UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. MATTHEW D. LANE, Defendant	Criminal No. Violations: Count One: Cyber Extortion Conspiracy (18 U.S.C. § 371) Count Two: Cyber Extortion; Aiding and Abetting (18 U.S.C. §§ 1030(a)(7)(B), (c)(3)(A) and 2) Count Three: Unauthorized Access to Protected Computers; Aiding and Abetting (18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii), and (iii), and 2) Count Four: Aggravated Identity Theft (18 U.S.C. § 1028A(a)(1)) Forfeiture Allegation: (18 U.S.C. §§ 982(a)(2)(B) & 1030(i))

INFORMATION

At all times relevant to this Information:

General Allegations

1. Defendant MATTHEW D. LANE lived in Worcester County, Massachusetts.

2. Co-Conspirator 1 ("CC-1") lived in Illinois.

3. Victim 1 was a U.S.-based telecommunications company. In or about October 2022, an unknown individual obtained unauthorized access to Victim 1's computer network and stole confidential customer information stored on that network ("the Stolen Victim 1 Data").

4. Victim 2 was a software and cloud storage company that served school systems in

the United States, Canada, and elsewhere.

5. Employee 1 was a contractor working for Victim 2. Victim 2 assigned Employee 1 credentials that Employee 1 used to access Victim 2's computer network, including a unique user identification number ending in 00A0 ("the Employee 1 Credentials").

The Cyber Extortion Conspiracy Targeting Victim 1

6. Between at least as early as April 2024 and in or about May 2024, LANE, CC-1, and co-conspirators known and unknown to the U.S. Attorney conspired to extort Victim 1 into paying a $200,000 ransom to avoid public disclosure of the Stolen Victim 1 Data.

Object and Purpose of the Cyber Extortion Conspiracy Targeting Victim 1

7. The object of the conspiracy was to commit cyber extortion by threatening to disclose the Stolen Victim 1 Data unless Victim 1 paid a ransom. The principal purposes of the conspiracy were for the co-conspirators to make money and to conceal their actions from Victim 1 and law enforcement.

Manner and Means of the Cyber Extortion Conspiracy Targeting Victim 1

8. Among the manner and means by which LANE, CC-1, and co-conspirators known and unknown to the U.S. Attorney carried out the conspiracy were the following:

a. Obtaining the Stolen Victim 1 Data;

b. Contacting Victim 1 representatives anonymously;

c. Demanding payment in exchange for not leaking the Stolen Victim 1 Data; and

d. Using encrypted messaging applications and online accounts to hide their identities and evade detection by Victim 1 and law enforcement.

Overt Acts in Furtherance of the Cyber Extortion Conspiracy Targeting Victim 1

9. Between at least as early as April 2024 and in or about May 2024, LANE, CC-1, and co-conspirators known and unknown to the U.S. Attorney committed and caused to be committed the following overt acts, among others, in furtherance of the cyber extortion conspiracy targeting Victim 1:

a. On or about April 22, 2024, LANE used an anonymized email address to contact Victim 1 and demanded a ransom of $200,000 in Bitcoin in exchange for not leaking the Stolen Victim 1 Data;

b. Later the same day, LANE messaged CC-1 over Signal, an encrypted messaging application, that LANE had sent the extortionate message to Victim 1 and that Victim 1 had responded;

c. On or about April 25, 2024, LANE messaged CC-1 that Victim 1 had asked for samples of the Stolen Victim 1 Data, which LANE stated he would provide;

d. Minutes later, LANE messaged CC-1 that LANE had sent samples of the Stolen Victim 1 Data to Victim 1;

e. On or about April 27, 2024, in response to a message from CC-1, LANE stated that Victim 1 was likely to pay the ransom.

f. On or about April 29, 2024, LANE messaged CC-1 requesting input on how to pressure Victim 1 into responding to their ransom demand more quickly. After receiving CC-1's response, LANE notified CC-1 that he had sent a message to Victim 1.

g. On or about May 3, 2024, LANE and CC-1 discussed by Signal how to pressure Victim 1 to respond to their ransom demand and how long they should wait for Victim

1's response.

h. On or about May 6, 2024, CC-1 messaged LANE to check for a response from Victim 1.

i. Later that day, LANE copied the response that he had received from Victim 1 into a Signal message to CC-1. The response from Victim 1 stated: "When you messaged us from this account back in November, you told us not to pay any ransom as multiple copies of the data were floating around. Now, you come to us asking to be paid. We need help to understand your position."

j. After sharing Victim 1's message, LANE sent a proposed response to CC-1, which CC-1 approved.

k. LANE then emailed the answer he had proposed to Victim 1: "A member of our group (now handled with) split off with the data and claimed it as theirs. We eventually had him dealt with[]in the coming year. We are the only ones with a copy of this data now. Stop this nonsense and your executives and employees will see the same fate as he did. Make the correct decision and pay the ransom. If you keep stalling, it will be leaked. Do not waste time."

l. After sending the message to Victim 1, LANE updated CC-1 that he had "threatened" Victim 1 again.

m. On or about May 8, 2024, CC-1 messaged LANE for an update on the communications with Victim 1.

n. LANE messaged CC-1 in response that he had reduced the ransom demand to $75,000.

o. On or about May 14, 2024, LANE messaged CC-1 that if Victim 1 did not

pay the ransom, LANE and CC-1 could sell the Stolen Victim 1 Data. LANE further suggested, "we need to hack another . . . company that[']ll pay."

LANE's Unauthorized Access to Victim 2's Computer Network

10. On or about September 4, 2024, LANE used the Employee 1 Credentials to gain unauthorized access to Victim 2's computer network.

11. On or about the same day, LANE obtained student and teacher data belonging to one of Victim 2's customers from Victim 2's network without authorization.

12. On or about December 19, 2024, LANE leased a computer server from a cloud storage provider located in Ukraine.

13. On or about December 20, 2024, LANE caused the Social Security numbers, dates of birth, and confidential medical information, among other data, of the students and faculty of Victim 2's customers to be transferred from Victim 2's computer network to the computer server in Ukraine that LANE had leased the day before.

14. On or about December 28, 2024, Victim 2 received a ransom demand. The demand threatened to "leak . . . worldwide" the names, email addresses, phone numbers, Social Security numbers, dates of birth, medical information, residential addresses, parent and guardian information, and passwords, among other data, of more than 60 million students and 10 million teachers if Victim 2 did not send 30 Bitcoin (approximately $2.85 million at the time) to a specific Bitcoin address.

COUNT ONE
Cyber Extortion Conspiracy
(18 U.S.C. § 371)

The U.S. Attorney charges:

15. The U.S. Attorney re-alleges and incorporates by reference Paragraphs 1-3 and 6-9 of this Information.

16. Between at least as early as April 2024 and in or about May 2024, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW D. LANE,

conspired with CC-1 and others known and unknown to the U.S. Attorney to knowingly and with intent to extort from Victim 1 money and other things of value, transmit in interstate commerce communications containing threats to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access, to wit, the Stolen Victim 1 Data, in violation of Title 18, United States Code, Section 1030(a)(7)(B) and (c)(3)(A).

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
Cyber Extortion; Aiding and Abetting
(18 U.S.C. §§ 1030(a)(7)(B), (c)(3)(A) and 2)

The U.S. Attorney charges:

17. The U.S. Attorney re-alleges and incorporates by reference Paragraphs 1-3 and 6-9 of this Information.

18. On or about May 6, 2024, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW D. LANE,

knowingly and with intent to extort from Victim 1 money and other things of value, transmitted in interstate commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization, to wit, the Stolen Victim 1 Data.

All in violation of Title 18, United States Code, Sections 1030(a)(7)(B), (c)(3)(A) and 2.

COUNT THREE
Unauthorized Access to Protected Computers; Aiding and Abetting
(18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii), and (iii), and 2)

The U.S. Attorney charges:

19. The U.S. Attorney re-alleges and incorporates by reference Paragraphs 1, 4-5, and 10-14 of this Information.

20. On or about September 4, 2024, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW D. LANE,

intentionally accessed a computer, to wit, Victim 2's computer network, without authorization, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain; in furtherance of a criminal act in violation of the laws of the United States, namely, threatening to impair the confidentiality of information obtained from a protected computer, in violation of Title 18, United States Code, Section 1030(a)(7)(B); and where the value of the information obtained exceeded $5,000.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), (ii), and (iii), and 2.

COUNT FOUR
Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1))

The U.S. Attorney charges:

21. The U.S. Attorney re-alleges and incorporates by reference Paragraphs 1, 4-5, and 10-14 of this Information.

22. On or about September 4, 2024, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW D. LANE,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, the Employee 1 Credentials, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, obtaining information through access without authorization to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2), as charged in Count Three of this Information.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

FORFEITURE ALLEGATION
(18 U.S.C. §§ 982(a)(2)(B) & 1030(i))

The U.S. Attorney further alleges:

23. Upon conviction of one or more of the offenses in violation of Title 18, United States Code, Sections 371 and 1030(a), set forth in Counts One through Three, the defendant,

MATTHEW D. LANE,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B) and 1030(i), any property constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses; and, pursuant to Title 18, United States Code Section 1030(i), any personal property used, or intended to be used, to commit, or to facilitate the commission of, such offenses and any property, real or personal, constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses. The property to be forfeited includes, but is not limited to, the following assets:

a. $160,981 to be entered in the form of a forfeiture money judgment

24. If any of the property described in Paragraph 23, above, as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), 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 party;

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 divided without difficulty;

it is the intention of the United States, pursuant to Title 18, United States Code, Sections 982(b)(2) and 1030(i)(2), each incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the property described in Paragraph 23 above.

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

LEAH B. FOLEY
United States Attorney

By: */s/ Kristen A. Kearney*
KRISTEN A. KEARNEY
Assistant U.S. Attorney