SUPPRESSED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

FILED

NOV - 8 2017

U. S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

UNITED STATES OF AMERICA,

Plaintiff,

v.

NATHAN WYATT,

Defendant.

No. 4:17CR00522 RLW/SPM

INDICTMENT

THE GRAND JURY CHARGES THAT:

At times relevant to this Indictment:

1. Victim 1 was a health care provider located in Farmington, Missouri, in the Eastern District of Missouri. Victim 1 utilized "protected computers," as that term is defined in Title 18, United States Code, Section 1030(e)(2), in interstate and foreign commerce to, among other things, store and transmit sensitive and personally identifying information (PII) about patients, including billing and medical records.

2. Victim 2 was a medical records company headquartered in Swansea, Illinois. Victim 2 utilized "protected computers," as that term is defined in Title 18, United States Code, Section 1030(e)(2), in interstate and foreign commerce to, among other things, store and transmit sensitive and personally identifying information, medical records, and billing records on behalf of its clients.

3. Victim 3 was a health care provider with multiple locations in the Eastern District of Missouri. Victim 3 utilized "protected computers," as that term is defined in Title 18, United States Code, Section 1030(e)(2), in interstate and foreign commerce to, among other

things, store and transmit sensitive and personally identifying information about patients, including billing and medical records.

4. Victim 4 was a certified public accountant business located in St. Louis, Missouri, in the Eastern District of Missouri. Victim 4 utilized "protected computers," as that term is defined in Title 18, United States Code, Section 1030(e)(2), in interstate and foreign commerce to, among other things, store and transmit sensitive and personally identifying information about clients, including sensitive financial records.

5. Victim 5 was a health care provider located in Athens, Georgia. Victim 5 utilized "protected computers," as that term is defined in Title 18, United States Code, Section 1030(e)(2), in interstate and foreign commerce to, among other things, store and transmit sensitive and personally identifying information about patients, including billing and medical records.

COUNT 1

18 U.S.C. § 371 - Conspiracy

THE GRAND JURY CHARGES THAT:

6. Paragraphs 1 through 5 are re-alleged and incorporated as if set forth here in their entirety.

7. From in or about February 2016, and continuing thereafter until in or about June 2017, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

did knowingly and willfully conspire and agree with others, both known and unknown to the Grand Jury, to commit offenses against the United States, namely:

a. Knowingly transferring, possessing, and using, 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), that is Title 18, United States Code, Section 1030(a)(7) (extortion involving computers), in violation of Title 18, United States Code, Section 1028A.

b. Intentionally accessing a computer without authorization, and thereby obtaining information from any protected computer for purposes of private financial gain, with the value of the information obtained exceeding $5,000, and the offense being committed in furtherance of a criminal act in violation of the laws of the United States, specifically Title 18, United States Code, Section 1030(a)(7) (extortion involving computers), in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B); and

c. Knowingly and with intent to extort from persons money and other things of value, transmitting in interstate and foreign commerce communications containing demands and requests for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Section 1030(a)(7)(C) and (c)(3)(A).

Manner and Means of the Conspiracy

8. The manner and means used to accomplish the objectives of the conspiracy included, among others, the following:

a. It was part of the conspiracy for the participants to remotely access the protected computer networks of Victims 1–5 without authorization by

using, among other things, compromised Remote Desktop Protocol Credentials.

b. It was part of the conspiracy for the participants to obtain personally identifying and sensitive records, including means of identification and other information, from the protected computer networks of Victims 1–5.

c. It was part of the conspiracy for the participants to offer the compromised records and information for sale on criminal forums and marketplaces.

d. It was part of the conspiracy for the participants to use email and telephone accounts to send messages containing threats to release the victim companies' compromised records and information unless the victim companies met the conspirators' extortionate demands for payment in bitcoin and/or wire transfer.

Overt Acts

9. It was further part of the conspiracy that the following acts in furtherance of and to effect the objects of the above-described conspiracy were committed in the Eastern District of Missouri and elsewhere:

a. WYATT registered a telephone account (Account A) used in the course of the conspiracy to register a virtual private network account and Twitter account used by conspirators to conduct the scheme.

b. WYATT registered a telephone account (Account B) used in the course of the conspiracy to send threatening and extortionate text messages to victims.

c. WYATT registered a virtual private network account used in the course of the conspiracy to access a PayPal account used by conspirators to conduct the scheme.

d. WYATT accessed a PayPal account used by conspirators to attempt to steal funds from Victim 2.

e. On or about June 10, 2016, one or more conspirators sent an email to Victim 1 using the pseudonym "Marco Weebler" and the email address m**********2@gmail.com. The email included PII obtained from Victim 1's compromised network and demanded payment in bitcoin in exchange for not releasing the compromised records and information.

f. On or about June 27, 2016, one or more conspirators sent an email to Victim 5 using the m**********2@gmail.com email account. The email included PII obtained from Victim 5's compromised network and demanded payment in bitcoin in exchange for not releasing the compromised records and information.

g. On or about June 28, 2016, one or more conspirators sent an email to Victim 5 using the m**********2@gmail.com email account again threatening to release the compromised records unless Victim 5 paid the bitcoin ransom.

h. On or about July 10, 2016, one or more conspirators sent an email to Victim 3 using the m**********2@gmail.com address, stating that Victim 3's network had been hacked and demanding payment in bitcoin in exchange

for not releasing compromised PII and other records. The email included PII obtained from Victim 3's network.

i. On or about July 12, 2016, one or more conspirators sent an extortionate text message from a phone account registered by WYATT (Account B) to Victim 3, stating that the deadline to meet the extortion demands was midnight of that night.

j. On or about July 17, 2016, one or more conspirators sent an email to Victim 4 from the m**********2@gmail.com account. This email warned that Victim 4 was not paying quickly enough, and that the co-conspirators were "considering punishment by purging some of your data and possibly leaking some of this entire fiasco."

k. Also on or about July 17, 2016, one or more conspirators sent a threatening voicemail to Victim 4 from a phone account registered by WYATT (Account B).

l. Also on or about July 17, 2016, one or more conspirators sent threatening text messages from a phone account registered by WYATT (Account B) to the daughter of one of the owners of Victim 1. These included texts stating, "hi…you look peaceful…by the way did your daddy tell you he refused to pay us when we stole his company files in 4 days we will be releasing for sale thousands of patient info. Including yours…". A second text stated "hmm maybe your [sic] just a dumb rich girl who dosent [sic] understand the dangers here…im gonna try Chels…she may have an iq…stay hot

Babe..." A third stated, "...could be averted if daddy wasn't such a fkin idiot. Firstly for not taking care of his patients...then for not paying when he had a small problem."

m. On or about July 23, 2016, one or more conspirators sent an email to Victim 4 from the m**********2@gmail.com account. This email threatened to begin "calling your clients one by one" unless the company paid the ransom.

n. On or about July 26, 2016, one or more conspirators sent an email to Victim 5 from the m**********2@gmail.com account. This email demanded payment via wire transfer to accounts controlled by WYATT.

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

COUNT 2

18 U.S.C. § 1028A(a)(1), (b), (c)(4))– Aggravated Identity Theft

THE GRAND JURY FURTHER CHARGES THAT:

10. The factual allegations contained in Paragraphs 1 through 5 are re-alleged and incorporated as if set forth here in their entirety.

11. On or about June 10, 2016, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), specifically Title 18, United States Code, Section 1030(a)(7) (extortion involving computers), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, personally identifying information about persons with

records held by Victim 1, knowing that said means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1), (b), (c)(4) and 2.

COUNT 3

18 U.S.C. § 1028A(a)(1), (b), (c)(4) – Aggravated Identity Theft

THE GRAND JURY FURTHER CHARGES THAT:

12. The factual allegations contained in Paragraphs 1 through 5 are re-alleged and incorporated as if set forth here in their entirety.

13. On or about July 10, 2016, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), specifically Title 18, United States Code, Section 1030(a)(7) (extortion involving computers), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, personally identifying information about persons with records held by Victim 3, knowing that said means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1), (b), (c)(4) and 2.

COUNT 4

18 U.S.C. § 1030(a)(7)(C) & (c)(3)(A) – Threatening to Damage Protected Computer

THE GRAND JURY FURTHER CHARGES THAT:

14. The factual allegations contained in Paragraphs 1 through 5 are re-alleged and

incorporated as if set forth here in their entirety.

15. On or about June 10, 2016 and July 17, 2016, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

with intent to extort from a person money and things of value, did transmit in interstate or foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, that is, WYATT sent email and text messages threatening to release data stolen from Victim 1's protected computer unless Victim 1 paid a bitcoin ransom.

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

COUNT 5

18 U.S.C. § 1030(a)(7)(C) & (c)(3)(A) – Threatening to Damage Protected Computer

THE GRAND JURY FURTHER CHARGES THAT:

16. The factual allegations contained in Paragraphs 1 through 5 are re-alleged and incorporated as if set forth here in their entirety.

17. On or about July 10, 2016 and July 12, 2016, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

with intent to extort from a person money and things of value, did transmit in interstate or foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, that is, WYATT sent email and text messages threatening to release data stolen obtained

from Victim 3's protected computer unless Victim 3 paid a bitcoin ransom.

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

COUNT 6

18 U.S.C. § 1030(a)(7)(C) & (c)(3)(A) – Threatening to Damage Protected Computer

THE GRAND JURY FURTHER CHARGES THAT:

18. The factual allegations contained in Paragraphs 1 through 5 are re-alleged and incorporated as if set forth here in their entirety.

19. On or about July 17 and July 23, 2016, in the Eastern District of Missouri and elsewhere, the defendant,

NATHAN WYATT,

with intent to extort from a person money and things of value, did transmit in interstate or foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, that is, WYATT sent an email message to Victim 4 threatening to release data stolen obtained from Victim 4's protected computer unless Victim 4 paid a bitcoin ransom.

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

Forfeiture Allegation

(18 U.S.C. §§ 982(a)(2)(B), 1030(i))

20. The factual allegations in Paragraphs 1 through 5 are re-alleged and incorporated as if fully set forth here for the purpose of alleging forfeitures pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i).

21. Upon conviction of the offenses in violation of 18 U.S.C. § 1030 set forth in Counts Four through Six of this Indictment, the defendant, NATHAN WYATT, shall forfeit to the United States of America the following:

(a) Pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense; and

(b) Pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

23. Pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b) and 1030(i), the defendant, NATHAN WYATT, shall forfeit substitute property, up to the value of the forfeitable property, or any portion thereof, if by any act or omission of the defendant the forfeitable property:

(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.

DATED:_____

A TRUE BILL

_____
FOREPERSON

JEFFREY B. JENSEN
United States Attorney

_____
LAURA-KATE BERNSTEIN
Trial Attorney
United States Department of Justice