

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- x
:
UNITED STATES OF AMERICA :
:
-v- :
:
JOSEPH JAMES O'CONNOR, :
a/k/a "PlugwalkJoe," :
:
Defendant. :
----- x

SEALED INDICTMENT

21 Cr.

21 CRIM 536

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

The Grand Jury charges:

Overview of the Criminal Conduct

1. Between in or about March 2019 and in or about May 2019, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, participated in a scheme to use SIM swaps to conduct cyber intrusions in order to steal approximately \$784,000 worth of cryptocurrency from a Manhattan-based cryptocurrency company ("Company-1").
2. During a cyber intrusion known as a SIM swap attack, cyber threat actors gain control of a victim's mobile phone number by linking that number to a subscriber identity module ("SIM") card controlled by the threat actors, resulting in the victim's calls and messages being routed to a malicious unauthorized device controlled by the threat actors. The threat actors then typically

use control of the victim's mobile phone number to obtain unauthorized access to accounts held by the victim that are registered to the mobile phone number.

3. During all times relevant to the Indictment, Company-1 provided wallet infrastructure and related software to cryptocurrency exchanges around the world. Between in or about March 2019 and in or about May 2019, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and his co-conspirators successfully perpetrated SIM swap attacks targeting at least three Company-1 executives ("Executive-1," "Executive-2," and "Executive-3").

4. Following a successful SIM swap attack targeting Executive-1 on or about April 30, 2019, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, successfully gained unauthorized access to multiple Company-1 accounts and computer systems.

5. On or about May 1, 2019, using their unauthorized access to Company-1 accounts and computer systems, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, stole and fraudulently diverted cryptocurrency of various types (the "Stolen Cryptocurrency") from cryptocurrency wallets maintained by Company-1 on behalf of two of its clients. The Stolen Cryptocurrency was worth at least approximately \$784,000 at the time of the theft and included approximately 770.784869 Bitcoin cash, approximately 6,363.490509 Litecoin, approximately

407.396074 Ethereum, and approximately 7.456728 Bitcoin.

6. After stealing and fraudulently diverting the Stolen Cryptocurrency, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, laundered it through dozens of transfers and transactions and exchanged some of it for Bitcoin using cryptocurrency exchange services. Ultimately, a portion of the Stolen Cryptocurrency was deposited into a cryptocurrency exchange account controlled by O'CONNOR.

Statutory Allegations

7. From at least in or about March 2019, up to and including at least in or about May 2019, in the Southern District of New York and elsewhere, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, computer intrusion, in violations of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii), 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(a)(5)(B), 1030(c)(4)(A)(i)(I) and 1030(c)(4)(B)(i).

8. It was a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby obtained information from protected computers, for

purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

9. It was further a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, would and did knowingly and with intent to defraud, access and attempt to access protected computers without authorization, and exceed authorized access, and by means of such conduct would and did further the intended fraud and obtain something of value that exceeded \$5,000 in a one-year period, in violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A).

10. It was further a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage, without authorization, to protected computers, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000 in value to one and more persons during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I) and

1030(c)(4)(B)(i).

11. It was further a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, knowingly and intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage, and caused loss to one and more persons during any one-year period aggregating at least \$5,000 in value, in violation of Title 18, United States Code, Section 1030(a)(5)(B) and 1030(c)(4)(A)(i)(I).

Overt Acts

12. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about April 30, 2019, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, perpetrated a SIM swap of the mobile phone number used by Executive-1. Within hours of this SIM swap attack, O'CONNOR and his co-conspirators leveraged control of Executive-1's phone number to obtain unauthorized access to Company-1 accounts and computer systems.

b. On or about April 30 and May 1, 2019, as part of their unauthorized access to Company-1 accounts and computer systems, O'CONNOR and his co-conspirators changed G Suite account passwords for several Company-1 employees. As a result, Company-

1 employees, including employees in the Southern District of New York, were unable to access their corporate G Suite accounts.

c. On or about May 1, 2019, using their unauthorized access to Company-1 accounts and computer systems, O'CONNOR and his co-conspirators diverted the Stolen Cryptocurrency from cryptocurrency wallets maintained by Company-1 on behalf of two of its clients to cryptocurrency addresses and wallets controlled by O'CONNOR and his co-conspirators.

d. On or about May 4, 2021, following SIM swap attacks targeting Executive-2 and Executive-3, O'CONNOR or one of his co-conspirators (the "Conspirator") accessed Executive-3's Skype account without authorization and used said account to send numerous messages via group chat to Company-1 employees, including to one or more employees in the Southern District of New York. During the Skype group chat, the Conspirator described, in substance and in part, the SIM swap targeting Executive-1, the unauthorized access to Company-1 accounts and computer systems, and the resulting theft of cryptocurrency. The Conspirator also posed questions to Company-1 employees about, in substance and in part, Company-1 computer infrastructure and its employees' cryptocurrency holdings.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

13. The allegations set forth in paragraphs 1 through 6 are incorporated by reference as though fully set forth herein.

14. From at least in or about March 2019, up to and including at least in or about May 2019, in the Southern District of New York and elsewhere, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

15. It was a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire and radio communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, O'CONNOR and others engaged in a SIM swapping scheme and obtained unauthorized access to online accounts and

computer systems to fraudulently obtain cryptocurrency, which scheme involved the use of interstate and foreign wires.

(Title 18, United States Code, Section 1349.)

COUNT THREE
(Aggravated Identity Theft)

The Grand Jury further charges:

16. The allegations set forth in paragraphs 1 through 6 are incorporated by reference as though fully set forth herein.

17. From at least in or about March 2019, up to and including at least in or about May 2019, in the Southern District of New York and elsewhere, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, O'CONNOR transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, mobile phone numbers and electronic account credentials of other persons during and in relation to the wire fraud conspiracy offense charged in Count Two of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), and 2.)

COUNT FOUR
(Conspiracy to Commit Money Laundering)

The Grand Jury further charges:

18. The allegations set forth in paragraphs 1 through 6 are incorporated by reference as though fully set forth herein.

19. In or about May 2019, in the Southern District of New York and elsewhere, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, knowingly did combine, conspire, confederate and agree together and with each other to violate the money laundering laws of the United States.

20. It was a part and object of the conspiracy that JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, and others known and unknown, knowing that the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, the computer intrusion and wire fraud scheme targeting Company-1, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii), 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(a)(5)(B), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i), and 1343, knowing that the transactions were designed in whole and in part to conceal and disguise the nature,

the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i), to wit, O'CONNOR and his co-conspirators caused the proceeds of computer intrusion and wire fraud scheme against Company-1 to be distributed among themselves and other co-conspirators by, among other things, causing the Stolen Cryptocurrency to be transferred through dozens of transfers and transactions and partially exchanged for Bitcoin using cryptocurrency exchange services, in order to conceal the nature, location, source, ownership, and control of the Stolen Cryptocurrency.

(Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATION AS TO COUNT ONE

21. As a result of committing the offense alleged in Count One of this Indictment, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offense, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

FORFEITURE ALLEGATION AS TO COUNT TWO

22. As a result of committing the offense alleged in Count Two of this Indictment, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, 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 and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

FORFEITURE ALLEGATION AS TO COUNT FOUR

23. As a result of committing the offense alleged in Count Four of this Indictment, JOSEPH JAMES O'CONNOR, a/k/a "PlugwalkJoe," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any and all property, real and personal, involved in said offense, or any property traceable to such property, including but not limited to a sum of money in United States currency representing the amount of property involved in said offense.

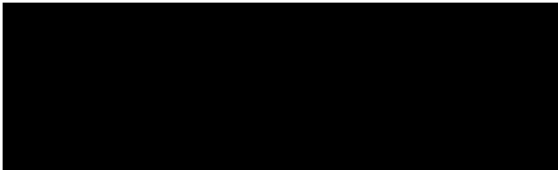
Substitute Assets Provision

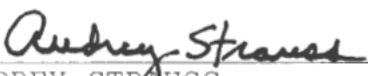
24. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or 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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982, 1030; Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461.)




AUDREY STRAUSS
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

JOSEPH JAMES O'CONNOR,

a/k/a "PlugwalkJoe,"

Defendant.

SEALED INDICTMENT

(18 U.S.C. §§ 371, 1028A, 1349, 1956(h))

AUDREY STRAUSS

ney



10
