

FILED Jun 08 2020

CAROL L. MICHEL CLERK

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF LOUISIANA **FELONY**

BILL OF INFORMATION FOR CONSPIRACY TO COMMIT WIRE FRAUD AND NOTICE OF FORFEITURE

UNITED STATES OF AMERICA * CRIMINAL NO. 20-cr-52
v. * SECTION: **SECT. T MAG 2**
RICHARD YUAN LI * VIOLATIONS: 18 U.S.C. § 2
18 U.S.C. § 371
18 U.S.C. § 1343
* * *

The United States Attorney charges that:

COUNT 1

A. AT ALL TIMES MATERIAL HEREIN:

- 1. The defendant, **RICHARD YUAN LI** (“LI”), attended high school in Buffalo, New York. Beginning in Fall 2018, **LI** was a student at University of California – San Diego (“UCSD”) and resided in Argo Hall on the campus of UCSD.
- 2. Victim A was a resident of New Orleans, Louisiana, within the Eastern District of Louisiana. Victim A was a physician who operated a medical practice in New Orleans.
- 3. Victim A subscribed to cellular phone service provided by Phone Company A with cellular phone number (504) 352-XXXX.

Fee _____
Process _____
Dktd _____
CtRmDep _____
Doc. No _____

4. Victim A used multiple email accounts, including xxxxxxxx@gmail.com and xxxxxxxx@aol.com (collectively, “Victim A’s email accounts”).

5. Victim A held and owned multiple cryptocurrency accounts, including with the following cryptocurrency exchange companies: Binance, Bittrex, Coinbase, Gemini, Poloniex, ItBit, and Neo Wallet.

6. A SIM Swap scam is a cellular phone account takeover fraud that results in the routing of a victim’s incoming calls and text messages to a different phone. Once a perpetrator is able to swap the SIM card, it is likely he is able to obtain access to a victim’s various personal accounts, including email accounts, bank accounts, and cryptocurrency accounts, as well as any other accounts that use two-factor authentication.

B. THE CONSPIRACY:

7. Beginning at a time unknown, but not later than January 3, 2018, and continuing through at least February 24, 2019, in the Eastern District of Louisiana and elsewhere, the defendant, **RICHARD YUAN LI**, and others known and unknown to the United States, did willfully and knowingly combine, conspire, confederate, and agree together and with each other to execute, and attempt to execute, a scheme and artifice to defraud and to obtain money, funds, and property by means of false and fraudulent pretenses, representations and promises and did transmit and cause to be transmitted by means of wire communication in interstate commerce certain writings, signs, signals and sounds, in violation of Title 18, United States Code, Section 1343.

C. PURPOSE OF THE CONSPIRACY:

8. The purpose of the conspiracy was for **LI**, and others known and unknown to the United States, to enrich themselves unjustly by conducting SIM Swap scams on cellular phone

service customers, including Victim A, and thereafter obtain cryptocurrency belonging to the customers by means of materially false and fraudulent pretenses and representations.

D. MANNER AND MEANS:

9. The manner and means by which **RICHARD YUAN LI** and others known and unknown to the United States sought to accomplish the object and purpose of the conspiracy included, among other things, the following:

10. **LI** and a co-conspirator implemented a scheme in which they defrauded Apple, Inc. into providing a second Apple iPhone without paying for it by convincing an Apple customer service representative that they had not received an Apple iPhone 8 they ordered (hereinafter “the Apple iPhone 8”).

11. **LI** and his co-conspirators then arranged for victims’ telephone numbers to be swapped to SIM cards contained in cellular phones in their possession, including the Apple iPhone 8.

12. **LI** and his co-conspirators used the victims’ cellphone numbers and deceptive techniques to gain access to email, electronic storage, and other accounts of victims.

13. **LI** and his co-conspirators reset the passwords for victims’ accounts so that the conspirators could control the accounts.

14. **LI** and his co-conspirators used information from the victims’ accounts to access victims’ cryptocurrency accounts and transfer without authority cryptocurrencies owned by the victims to themselves.

15. **LI** and his co-conspirators contacted victims and demanded victims pay a ransom in exchange for releasing some or all of the personal information and cryptocurrency back to victims.

OVERT ACTS:

16. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed and caused to be committed the following overt acts, among others, in the Eastern District of Louisiana and elsewhere:

17. On or about January 5, 2018, **LI**, impersonating a co-conspirator, contacted Apple customer service via telephone and stated that he had not received the Apple iPhone 8 that he had ordered previously and requested a replacement iPhone.

18. On or about January 23, 2018, **LI** registered the Apple iPhone 8 using his email address, ryliXXXXX@me.com.

19. On or about November 10, 2018, Victim A's telephone number was swapped to a SIM card contained in the Apple iPhone 8, which **LI** possessed. The SIM swap caused, among other things, the transmission of a series of writings, signs, signals, and sounds that traveled in interstate commerce, including between the States of Florida, Louisiana, and California.

20. On or about November 10, 2018, **LI** or his known and unknown co-conspirators gained access to Victim A's email accounts and cryptocurrency accounts as a result of the SIM Swap.

21. On or about November 10, 2018, shortly after Victim A regained service to Victim A's cellular phone, **LI** or one of his co-conspirators contacted Victim A via telephone. The caller told Victim A that he had viewed pictures stored in Victim A's Gmail account. The caller also identified the cryptocurrency accounts Victim A held along with the approximate account balances of each accounts. The caller told Victim A to pay him 100 Bitcoin to prevent the pictures from being released and the contents of Victim A's cryptocurrency accounts from being taken.

22. On or about November 10, 2018, **LI** or his co-conspirators converted to their benefit cryptocurrency belonging to Victim A.

23. Between on or about October 11, 2018, and December 6, 2018, **LI** participated in unauthorized SIM Swaps with known and unknown co-conspirators that targeted at least nineteen (19) other victims, including Victim A and Victim B, in approximately twenty-eight (28) swapping incidents.

All in violation of Title 18, United States Code, Sections 371 and 2.

NOTICE OF FORFEITURE

1. The allegations of Count 1 are incorporated by reference as though set forth fully herein for the purpose of alleging forfeiture to the United States.

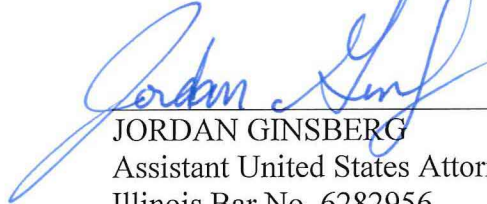
2. As a result of the offenses alleged in Count 1, defendant, **RICHARD YUAN LI**, shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property real or personal which constitutes or is derived from proceeds traceable to said offenses.

3. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred, sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

the United States shall seek a money judgment and, pursuant to Title 21, United States Code, Section 853(p), forfeiture of any other property of the defendant up to the value of said property.

PETER G. STRASSER
UNITED STATES ATTORNEY



JORDAN GINSBERG
Assistant United States Attorney
Illinois Bar No. 6282956

New Orleans, Louisiana
June 8, 2020