
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

v.

ASHISH BAJAJ

:
: Hon. André M. Espinosa
:
: Mag. No. 21-11149
:
: CRIMINAL COMPLAINT
:
: **FILED UNDER SEAL**

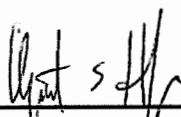
I, Elizabeth S. Hornberger, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

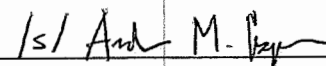
SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Elizabeth S. Hornberger
Special Agent
Federal Bureau of Investigation

Special Agent Hornberger attested to this Affidavit by telephone pursuant to F.R.C.P. 4.1(B)(2)(A) on this 29th day of July, 2021.



HONORABLE ANDRÉ M. ESPINOSA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Count One
(Conspiracy to Commit Wire Fraud)

From at least as early as in or around April 2020 through in or around July 2021, in the District of New Jersey and elsewhere, defendant

ASHISH BAJAJ

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

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

ATTACHMENT B

I, Elizabeth S. Hornberger, am a Special Agent of the Federal Bureau of Investigation. The information contained in the Complaint is based upon my personal knowledge, as well as information obtained from other sources, including: (a) statements made or reported by various witnesses with knowledge of relevant facts; (b) my review of publicly available information; and (c) my review of evidence, including business records, bank records, and other documents and records. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact that I know concerning this investigation. Where the contents of documents and the actions and statements of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Individuals and Entities

1. At all times relevant to this Complaint:
 - a. Defendant ASHISH BAJAJ (“BAJAJ”) resided in New York and California.
 - b. Crypto E Service LLC (“Crypto E Service”) was a company associated with BAJAJ established in New York, New York.
 - c. Victim-1 was a resident of New Jersey.
 - d. Victim Company-1 was established and operated in New Jersey, and was associated with Victim-1.
 - e. Victim-2 was a resident of California.
 - f. Victim-3 and Victim-4 were spouses who resided in California.
 - g. Bank-1 was headquartered in New York.
 - h. Bank-2 was headquartered in Texas.
 - i. Bank-3 was headquartered in California.
 - j. Bank-4 was headquartered in New York.
 - k. Bank-5 was headquartered in California.

Overview

2. From at least as early as in or around April 2020 through in or around July 2021, BAJAJ and his co-conspirators received at least approximately \$2.3 million in fraudulently obtained funds by impersonating fraud prevention representatives from banks located in the United States. BAJAJ and/or the co-conspirators misrepresented to victims—many of whom were elderly—that they worked at a “hub” for multiple financial institutions’ fraud departments and were reaching out because the victims’ bank accounts had been hacked. BAJAJ and the co-conspirators asked the victims to assist with their fraud prevention efforts by setting up “sting” operations to catch the fraudsters who allegedly hacked the victims’ bank accounts. The requested assistance included initiating various wire transactions to various bank accounts, including bank accounts in India, ultimately resulting in a loss to the victims. Over the course of the investigation, law enforcement has identified multiple victims of this scheme.

Victim 1

3. In or around April 2020, Victim-1, who is approximately 73 years old, was contacted by individuals identifying themselves as N.T. and C.W. N.T. and C.W. each claimed to be a representative of Bank-1.

4. N.T. and C.W. told Victim-1 that Bank-1 was investigating fraud related to Victim-1’s personal account at Bank-1. Victim-1 discussed Victim Company-1’s bank account with N.T. and C.W. as well (together, the “Victim-1 Accounts”). N.T. and C.W. indicated to Victim-1 that they required Victim-1’s assistance identifying fraud implicating the Victim-1 Accounts.

5. N.T. instructed Victim-1 to assist him by setting up “sting” operations designed to catch in the act the fraudsters who had hacked the Victim-1 Accounts. This assistance included initiating various wire transactions from the Victim-1 Accounts. Based on N.T.’s representations about the operation, Victim-1 did not believe the money would ever leave the Victim-1 Accounts.

6. Over the course of several months, as directed by N.T., Victim-1 initiated multiple outgoing interstate wire transactions—including wire transactions that traveled through New Jersey—totaling approximately \$1,450,000 to multiple accounts, including to businesses located in India. This money has not been recovered.

Victim 2

7. Beginning in or around May 2020, Victim-2, who is approximately 65 years old, received phone calls from an individual identifying himself as N.D..

N.D. claimed to be an employee within the fraud department of Bank-1. N.D. told Victim-2 that Victim-2's various accounts, including her bank accounts, had been hacked. N.D. further instructed Victim-2 to send wire transactions from her account at Bank-1 to an account in India to catch the individuals responsible for the hack. N.D. indicated to Victim-2 that she would receive her money back.

8. In particular, N.D. instructed Victim-2 to send money to BAJAJ, who was associated with Crypto E Service. N.D. explained to Victim-2 that BAJAJ worked with N.D.

9. Following these instructions, in or around May 2020, Victim-2 wired approximately \$34,000 from her account at Bank-1 to a bank in India. Victim-2 understood that she was sending this money to BAJAJ. The approximately \$34,000 wire transfer was subsequently returned to Victim-2 due to an address error. Victim-2 was also instructed to complete a Zelle¹ cash application transfer of approximately \$1,500, which she believed was going to BAJAJ.

10. In total, Victim-2 was instructed to transfer approximately \$650,000 over the course of the scheme. This money has not been recovered.

Victims 3 and 4

11. In or around September 2020, Victim-3, who is approximately 76 years old, communicated with C.W., who purported to be from Bank-2. C.W. transferred Victim-3 to B.S.² B.S. indicated to Victim-3 that he worked in the fraud department of Bank-3, which had identified fraud related to Victim-3's account. B.S. asked for Victim-3's assistance in catching the individuals perpetrating the fraud by wiring funds to an account in India. Victim-3 sent a total of approximately \$130,000 from his account at Bank-3 to the account in India.

12. On one occasion while Victim-3 was speaking to B.S., B.S. also spoke to Victim-4, who is approximately 67 years old. B.S. transferred Victim-4 to N.D., who claimed to be a representative from Bank-2's fraud department. N.D. told Victim-4 that Victim-4's bank account at Bank-4 had been compromised. Victim-4 was directed to go to Bank-4 to complete an approximately \$130,000 wire transfer to assist in catching the individuals perpetrating the fraud. Victim-4 believed her money would be returned following the "sting" operation.

¹ Zelle is a digital payment network. Zelle enables individuals to electronically transfer money from their bank account to another registered user's bank account using a mobile device or the website of a participating banking institution.

² N.T., C.W., B.S., and N.D. are believed to be aliases for BAJAJ and/or his co-conspirators.

13. Victim-4 wired approximately \$130,000 from her bank account at Bank-4. This money has not been recovered.

Identifying BAJAJ as a Member of the Conspiracy

14. Victim-4 provided law enforcement with several phone numbers used by C.W., B.S., and N.D., including a telephone number ending -7824 (the "7824 Number"). According to Victim-4, both B.S. and N.D. utilized the 7824 Number. Victim-4 also provided law enforcement with phone records, which included multiple calls from the 7824 Number from on or about September 21, 2020 to on or about September 22, 2020. Victim-4 also provided law enforcement with a voice message from C.W. to Victim-3, in which C.W. requested that Victim-3 call the 7824 Number.

15. Law enforcement subsequently learned that the 7824 Number was subscribed to BAJAJ, with an associated address in Anaheim, California (the "Anaheim Address").

16. Over the course of the investigation, law enforcement learned that BAJAJ has maintained myriad bank accounts over the course of the scheme, including accounts at Bank-1 and Bank-5. For instance, law enforcement obtained records of BAJAJ's account at Bank-5 (the "3639 Account"), which BAJAJ opened on or about December 30, 2020 and closed on or about February 11, 2021. BAJAJ is the sole signatory on the 3639 Account, and he listed the Anaheim Address as his address on that account.

17. A review of the 3639 Account revealed that BAJAJ made approximately 20 payments to the telecommunications service provider of the 7824 Number between on or about January 11, 2021 to on or about January 29, 2021.

18. In addition, the 3639 Account records show Zelle transfers into the 3639 Account from what appear to be additional victims based on the volume, monetary amounts, timing, and the identifiers associated with the payments.

19. Law enforcement has identified at least two bank accounts BAJAJ opened in the name of Crypto E Service. BAJAJ is the sole signatory on both accounts, which are associated with an address in New Rochelle, New York (the "New Rochelle Address"). The New Rochelle Address is the same address BAJAJ listed for a personal account he opened at Bank-1. Moreover, a review of commercially available databases revealed that BAJAJ is associated with the New Rochelle Address.