FILED
IN CLERK'S OFFICE
US DISTRICT COURT E.D.N.Y.
* SEPTEMBER 23, 2026 *
BROOKLYN OFFICE

NJM/JAS:AFM/LRO/VR/BZM
F. #2022R00375

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

ZOHAR PINHASI,
also known as "Zack Silver" and
"Zack Green,"

Defendant.

----------X

INDICTMENT

Cr. No. 26-CR-271
(T. 18, U.S.C., §§ 981(a)(1)(c), 1343, 1349, 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461)

Judge Ramon E. Reyes, Jr.
Magistrate Judge Taryn A. Merkl

THE GRAND JURY CHARGES:

INTRODUCTION

At times relevant to this Indictment, unless otherwise noted:

I. Definitions

1. "Encryption" was the translation of data into a secret code, rendering it effectively inaccessible to the user. To access encrypted data, a user needed a password, commonly referred to as a "decryption key" or "decryptor," that enabled the user to decrypt the data.

2. "Malware" was a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and take other unauthorized action on a computer system.

3. "Ransomware" was a type of malware that infected a computer or computer network and encrypted some or all of its data. Distributors of ransomware typically extorted the user of the encrypted computer(s) by demanding that the user pay a ransom (often in

cryptocurrency) to receive a decryption key and recover the encrypted data. As part of the extortion scheme, cybercriminals typically offered to "unlock" (or decrypt) a small subset of encrypted files from the victim's computer to demonstrate that the perpetrator was capable of unlocking the encrypted data, thereby inducing the victim to pay the ransom.

II. The Defendant

4. The defendant ZOHAR PINHASI was a citizen of Israel and of the United States, and a resident of Florida. PINHASI used various aliases, including "Zack Silver" and "Zack Green."

5. The defendant ZOHAR PINHASI owned and operated MonsterCloud LLC ("MonsterCloud"), a purported ransomware remediation company headquartered in Florida. PINHASI served as MonsterCloud's Chief Executive Officer and oversaw MonsterCloud's operations. PINHASI's responsibilities included managing other MonsterCloud employees, setting the prices charged to MonsterCloud clients, and communicating with cybercriminals on behalf of MonsterCloud.

6. The defendant ZOHAR PINHASI had multiple co-conspirators, individuals whose identities are both known and unknown to the Grand Jury, including MonsterCloud employees and contractors, who assisted PINHASI in carrying out the scheme described below.

III. The Scheme to Defraud

A. Overview of the Scheme

7. Between approximately June 1, 2018 and June 30, 2023, the defendant ZOHAR PINHASI held out MonsterCloud as a ransomware remediation company with "proprietary tools" to recover data encrypted by ransomware. PINHASI discouraged prospective

clients from making ransom payments and falsely represented that MonsterCloud could recover encrypted files without paying cybercriminals using specialized, proprietary technology.

8. For example, the defendant ZOHAR PINHASI solicited prospective clients through the MonsterCloud website, which contained language dissuading prospective clients from making ransom payments to cybercriminals and falsely suggesting that MonsterCloud had proprietary technology that could recover encrypted data without making ransom payments. Among other things, MonsterCloud's website proclaimed that "our team specializes in helping businesses recover their data without succumbing to ransom demands," and boasted that MonsterCloud used "advanced decryption techniques and cutting-edge technology." The website also cautioned prospective clients that paying ransoms to cybercriminals would not guarantee the recovery of any data, might encourage subsequent cyberattacks, and rewarded illegal behavior. Multiple clients engaged MonsterCloud specifically because those clients did not want to pay a cybercriminal and would not have authorized any payment to a cybercriminal. Many of MonsterCloud's clients initially consulted MonsterCloud by submitting a request on the "Contact Us" section of MonsterCloud's website, indicating that these clients had also reviewed the site's content.

9. In fact, neither the defendant ZOHAR PINHASI nor his co-conspirators had specialized or proprietary technology to decrypt data. Rather, PINHASI contacted and paid the cybercriminals who had victimized MonsterCloud's clients, in exchange for a decryption key (or multiple description keys) that MonsterCloud employees then used to decrypt each client's files. PINHASI typically charged MonsterCloud's clients a fee that was substantially higher—sometimes multiple times higher—than the ransom that MonsterCloud paid to the cybercriminals.

B. MonsterCloud's Ransomware Recovery Process

10. MonsterCloud's purported ransomware recovery services proceeded in two stages: (i) an "initial" or "analysis" phase, with a money-back guarantee, during which MonsterCloud would provide what the defendant ZOHAR PINHASI called "recovery proofs" to the prospective client; and (ii) a second, more expensive phase, during which MonsterCloud would contract to recover the client's remaining data.

11. MonsterCloud employed a "Controller" ("Employee-1"), an individual whose identity is known to the Grand Jury, who was responsible for client intake and collected basic information about the prospective client and the ransomware attack. Many prospective MonsterCloud clients—businesses and organizations experiencing ransomware attacks—were unable to meaningfully operate, or were otherwise suffering substantial financial losses, as a result of the attacks.

12. After collecting information from the prospective client, Employee-1 shared the information with the defendant ZOHAR PINHASI, who directed Employee-1 to quote the client a price for the analysis phase. The quote for the analysis phase was typically between approximately $2,500 and $10,000.

13. Thereafter, the defendant ZOHAR PINHASI, or another MonsterCloud employee, obtained from the prospective client a copy of the cybercriminal's ransom note, which typically included a ransom demand and instructions for contacting the cybercriminal. PINHASI or another MonsterCloud employee would also obtain a selection of sample encrypted files (usually two) from the client's system. After the analysis phase, PINHASI then provided the decrypted samples to the prospective client as "recovery proofs," representing that MonsterCloud was able to decrypt the client's files. However, in many instances, PINHASI had actually shared

the sample files with the cybercriminal and obtained decryption samples without informing or revealing to the client that MonsterCloud had not employed any proprietary technology.

14. MonsterCloud's success in its analysis phase reinforced the defendant ZOHAR PINHASI's false claims regarding MonsterCloud's proprietary decryption technology and induced clients to contract for "full" ransomware recovery—a more expensive service, costing up to two or more times the ransom.

15. MonsterCloud's fees were generally substantially higher than the amounts that cybercriminals charged as ransoms. For instance, in or around August 2023, the defendant ZOHAR PINHASI made a ransom payment of approximately $8,200 to a cybercriminal and charged the client approximately $150,000—nearly twenty times the cost of the ransom demand. Similarly, in or around October 2021, PINHASI made a ransom payment of approximately $236,000 and charged the client approximately $380,000—a mark-up of nearly $150,000. PINHASI typically did not disclose to MonsterCloud's clients that ransom payments had been made or the difference between MonsterCloud's fees and the ransom payment.

16. MonsterCloud's written contracts with some of its clients for full ransomware recovery services represented that, on occasion, MonsterCloud *might* communicate with or pay cybercriminals. For instance, certain of MonsterCloud's contracts provided that MonsterCloud would contact a cybercriminal "only once all possible means of directly decrypting Client's files have been exhausted." In fact, dealing with cybercriminals was generally the defendant ZOHAR PINHASI's first step in accessing encrypted files; it was the typical way PINHASI obtained "recovery proofs," and it was the standard way by which PINHASI obtained decryption keys.

17. Throughout the ensuing recovery process, the defendant ZOHAR PINHASI falsely represented that MonsterCloud had specialized methods of decrypting ransomware, which it could not disclose because they were "trade secrets" involving "proprietary means and methods." In fact, PINHASI had no specialized technical method for decrypting files.

18. The defendant ZOHAR PINHASI generally did not disclose, or permit other MonsterCloud employees to disclose, to MonsterCloud clients that MonsterCloud paid cybercriminals for decryption keys. For example, PINHASI directed MonsterCloud employees and contractors to use the term "recovery tool" instead of "decryptor."

19. MonsterCloud's website included "testimonials" and other promotional content, including from at least one compensated spokesperson, as a means of marketing MonsterCloud's services. In May 2019, one such spokesperson—an individual who had provided a paid testimonial for the MonsterCloud website—contacted the defendant ZOHAR PINHASI with questions about PINHASI's business practices and truthfulness. Among other things, the spokesperson asked PINHASI whether MonsterCloud actually had any proprietary software that would allow MonsterCloud to decrypt encrypted data. PINHASI responded: "MonsterCloud doesn't hold any Proprietary technology [to] decrypt the ransomware data," adding that PINHASI would "explain further in [] phone conversations."

20. Over the course of the scheme, the defendant ZOHAR PINHASI and his co-conspirators facilitated dozens of ransom payments to cybercriminals under the guise of ransomware remediation. In total, PINHASI paid more than approximately $8 million in ransom payments to cybercriminals extorting MonsterCloud clients, and in many cases did not inform or consult the clients before doing so. Hundreds of companies around the United States and Canada

collectively paid PINHASI and MonsterCloud more than $19 million for MonsterCloud data recovery and remediation services. Many of these companies, including at least two with offices in the Eastern District of New York, paid a premium based on PINHASI's false representations of MonsterCloud's proprietary decryption abilities, and were never informed that MonsterCloud paid the ransom to the cybercriminals.

IV. The Victims

21. The defendant ZOHAR PINHASI and his co-conspirators defrauded numerous victims ("MonsterCloud Victims") around the United States. MonsterCloud Victims were typically in the midst of responding to a ransomware attack that had encrypted victim files with malware in an attempt to extort a ransom payment in exchange for a decryption key. Examples of MonsterCloud Victims, entities whose identities are known to the Grand Jury, are described below:

(a) Victim 1, an entity the identity of which is known to the Grand Jury, was a company in the home decor industry located in the Eastern District of New York.

(b) Victim 2, an entity the identity of which is known to the Grand Jury, was a company in the display manufacturing industry located in the Eastern District of New York.

COUNT ONE
(Conspiracy to Commit Wire Fraud)

22. The allegations contained in paragraphs one through 21 are realleged and incorporated as if fully set forth in this paragraph.

23. From at least on or about June 1, 2018, and continuing through on or about June 30, 2023, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendant, ZOHAR PINHASI, also known as "Zack Silver" and "Zack

Green," together with others known and unknown to the Grand Jury, did knowingly and intentionally conspire to devise a scheme and artifice to defraud and obtain money from one or more individuals and entities, by means of one or more materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, transmit and cause to be transmitted, by means of wire communications in interstate commerce, one or more writings, signs, signals, pictures, and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online and telephonic communications and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNTS TWO AND THREE
(Wire Fraud)

24. The allegations contained in paragraphs one through 21 are realleged and incorporated as if fully set forth in this paragraph.

25. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendant, ZOHAR PINHASI, also known as "Zack Silver" and "Zack Green," together with others known and unknown to the Grand Jury, did knowingly and intentionally devise a scheme and artifice to defraud the victims set forth, and to obtain and attempt to obtain money, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, as set forth below:

COUNT	APPROXIMATE DATE	VICTIM	WIRE TRANSMISSION
TWO	4/26/2021	VICTIM 1	A wire transfer in the amount of approximately $175,000 sent from VICTIM 1, located within the Eastern District of New York, to PINHASI's bank account, maintained in Florida
THREE	8/2/2021	VICTIM 2	A telephone call between a representative of VICTIM 2, located within the Eastern District of New York, and PINHASI, located in Florida

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION

26. The United States hereby gives notice to the defendant that, upon his conviction of any of the offenses charged herein, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offenses.

27. 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 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 intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

A TRUE BILL

/s/
FOREPERSON

By David Pitluck, Assistant U.S. Attorney
JOSEPH NOCELLA, JR.
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK