ok 1/3
01/29/2019	██████████	Thanks Got it
01/29/2019	Manager	Welcome 2/3
01/29/2019	██████████	Calls ???
01/29/2019	Manager	coming sir dont worry
01/29/2019	██████████	Bhai can you refund us money for rest of calls
01/29/2019	Manager	Why
01/29/2019	██████████	8 calls came in and every one said same thing You can deduct for 8 calls
01/29/2019	Manager	Wht they said

01/29/2019	[REDACTED]	They said , r u 3 rd party , r u Microsoft same Lines So I don't need more calls No hard feeling You can transfer me 10k back And rest you can keep Don't send more calls
01/29/2019	Manager	no issue sir we can refund ... these days all customers are familiar with these types of pop up ok pausing
01/29/2019	[REDACTED]	Thanks [REDACTED] 827 [REDACTED] ICIC0001400

40. In the following Skype exchange between the Informant and [REDACTED] [REDACTED] provided a telephone number and instructed the Informant to direct calls to it. The Informant instructed [REDACTED] to text the information to the group, rather than in a private message or "pm."

Date	From	Body
02/04/2019	[REDACTED]	[REDACTED] Guys use this Make sure please send good quality 3CC
02/05/2019	[REDACTED]	Guys anyone there
02/05/2019	Informant	This is pm
02/05/2019	[REDACTED]	[brother] connect me there Can't Find Group

41. In the following WhatsApp group exchange between the Informant, the Informant's manager, and [REDACTED] provided a telephone number and requested that the Informant direct calls to the number.

Date	From	Body
02/05/2019	[REDACTED]	Hi guys [REDACTED] Please send on this number Good quality
02/05/2019	[REDACTED]	Anyone here ???? Guys send 3 cc
02/05/2019	Manager	Yes
02/05/2019	[REDACTED]	Please start 3CC - good quality this time
02/05/2019	[REDACTED]	?????
02/05/2019	Manager	u live
02/05/2019	[REDACTED]	Thanks
02/05/2019	[REDACTED]	No call yet ??? Not even 1
02/05/2019	Manager	sir budget exhaust ho gaya tha updating funds wait plz (sir budget got exhausted updating funds plz wait) ⁴
02/05/2019	[REDACTED]	Ok thanks - Please do -
02/05/2019	Manager	1 live
02/05/2019	[REDACTED]	Guys ??? Send us calls
02/05/2019	Manager	1 running
02/05/2019	Manager	5 calls yesterday

⁴ A linguist fluent in Hindi and English provided the text translations for this affidavit.

Call Traffic Sold to [REDACTED]

42. Records of communications between [REDACTED] and the Informant indicate that in August and September of 2017 [REDACTED] bought call traffic from the Informant and had that call traffic directed to a particular telephone number. From late May through early June of that same year, there were complaints of that number being used by individuals misrepresenting themselves to be Microsoft representatives.

43. The Informant advised that he sold calls to [REDACTED] using his CRS2 account. The Informant advised that all of the calls were sold for the purpose of conducting tech support fraud.

44. In the following August 2017 Skype exchange between the Informant and [REDACTED], which were extracted from the Informant's cellular telephone, [REDACTED] discusses purchasing 10 "cc," which the Informant explained references the capacity to receive ten concurrent or simultaneous calls. The Informant advises that the calls would be priced at \$10 per call. [REDACTED] then provides the Informant with an email address so that [REDACTED] could track the calls being sold to him. At the end of the exchange [REDACTED] confirmed that only 58 calls were sent to him.

Date	From	Body
08/04/2017	[REDACTED]	10cc de doge ? (Will you give 10cc?)
08/04/2017	Informant	ji (Yes)
08/04/2017	[REDACTED]	what rate ?
08/04/2017	Informant	\$10
08/04/2017	[REDACTED]	INR mei batao baba (tell me in Indian rupees friend)
08/04/2017	Informant	650
08/04/2017	[REDACTED]	ok when can u start ?
08/04/2017	Informant	in 12 mins
08/04/2017	[REDACTED]	ok ping me when started ?

08/04/2017	Informant	ok
08/04/2017	██████	start nhi hua? (did it start)
08/04/2017	Informant	started hai but slow hai (it started but is slow)
08/04/2017	██████	5 cc hi de do jab tak slow h (friend give me 5cc till it is slow) baba har baar hi apna count difference ata h (everytime I get a count difference)
08/04/2017	Informant	baba (friend) yr email dedo (give me email) access deta hu [CRS2] ka (will give you access to (CRS2)) dekh lena (take a look) khud (yourself) aur kya olu (and what can I say) bolu (tell me) I use [CRS2] (I use (CRS2)) not [other call routing system] (not (other call routing system))
08/04/2017	██████	████████████████████@gmail.com bht jada difference h bhia (there is a lot of difference brother) around 10-15 calls ka (for around 10-15 calls)
08/05/2017	██████	baba i have 58 calsl only (friend I have 58 calls only) pls check again (pls check again)
08/05/2017	Informant	Dat end (that end)
08/05/2017	██████	ok baba (ok friend)

08/04/2017	Informant	ok
08/04/2017	██████	start nhi hua? (did it start)
08/04/2017	Informant	started hai but slow hai (it started but is slow)
08/04/2017	██████	5 cc hi de do jab tak slow h (friend give me 5cc till it is slow) baba har baar hi apna count difference ata h (everytime I get a count difference)
08/04/2017	Informant	baba (friend) yr email dedo (give me email) access deta hu [CRS2] ka (will give you access to (CRS2)) dekh lena (take a look) khud (yourself) aur kya olu (and what can I say) bolu (tell me) I use [CRS2] (I use (CRS2)) not [other call routing system] (not (other call routing system))
08/04/2017	██████	████████████████████ bht jada difference h bhia (there is a lot of difference brother) around 10-15 calls ka (for around 10-15 calls)
08/05/2017	██████	baba i have 58 calsl only (friend I have 58 calls only) pls check again (pls check again)
08/05/2017	Informant	Dat end (that end)
08/05/2017	██████	ok baba (ok friend)

45. In the following Skype exchange between the Informant and [REDACTED] requested that fifteen to twenty calls be sent to his call center and provided a toll free number for the call center. The Informant then directed [REDACTED] to continue the conversation in a group chat.

Date	From	Body
09/16/2017	[REDACTED]	Baba can u send calls to me at 2cc (Friend can you send calls to me at 2CC) 15-20 calls Need for my center Hanji malik? (Yes boss?)
09/16/2017	Informant	After 10 Karwa duga (Will get it done) Baba (friend)
09/16/2017	[REDACTED]	Ok baba (ok friend) Agents are waiting just need 15-20 calls at 2 cc
09/16/2017	Informant	Ji baba (yes friend)
09/16/2017	[REDACTED]	Baba (friend) Kara do start ab (get it started now) Agents are idle ?? Yaar baba kya hua? (Friend what happened?) Kaha Gaye ? (Where are you?) Baba jee (friend) Baba ? (Friend?) Dhokha de diya baba tumne (you cheated me friend) Center k lie bhi (for the center also) Baba 750 Mei de do yaar 2 cc only needed (friend give it to me for 750, 2 cc only needed)
09/16/2017	Informant	Baba calls nai aarahi hai (Friend calls not coming through)
09/18/2017	[REDACTED]	baba (friend) aaj (today) doge calls ? (will you give calls?) baba (friend)

09/18/2017	Informant	bolo (tell me)
09/18/2017	██████	calls h kuch? (do you have some calls?) gareeb k lie (for a poor person like me)
09/18/2017	Informant	centres ke liye only (for only centers)
09/18/2017	██████	kya rate doge malik ? (what rate will you charge boss)
09/18/2017	Informant	700 per call
09/18/2017	██████	de do 10 cc 700 mei (give 10 cc for 700) if possible ?
09/18/2017	Informant	5 cc
09/18/2017	██████	ok de do (ok give it) ██████
09/18/2017	Informant	group chat

46. FBI agents reviewed FTC complaints by searching for the number ██████. From the time period of May 24, 2017 until June 2, 2017, four complaints were identified in which the subject phone number ██████ was referenced. The complainants stated that callers from that number claimed to be Microsoft technical support representatives. Three of the four complaints were submitted by Microsoft's Cyber Crime Center, indicating that the purported representatives on the calls were not, in fact, associated with Microsoft.

*Conversation between the Informant and ██████ from May 2019 - June 2019
and the Use of Remote Access to Extract Funds from Accounts*

47. The Informant, at FBI's direction, communicated with ██████ and offered to allow ██████ to funnel funds into a bank account, an FBI covert account.

48. The Informant between May 2019 and June 2019, after he had been arrested and began assisting the FBI, had monitored communications with ██████ via WhatsApp text messages and voice calls. In those communications, ██████ discussed defrauding victims. The Informant was in Rhode Island during all of those communications, and the calls and messages to ██████ and received from ██████ were recorded in Rhode Island.

49. On May 22, 2019, [REDACTED] attempted to call the Informant from telephone number [REDACTED] via WhatsApp. Shortly thereafter, [REDACTED] and the Informant exchanged text messages and spoke by telephone on three occasions. The calls were recorded.

50. In the calls, which I listened to, the Informant can be heard speaking in Hindi to a male, who the Informant identified as [REDACTED]. The calls were translated by a linguist fluent in Hindi and English. The Informant advised that, as is common in the telemarketing fraud industry, the scam targets were referred to as "customers." The linguist provided the following summary of the calls:

- [REDACTED] advised that he was in the US on an open ended trip.
- [REDACTED] told the Informant that he continued to get customers and asked if the Informant had any bank accounts that [REDACTED] could transfer money into.
- [REDACTED] advised that he would use the account for himself and that he would be able to have funds wired into the account in one to two days.
- The funds would come from a Chase bank account with a total amount of \$180,000. The account could do wire transfers of \$25,000 per day.
- The Informant asked [REDACTED] to send a copy of the wire slip once the transaction was done.
- The Informant asked [REDACTED] what the customer was told, and [REDACTED] stated that he had not told the customer anything. [REDACTED] explained that the wire would be done without the customer's knowledge. When the Informant asked about a one-time password that would be sent to the customer, [REDACTED] replied with a laugh and said that they would obtain the password and the Informant shouldn't worry about it.
- [REDACTED] advised that he talked to the customer every day and had activated the account for wire transfers with a limit of \$25,000.
- [REDACTED] asked about pricing, and the Informant told [REDACTED] that he would be given 75 percent of the amount within 24-48 hours after doing the wire.
- [REDACTED] stated he would send the Informant a screen shot of the wire when completed.

51. I know from my training and experience as well as from my investigation of electronic account intrusions that financial accounts can be electronically accessed in at least two ways. First, one can obtain remote access to an account holder's computer and use that

49. On May 22, 2019, [REDACTED] attempted to call the Informant from telephone number [REDACTED] via WhatsApp. Shortly thereafter, [REDACTED] and the Informant exchanged text messages and spoke by telephone on three occasions. The calls were recorded.

50. In the calls, which I listened to, the Informant can be heard speaking in Hindi to a male, who the Informant identified as [REDACTED]. The calls were translated by a linguist fluent in Hindi and English. The Informant advised that, as is common in the telemarketing fraud industry, the scam targets were referred to as "customers." The linguist provided the following summary of the calls:

- [REDACTED] advised that he was in the US on an open ended trip.
- [REDACTED] told the Informant that he continued to get customers and asked if the Informant had any bank accounts that [REDACTED] could transfer money into.
- [REDACTED] advised that he would use the account for himself and that he would be able to have funds wired into the account in one to two days.
- The funds would come from a Chase bank account with a total amount of \$180,000. The account could do wire transfers of \$25,000 per day.
- The Informant asked [REDACTED] to send a copy of the wire slip once the transaction was done.
- The Informant asked [REDACTED] what the customer was told, and [REDACTED] stated that he had not told the customer anything. [REDACTED] explained that the wire would be done without the customer's knowledge. When the Informant asked about a one-time password that would be sent to the customer, [REDACTED] replied with a laugh and said that they would obtain the password and the Informant shouldn't worry about it.
- [REDACTED] advised that he talked to the customer every day and had activated the account for wire transfers with a limit of \$25,000.
- [REDACTED] asked about pricing, and the Informant told [REDACTED] that he would be given 75 percent of the amount within 24-48 hours after doing the wire.
- [REDACTED] stated he would send the Informant a screen shot of the wire when completed.

51. I know from my training and experience as well as from my investigation of electronic account intrusions that financial accounts can be electronically accessed in at least two ways. First, one can obtain remote access to an account holder's computer and use that

computer to access the accounts. Second, one through remote access to an account holder's computer can acquire password, username, and other information necessary for electronic access to accounts and can use that information to gain access to the accounts. Based on [REDACTED] statements above, I believe there is sufficient cause to believe that [REDACTED] was deploying or was planning to deploy one of these two methods to access victims' accounts.

52. Following the call, the Informant provided to [REDACTED] information for a covert, FBI-controlled bank account, including bank name, account holder name, account number, routing number, and bank address. For convenience the account is referred to as "Account 1." The information provided was the information necessary to make wire transfers to Account 1, because it was anticipated that [REDACTED] would be transferring money via wire. As described below, [REDACTED] opted, at least initially, to use a different money transfer technique.

53. On May 30, 2019, [REDACTED] and the Informant exchanged the following WhatsApp messages. [REDACTED] asked the Informant whether Zelle⁵ transfers could be made into Account 1. [REDACTED] said that he could transfer to the Informant money from a victim's Chase bank account but was unable to because the Informant was unavailable.

Date	From	Body
05/30/2019	[REDACTED]	Can we do Zelle ?
05/30/2019	Informant	Amount ?
05/30/2019	[REDACTED]	Zelle can be done for 2500 You didn't reply I had that customer
05/30/2019	Informant	Depends upon the limit of bank You texted in the middle of the night
05/30/2019	[REDACTED]	Chase bank

54. Again on May 30, 2019, [REDACTED] and the Informant exchanged the following WhatsApp messages. [REDACTED] stated that he configured a victim's personal Chase bank account to be able to make Zelle transfers. [REDACTED] stated that because the Informant was unavailable,

⁵ Zelle is a mobile payment platform that allows account holders at Zelle-member banks to send money to other account holders at Zelle-member banks.

no transfer was made to the Informant's account. [REDACTED] requested the email address associated with the Account 1, and the Informant provides [REDACTED] with that email address.

Date	From	Body
05/30/2019	Informant	If I meet you can we do then ? I am keeping that account only for you .. I want things to work
05/30/2019	[REDACTED]	Yea I understand. Zelle would have surely worked yesterday if I wld have had the info . Anyways I ll try with the same cm and see if it's works today. Will try Zelle. Got it activated yesterday, it's a chase personal acct Not sure abt the limit . What's the email/phone for Zelle?
05/30/2019	Informant	Sending details Now For zelle
05/30/2019	[REDACTED]	Ok thanks
05/30/2019	Informant	Can I call
05/30/2019	[REDACTED]	Give me 10 min
05/30/2019	Informant	Ok
05/30/2019	[REDACTED]	Or speak in Hindi
05/30/2019	Informant	Waiting
05/30/2019	[REDACTED]	Thanks
05/30/2019	Informant	?
05/30/2019	[REDACTED]	Now
05/30/2019	Informant	[Email associated with Account 1]

55. Following those text exchanges, the Informant communicated with [REDACTED] by telephone, and those calls were recorded. I listened to the calls, during which the Informant spoke in Hindi to a male individual, who the Informant identified as [REDACTED]. The recorded calls were also listened to by a Hindi linguist and the following summary of the calls contents was provided to me:

- [REDACTED] asked if the Informant could get a credit card activated and advised that the total card limit of \$15,000 to \$20,000 could be used in one day.

- The Informant asked [REDACTED] if the credit card's owner would receive a request for a one-time password and [REDACTED] advised that the customer would not.
- [REDACTED] confirmed that he had a physical credit card in the name of a customer and planned on getting two more.
- [REDACTED] advised that \$9,500 was transferred to Account 1.
- The Informant told [REDACTED] that the wire was still in transit and had not actually been completed because it was scheduled for tomorrow. The Informant also told [REDACTED] that the customer would get a call, but an unknown male who was with [REDACTED] stated that the customer had a bank card and so did they.

56. On June 3, 2019, the Informant made a recorded telephone call with [REDACTED] I listened to the call, during which the Informant spoke in Hindi to a male individual, who the Informant identified as [REDACTED]. The recorded call was also listened to by a Hindi linguist who provided the following summary of the call:

- The Informant commented that [REDACTED] had deleted some of his WhatsApp messages.
- The Informant advised [REDACTED] that he did not receive the wire transfer for \$9,500 and asked [REDACTED] to check the customer's bank account.

57. On June 7, 2019, the Informant made a recorded telephone call with [REDACTED] I listened to the call, during which the Informant spoke in Hindi to a male individual, who the Informant identified as [REDACTED]. The recorded call was also listened to by a Hindi linguist and a summary of the call contents was provided to me. The following was discussed:

- The Informant told [REDACTED] that the Informant was still located in Rhode Island.
- [REDACTED] told the Informant that he attempted to wire \$4,800 yesterday but that it also did not go through and was wondering what was happening.
- [REDACTED] stated that the customer authorized the transfer, but then the people from the bank instructed the customer not to authorize it. The Informant suggested having a three way call with the bank and the customer so that the bank will authorize it.
- The Informant asked which state the credit card that [REDACTED] was sending was coming from and [REDACTED] replied that one was coming from "Vegas" and that he would have to find out where the other one was coming from.

- [REDACTED] instructed the Informant to use the cards as soon as possible and advised that he could send one card a week that would either be in the customer's name or the Informant's name.

[REDACTED] Has Proceeds from Tech Support Sent to Covert Account via Zelle

58. After having previously discussed making a Zelle transfer, as described above, [REDACTED] in July 2019 initiated a Zelle transfer to Account 1, and investigation indicated that the funds were proceeds of tech support fraud.

59. On June 17, 2019, [REDACTED] and the Informant exchanged the following WhatsApp messages where [REDACTED] provided the Informant with screenshots indicating that a Zelle transfer had been made into Account 1 from a Chase bank account.

Date	From	Body
06/17/2019	[REDACTED]	[Forwarded screenshot of a Chase bank account online transfer with transaction number JPM241833112] Zelle
06/17/2019	[REDACTED]	Is Zelle not registered??
06/17/2019	[REDACTED]	(Forwarded screenshot of the same Chase bank account online transfer) Please register with Zelle

60. On June 17, 2019, the email address associated with Account 1, previously provided to [REDACTED] by the Informant, received an email message from "Notifications@zellepay.com" indicating that \$2,000 was sent to the account holder. The email message included the account holder's name. That account holder is referred to here as "SW." Account 1 was not configured to receive Zelle transfers, which prevented the transfer of \$2,000 from SW's account to Account 1.

61. In December, 2019, FBI agents interviewed SW who was initially very skeptical about whether she was actually being contacted by law enforcement. SW advised that when she was speaking to the individuals who had initiated the transfer from her bank account, they had repeatedly told her it was not a scam. SW provided the following information:

- On June 17, 2019, SW was playing a game on her computer when it froze and her computer screen said there was a virus on the computer. The screen listed a telephone number to call.

- SW called the telephone number on the screen and a male individual, who sounded American, answered the call.
- The male individual said he could unfreeze SW's computer and asked for remote access into SW's computer. SW told him yes and a box appeared on SW's screen asking for permission to give control of SW's computer to the individual.
- After access was given the male individual ran a test on SW's computer which showed a black box on SW's computer running files and showing run commands.
- After the test was complete the male individual told SW she needed additional security on her computer.
- SW told the individual she already had McAfee on her computer but the male individual told her McAfee would not solve her computer problem. SW believes the male individual downloaded a software application called CCleaner on her computer. SW also believes the male individual may have put something called Zema or Zemaware on her computer.
- The male individual told SW she needed to pay for the security software right then and told SW it cost \$500. At this point SW began to question the individual on the phone and told him she thought this sounded suspicious.
- The male individual wanted SW to transfer the money from her bank account and told her to access her banking account online. SW accessed her JPMorgan Chase checking account while the male individual still had access and dual control of her computer. The male individual showed SW how to set up a transfer from her checking account.
- The male individual set up a transfer in SW's bank account for \$2,000 to another person. SW questioned the male individual, telling him it felt like a scam because the transfer was going to a person and not a company, and that it was for \$2,000 and not \$500. The male individual told her it didn't cost \$2,000, but that was just to get the transfer set up.
- A second male individual told SW she could write a check which SW did. SW wrote a check for \$548 and scanned the check into her computer. SW watched as the second male individual accessed the scanned check on her computer, expanded it on the screen and took a picture of the check. The call then ended.
- SW immediately went back into her bank account and cancelled the transfer of \$2,000 on the JPMorgan Chase website. SW did not cancel the check or put in a stop payment. The check was never cashed.

62. Investigation into the Chase bank account owned by SW and the Zelle transfer confirmed that a \$2,000 transfer was initiated from her account with a transaction number of

JPM241833112, the same transaction number visible in the screen shot sent by [REDACTED] to the Informant on June 17, 2019.

*Conversation between [REDACTED] and Informant from
September 2019 - October 2019 Concerning the Routing of
Additional Money into the Covert Account*

63. In communications between [REDACTED] and the Informant, [REDACTED] advised that additional money would be coming to Account 1. A subsequent review of Account 1 transaction records allowed the FBI to identify the people whose accounts had been targeted by [REDACTED].

64. On September 17, 2019, [REDACTED] and the Informant exchanged the following WhatsApp messages where [REDACTED] told the Informant that he needed a bank account and could transfer \$5,000 a day into the account. The Informant again provided bank account details for Account 1 and they agreed on a split of profits where [REDACTED] would receive 80 percent of the amount that was transferred to the Informant.

Date	From	Body
09/17/2019	[REDACTED]	Call me It's urgent.
09/17/2019	Informant	Hi Sorry was sleeping when you called Everything fine?
09/17/2019	[REDACTED]	Yeah all good . Need account + lower percentage , 5k everyday -
09/17/2019	Informant	For sure ya fir just like old times
09/17/2019	[REDACTED]	This time it will be good hopefully Zz
09/17/2019	Informant	Ok Can we start from today ?
09/17/2019	[REDACTED]	Yes , let me knows what's the percentage, I will get them started I have [covert account holder's last name] Account Is it still up and running
09/17/2019	Informant	[Account 1 information]

		Yeah use the same for now
09/17/2019	██████████	Ok , percentage
09/17/2019	Informant	80 % payout
09/17/2019	██████████	20 yours, 80 mine Payout ??v Wire or cash

65. On September 21, 2019, ██████████ and the Informant exchanged the following WhatsApp messages where ██████████ forwarded messages from another individual and asked the Informant to confirm the amount of two small deposits which had been made into Account 1 in order for a larger wire transfer into Account 1 to be approved. The Informant explained that "Cx" is an abbreviation for customer, referring to a victim, used by both the Informant and others in the tech-support fraud industry.

Date	From	Body
09/21/2019	██████████	Bhai (Brother) need to confirm me the amont So that I can initiate
09/21/2019	Informant	Acct can do any amount Send and will be in acct on Monday
09/21/2019	██████████	██████████ forwarded the following lines of text from communication with someone else: "Cx has some credit union account. They hv sent 2 small deposits for verification Once its verified then only wire can happen"]
09/21/2019	██████████	Please confirm this -

66. On September 27, 2019, ██████████ and the Informant communicated via a WhatsApp voice call which was recorded. I listened to the call, during which the Informant spoke in Hindi to a male individual, who the Informant identified as ██████████. The recorded call was also listened to by a Hindi linguist, who provided the following summary:

- The Informant asks ██████████ what happened with the transaction verification
- ██████████ says that the customer told him he was putting \$25,000 but later never confirmed it.

67. FBI agents reviewed transactions in Account 1. The following transactional information appeared in the account. (For ease of review, victim names have been highlighted.) Further investigation by FBI agents identified the victims associated with the transactions, who are referred to as "DH," "DR," "DS" and "PH."

Post Date	Reference	Debit	Credit	Text
9/20/2019	UNITED COMMUNITYUNIT		\$0.03	UNITED COMMUNITYUNITED COM VICTIM DH
9/20/2019	UNITED COMMUNITYUNIT		\$0.69	UNITED COMMUNITYUNITED COM VICTIM DH
9/20/2019	UNITED COMMUNITYUNIT	\$0.03		UNITED COMMUNITYUNITED COM VICTIM DH
9/20/2019	UNITED COMMUNITYUNIT	\$0.69		UNITED COMMUNITYUNITED COM VICTIM DH
11/1/2019	PNCBANK_XTRANSFRTRIA		\$0.28	PNCBANK_XTRANSFRTRIALCREDIT VICTIM DR
11/1/2019	PNCBANK_XTRANSFRTRIA		\$0.46	PNCBANK_XTRANSFRTRIALCREDIT VICTIM DR
11/1/2019	PNCBANK_XTRANSFRTRIA	\$0.74		PNCBANK_XTRANSFRTRIALDEBIT VICTIM DR
11/4/2019	PENTAGON FEDERALTRIA		\$0.06	PENTAGON FEDERALTRIAL CR VICTIM PH
11/4/2019	PENTAGON FEDERALTRIA		\$0.12	PENTAGON FEDERALTRIAL CR VICTIM PH
11/6/2019	WELLS FARGO IFITRIAL		\$0.08	WELLS FARGO IFITRIAL DEP VICTIM DS
11/6/2019	WELLS FARGO IFITRIAL		\$0.23	WELLS FARGO IFITRIAL DEP VICTIM DS
11/6/2019	WELLS FARGO IFITRIAL	\$0.31		WELLS FARGO IFITRIAL DEP VICTIM DS

Interview of DH

68. DH was interviewed, and his statements indicated that there had been an attempt to extract money from him using tech support fraud.

69. On January 16, 2020, FBI agents spoke to DH, who was 74 years old. DH relayed the following information:

- In approximately September 2019, DH received a telephone call from someone who advised that DH's computer security and/or virus software was outdated and they offered to pay DH \$300 for the old software.
- The caller spoke with an Asian accent and was calling from a busy office.
- The caller requested remote access to DH's computer and DH gave the caller access but did not recall which website was used to grant the access.
- DH was directed to withdraw \$4,500 and purchase various gift cards. DH withdrew the money and was on his way to purchase the gift cards when he realized it may be a scam.
- DH returned to the bank deposited the funds back into his account and told the bank what had happened. The bank was able to close his accounts the same day.
- DH did not recall giving the caller access to his bank accounts, but may have.
- The caller attempted to re-contact DH after he closed his accounts, but DH did not answer the call.

Interview of DR

70. DR was interviewed, and her statements indicated that there had been an attempt to extract money from her using tech support fraud.

71. On January 16, 2020, FBI agents spoke to DR, who was 83 years old. DR relayed the following information:

- In approximately November 2019, DR heard a loud noise from her computer that stated her computer had been hacked and provided a number to call "Microsoft Support".
- DR dialed the number and was connected to a man with either a Middle Eastern or Indian accent.
- While on the phone with the man, DR's PNC online banking account was open and it appeared to DR that the man could see everything on the screen because it seemed like "they were on there with me" during the call.
- Shortly after DR's conversation with the man, she received a notification on her phone indicating an attempt to transfer funds to a bank account in New York (where Account 1 is located). DR went immediately to the bank and shut down her online banking for her account.

Interview of DS

72. DS was interviewed, and her statements indicated that there had been an attempt to extract money from her using tech support fraud.

73. In January 2020, FBI agents spoke to DS, who was 82 years old. DS provided the following information:

- In November 2019, DS was reviewing her Wells Fargo bank statement online and saw several unauthorized charges for \$6,000.
- DS saw that four of five withdrawals of \$6,000 had been made from her checking account.
- DS contacted Wells Fargo and did not suffer a loss from these unauthorized withdrawals.
- DS has changed her online passwords and opened new bank accounts.
- DS told the Agent that she does not recall the details from this time and stated that she had blocked out this time in her life. DS received and answered one phone call from an unknown individual around this time. She did not recall the content of that call. DS stated that the individual kept calling, but in November DS stopped answering those phone calls. Finally, the individual stopped calling.

Introduction of Anjum by [REDACTED]

74. As the investigation proceeded as to PH, in communications with the Informant, [REDACTED] indicated that he was working with another person, Anjum. [REDACTED] indicated that Anjum was asking about the status of certain fund transfers.

75. On October 17, 2019, [REDACTED] and the Informant exchanged the following WhatsApp messages discussing a bank account screen shot that [REDACTED] had provided the Informant on October 16, 2019. The bank account screen shot indicated that a wire transfer of \$4,500 was initiated to Account 1. [REDACTED] asked if the Informant had received a wire transfer for \$8,786 and a separate transfer for \$4,500. [REDACTED] also forwarded a screen shot of WhatsApp messages he had exchanged with the contact name "Abrar Usa." In those screen shot messages [REDACTED] was asked to check on the wires.

Timestamp-Date	From	Body
10/17/2019	██████████	Bjai Wire Ka update dedo Yaar (Give the update for wire) He is behind my life [screen shot of WhatsApp messages with "Abrar Usa"]
10/17/2019	Informant	Hi how are you ?
10/17/2019	██████████	M good brother
10/17/2019	Informant	Confirmation only came for 4500 , and rest nothing came in yet
10/17/2019	██████████	Ok , how about 8786
10/17/2019	Informant	Never got that [image of previously provided bank account screen shot] Need a confirmation like this for that What bank did you wire from ? And can you get me customer's ID
10/17/2019	██████████	[Forwarded message: 8786 was from chase bank]
10/17/2019	Informant	How about the other one ?
10/17/2019	██████████	4500 one is from Wells Fargo

76. On October 21, 2019, ██████████ and the Informant communicated via a WhatsApp voice call, which was recorded. I listened to the call, during which the Informant spoke in Hindi to a male individual, who the Informant identified as ██████████. The recorded call was also listened to by a Hindi linguist, who provided the following summary:

- Informant advised that neither transfer had been received into Account 1 and asks for a screen shot showing the debit.
- ██████████ tells the Informant that he is getting it done through another person and that the person told ██████████ that they don't ask the customer for screen shots as long as the wire works.
- The Informant reiterates that no wire has been received.
- ██████████ says he will create a group chat on WhatsApp which would include ██████████, the Informant, and the other person.

77. Following the voice call, ██████████ created a group chat which included ██████████, the Informant, and telephone number ██████████ which ██████████ identified as "Abrar."

\$15,000 Bank Check & Interview of PH

78. As investigation proceeded, a \$15,000 check from PH was directed to Account 1, the FBI's covert account, and investigators learned from PH that she had been a victim of tech support fraud and that \$15,000 had been drawn from her accounts without her knowledge. Also, Anjum and [REDACTED] contacted the Informant and inquired about the status of a \$15,000 transfer, Anjum specified that that money had come from PH, and Anjum and [REDACTED] sought to have the money directed to them.

79. On October 29, 2019, the bank in which Account 1 is held received a check in the amount of \$15,000, and the payor listed on the check was PH. It was a computer generated check and indicated that the sum on the check was to be deposited into Account 1. The check also listed PH's bank name. The FBI did not have this check deposited.

80. On November 07, 2019, FBI Agents spoke to PH via phone. PH identified herself as PH, and further identified herself through her address and phone number. PH relayed the following information:

- In October 2019, PH was on her computer when a pop-up message appeared to freeze her computer. The pop up message said it was from Microsoft and contained a 1-800 number for her to contact.
- PH called the 1-800 number and spoke with Harry Wilson who had an Indian accent.
- Wilson remotely connected to her computer and PH saw Wilson open a file containing PH's online passwords.
- Wilson opened a notepad document on her computer and told PH that she needed to protect her computer. Wilson also told PH that she could purchase one of two security packages.
- Wilson instructed PH to purchase gift cards to pay for the security package.
- When PH refused to purchase a security package Wilson became angry.
- Later the same day, PH received a phone call from another individual with the same type of accent as Wilson.
- The individual still had remote access to PH's computer and said they were calling from Mount View, California.
- The individual told PH that he was checking her firewall and that it needed replaced.

- PH deleted the software the individuals had used to remotely access her computer.
- PH began receiving scam email messages from PayPal.
- PH later received a call from her bank about potential fraud occurring in her account.
- When PH checked records associated with her bank accounts, she saw that \$450.00 had been debited from her account and also saw a debit for \$15,000 for which she was liable.
- PH last spoke with the individuals on November 5, 2019.

81. On November 7, 2019, Anjum sent a WhatsApp text message containing a screen shot. The screen shot indicated a \$15,000 transaction on an account associated with PH's bank.

82. Shortly thereafter, Anjum sent the following WhatsApp messages requesting that the Informant confirm that Account 1 had received \$15,000 and stating that another \$15,000 would later be wired but was on hold for the moment.

Timestamp-Date	From	Body
11/7/2019	Anjum	[Informant] plz check. 15k deposited in [Covert] account
11/7/2019	[REDACTED]	[Informant] please update ASAP
11/8/2019	Anjum	[Informant] buddy please respond
11/8/2019	[REDACTED]	[Informant] ??? You there
11/8/2019	Anjum	[Informant] please update. [Informant] we need an update as another 15k needs to be wired. I hv put that on hold for now.

83. On November 12, 2019, the Informant, Anjum, and [REDACTED] exchanged the following WhatsApp messages where the Informant requests a name associated with the \$15,000. Anjum provides PH's name as the individual who sent the \$15,000 and asks the Informant to confirm two other transactions.

Date	From	Body
11/12/2019	[REDACTED]	Cool , just update him about the wire , bank should be opened now
11/12/2019	Informant	So I got the 15K, but I have 3 15K at the same time same date .. so can you please provide customer's

		name or id proof makes my life easy that which one is yours..
11/12/2019	██████████	Ok Will update you Now
11/12/2019	Informant	Waiting
11/12/2019	Anjum	Will reply in a while In meeting
11/12/2019	Informant	Ok
11/12/2019	Anjum	[PH]
11/12/2019	Sharma	Ok
11/12/2019	Informant	Alright
11/12/2019	Anjum	Also plz confirm 2 new small amounts under \$1
11/12/2019	Informant	When was it sent
11/12/2019	Anjum	Friday
11/12/2019	Informant	Screen shots? We got the wire 15k from [PH] but the bank send us a physical cheque for the same amount .. so I presented the cheque today waiting for it to be clear soon And I will update you the screen shot of small transactions in 2 hours or so taking a lunch break
11/12/2019	Anjum	Ok

84. On November 16, 2019 and November 18, 2019, Anjum, ██████████ and the Informant exchanged the following messages on WhatsApp. The Informant - per FBI's direction - tells Anjum and ██████████ that the check was cashed, and Anjum requests that the money be transferred to him immediately.

Date	From	Body
11/16/19	Informant	Check cleared
11/16/19	Anjum	Plz transfer [Informant]
11/16/19	Informant	Banker can transfer next week Will call Monday
11/16/19	Anjum	Next week is too late
11/16/19	Informant	Calling banker now

11/16/19	Anjum	The more its delayed the more wires are not happening and it's a loss for everyone including you
11/16/19	██████	[Informant] it's not what you promised, we were supposed to get money as it cleared, we should get the money on Monday
11/18/19	Anjum	[Informant] plz update asap.
11/18/19	Informant	Hi morning Where do you want the money? US or india
11/18/19	██████	Cash in India??? Or USA whatever earliest
11/18/19	Anjum	Bank Wells Fargo [Account and Routing Informaton] Name: Abrar Anjum
11/18/19	██████	[Informant] please wire today itself And send the screen shot
11/18/19	Informant	Alright
11/18/19	██████	Thanks

85. On November 20, 2019, the Informant made a recorded telephone call with ██████ I listened to the call, during which the Informant spoke in Hindi to a male individual, who the Informant identified as ██████ The recorded call was also listened to by a Hindi linguist and a summary of the calls contents was provided to me. The following was discussed:

- The Informant tells ██████ that DH, DR, PH, and DS have only made small attempts to transfer money into the Account 1 and only PH has made a small transfer.
- ██████ tells the Informant that the guy he is working with is saying that he does not want to send anymore wires until the remaining money he is owed is sent to him.
- ██████ identifies his partner as "Abrar" (Anjum's first name) and says that "Abrar" is partners with another individual.
- ██████ says he received a call from Abrar who told him that if he had received payment, he would have done more wires.
- The Informant asked if Abrar and his partner were doing refunds, and ██████ replied that he didn't know. However, ██████ did know that Abrar and his partner had a call center, sold calls, and did money wires.
- ██████ met Abrar and his partner at the Taj hotel in India and knew Abrar from before.

86. On November 21, 2019, Agents, utilizing a covert bank account, transferred \$7,000 to Anjum's Wells Fargo Bank account.

87. On November 22, 2019, Anjum, [REDACTED] and the Informant exchanged the following WhatsApp messages regarding the transfer of funds to Anjum's bank account.

Timestamp-Date	From	Body
11/22/19	Informant	[Sends a screenshot showing a \$7,000 wire sent on 11/21/19]
11/22/19	Anjum	Why 7k??
11/22/19	Informant	Banker sent 7K
11/22/19	Anjum	R u guys crazy or what After waiting for over 3weeks u sending just 7k [REDACTED] its my last request get it sorted by hook or by crook. Tmrw I want the whole money in my account
11/22/19	[REDACTED]	Sure Abrar, it should done today only...
11/22/19	Anjum	Waiting.... TD Bank [Account and Routing Number] Name: Abrar Anjum Please transfer the rest of the amount to this account

88. Aside from the \$7,000, no additional money was directed to Anjum or [REDACTED].

[REDACTED] Involvement in Theft from PH's Account

89. In December, [REDACTED] contacted the Informant and expressed concerned about Anjum and [REDACTED] not have receiving their share of the remainder of the \$15,000 from PH. [REDACTED] also explained that Anjum and [REDACTED] were his partners and that he had fronted them their share of the remainder and sought payment from the Informant. [REDACTED] indicated that the \$15,000 at issue was money taken from PH.

90. On December 2, 2019,⁶ the Informant received a WhatsApp message, via phone number [REDACTED], from [REDACTED]. The following WhatsApp messages were exchanged between [REDACTED] and Informant regarding the payment for PH's \$15,000 check previously discussed with [REDACTED] and Anjum. In the conversation [REDACTED] tells the Informant that PH was his victim and says that he, [REDACTED], had to pay Anjum the remainder himself:

Date:	From:	Body:
12/2/2019	[REDACTED]	There BABA [father]
12/2/2019	Informant	Yes
12/2/2019	[REDACTED]	Baba [Father]
12/2/2019	Informant	Bolo [Speak]
12/2/2019	[REDACTED]	There has been some wire done into ur account Thru my end Of 15K The guy is saying he got only 7K paid from you and the rest is due at ur end It was thru Abraar n [REDACTED]
12/2/2019	Informant	Baba yr I already explained that shit
12/2/2019	[REDACTED]	I have paid client thru my pocket and now they are saying you are not paying them Can we talk on call? I have paid additional 2950 from my pocket bro so please kara do bhai jee unka jo bhi balance h so that they can pay me rest (I have paid additional 2950 from my pocket bro so please get it done brother whatever balance he has so that they can pay me rest)
12/2/2019	Informant	Yes give me 5 min
12/2/2019	[REDACTED]	Ok call me when you can I am waiting

91. On December 2, 2019, [REDACTED] and the Informant communicated via a WhatsApp voice call which was recorded. I listened to the call, during which the Informant spoke in Hindi

⁶ At the time of this communication, it was December 3 in India, and December 2 in the United States.

to a male individual, who the Informant identified as [REDACTED]. The recorded call was also listened to by a Hindi linguist, who provided the following summary:

- The Informant asked [REDACTED] how he became involved with Anjum and [REDACTED] told the Informant that the wire belongs to his acquaintance.
- [REDACTED] told the Informant that [REDACTED] told him this wire belonged to the Informant.
- [REDACTED] told the Informant that Anjum and [REDACTED] never told him that the Informant was handling the wire. If they had, [REDACTED] would have talked directly to the Informant.
- [REDACTED] told the Informant that [PH] was the first transaction with the Informant and it took a long time and they didn't even get the money.
- [REDACTED] tells the Informant that he paid the person \$7,000 and paid the remaining \$2,500 out of his own pocket.
- The Informant told [REDACTED] that he was told by [REDACTED] and Anjum that he would get a wire, but received a physical check instead.
- The Informant told [REDACTED] that he asked Anjum and [REDACTED] for the victim's details and did not get them. [REDACTED] told the Informant that he did not share the details with Anjum and [REDACTED].
- [REDACTED] told the Informant that he now owes his own money, \$3,000, and asked the Informant for a solution to the problem.
- [REDACTED] said he is working on a 60/40 with Anjum and [REDACTED]. [REDACTED] said that he will get 65% from this transaction per agreement.
- [REDACTED] told the Informant that it is a "tech" payment and that he only does those.
- [REDACTED] told the Informant that he is coming to America in January and he will visit the Informant.

92. On December 11, 2019, and December 18, 2019, the following WhatsApp messages were exchanged between [REDACTED] and Informant regarding the payment for PH's \$15,000 check:

Date:	From:	Body:
12/11/19	Informant	I talked to my banker regarding the same, I am Not saying no buy he has not replied to me yet for the same..he was like we already had a bad deal with them and made a loss of 15k plus I sent you 7 K and did not even got my cut, how can you say that you pay them another 1500-2000 from us he will work again..
12/11/19	[REDACTED]	Wait baba (friend)

		I have daily work for you [REDACTED] forwards the Informant a "Premier Checking Account" showing two wire transfers] See wire done yesterday for 20k The only reason this is can't go in loss for nothing bro
12/11/19	Informant	That's a transfer from saving to checking lol
12/11/19	[REDACTED]	Kya yaar baba [What friend]
12/11/19	Informant	Anyways I believe your word but I am still waiting on my guy
12/11/19	[REDACTED]	\$14904 and \$4596 [referring to the wire transfer amounts] IF you feel it's right to pay \$2750 which I paid from my pocket then you can pay bro for old sake times and we can start our business fresh else I'll take it from [REDACTED] have no other option bro Will have daily good work rest I leave to your fine judgement
12/18/2019	[REDACTED]	Baba are we resolving this?

93. On January 8, 2019, the following WhatsApp messages were exchanged between [REDACTED] and Informant regarding the victim details of the \$15,000 check:

Date:	From:	Body:
1/8/2019	Informant:	Hi how are you Baba Ji? Can you please send the wire screen shot again with customer name, I will look into it today and get back to you soon..
1/8/2019	[REDACTED]	M good bro It was a check That u got [A photo of a screen shot was sent to the Informant showing a \$15,000 transaction that took place on 11/1/2019 from Alexandria, VA. The screen shot included a reference ID number.] [PH]
1/8/2019	Informant	Alright thanks, I will get back to you soon on this..how's work?
1/8/2019	[REDACTED]	Work is fine bro Not great but yeah it's ok 2750 ki baat h kara do (it is a matter of 2750 get it done)

		We can do Bigger things together
1/8/2019	Informant	How big are we talking here? I need assurance to convince him to send you money.
1/8/2019	██████	Baba (friend) daily around 5-20K anything Plus 2-5K zelle if you provide that
1/8/2019	Informant	Alright
1/8/2019	██████	Let me know hen we can start Sooner will be better
1/8/2019	Informant	Ok
1/8/2019	██████	Any update baba? So we can start our work too?

III. CONCLUSION

94. Based on the above, I believe that there is probable cause to believe that ██████ ██████ ██████, and Abrar Anjum committed the offenses specified in paragraph 2 above.



 SPECIAL AGENT CRAIG GRAHAM
 Federal Bureau of Investigation

Subscribed and sworn to before
me this 23rd day of January 2020,
at Providence, Rhode Island



 LINCOLN D. ALMOND
 United States Magistrate Judge

EXHIBIT 1



EXHIBIT 2



EXHIBIT 3

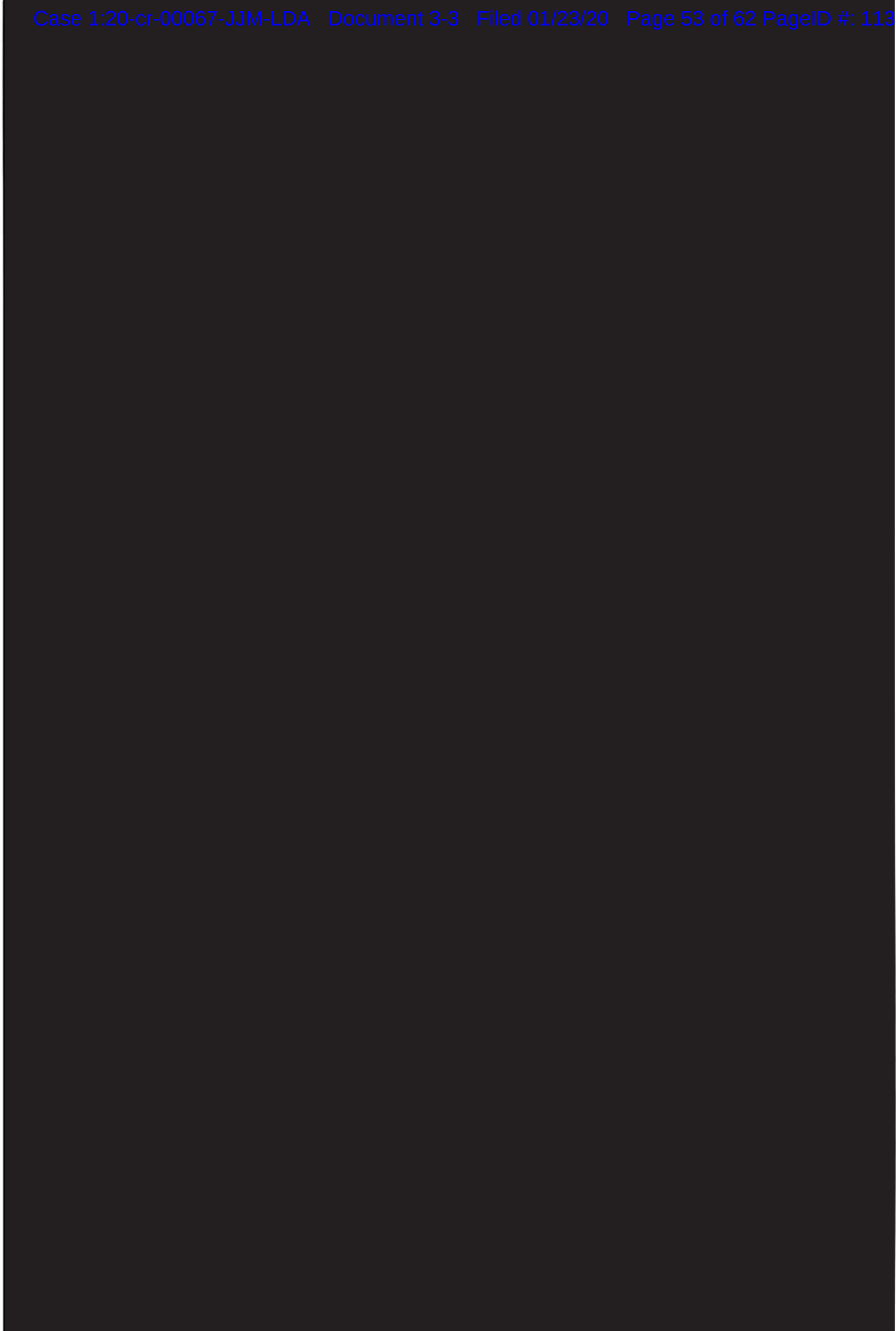


EXHIBIT 4

EXHIBIT 5

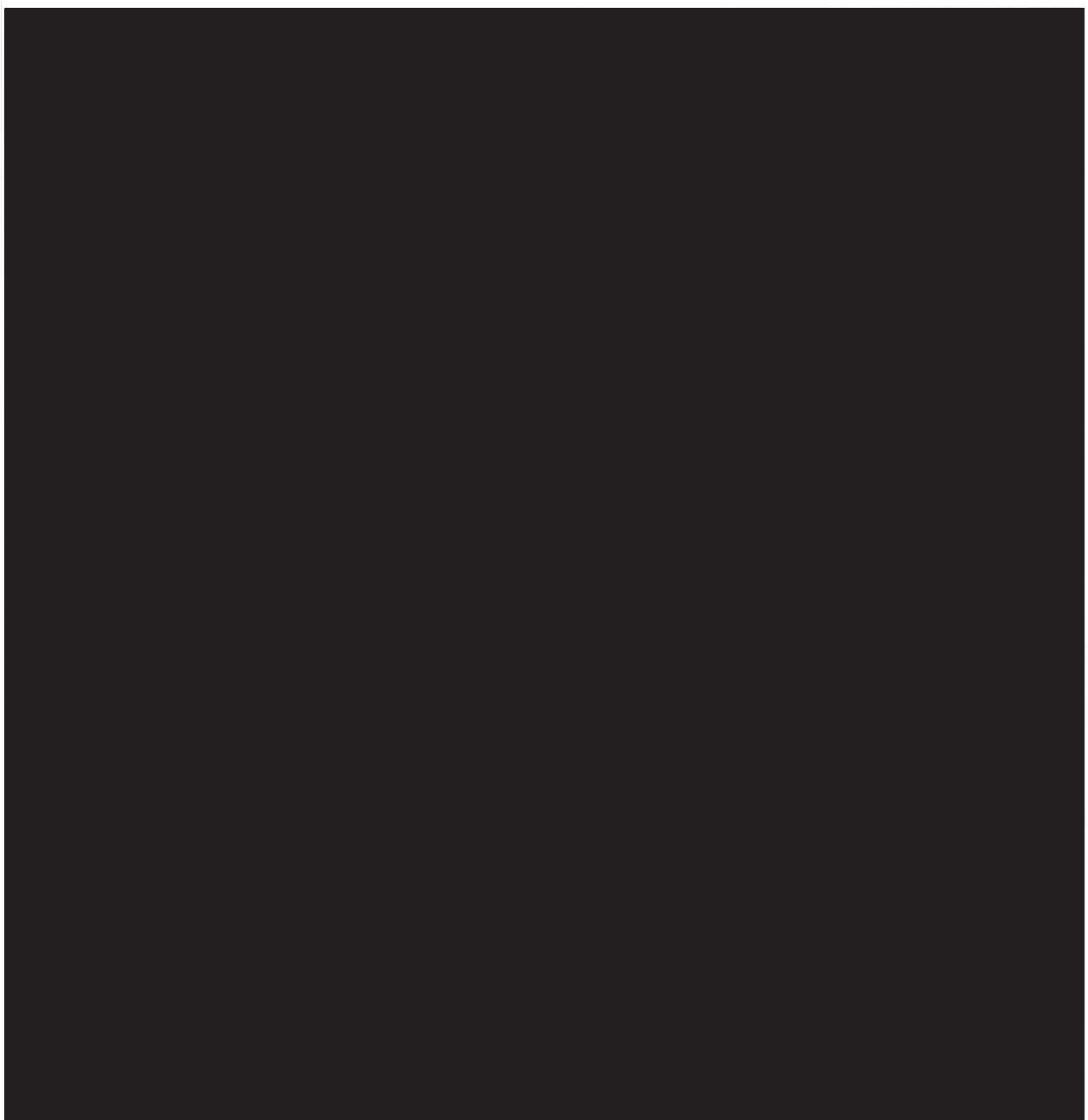
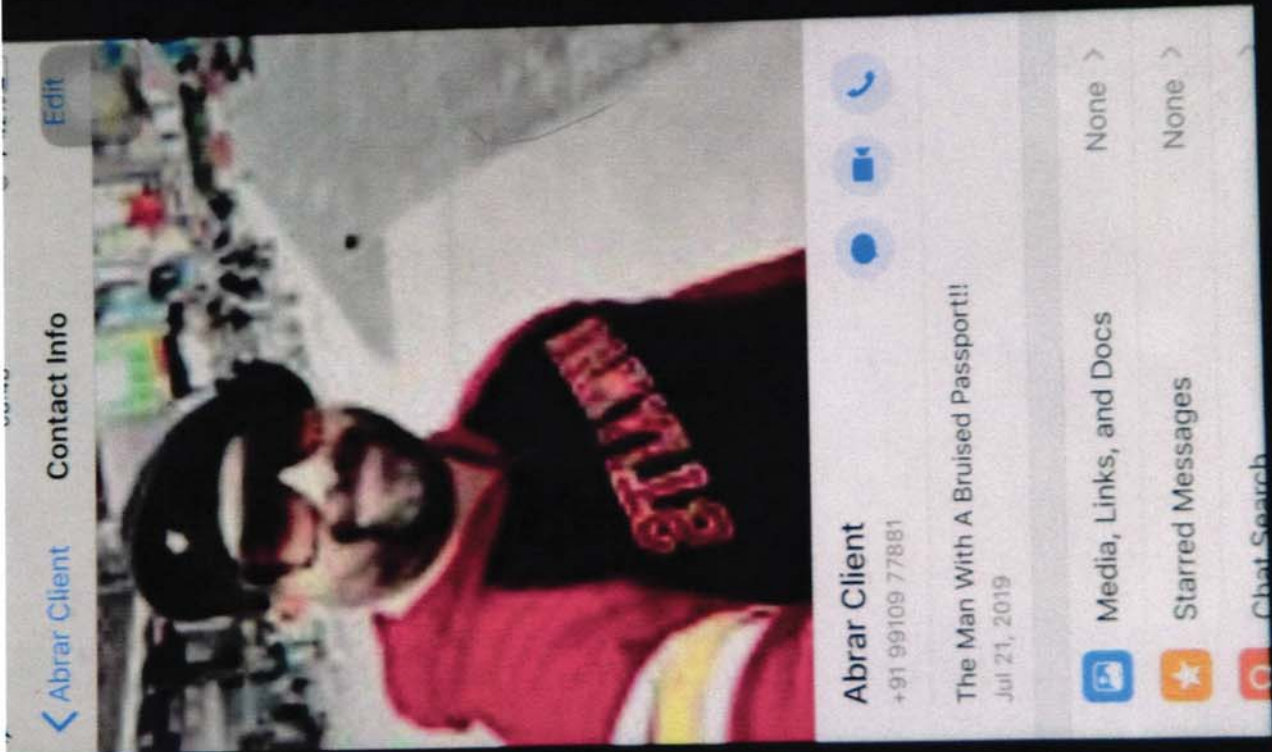


EXHIBIT 6



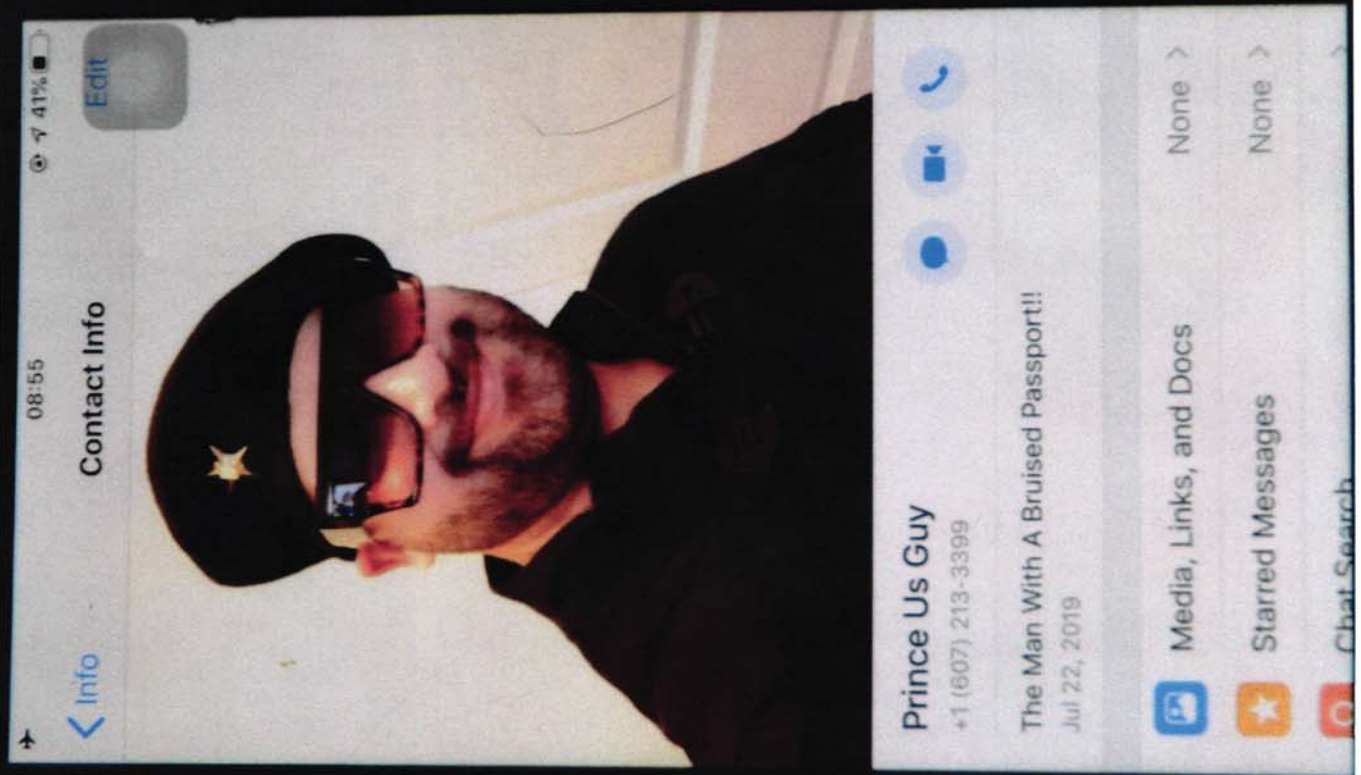


EXHIBIT 7

