UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA v. JUAN RICARDO PALACIO ESCOBAR, Defendant.	Cr. No. 1:26-cr-00096-MRD-RLA In violation of 18 U.S.C. § 1343

INDICTMENT

The Grand Jury charges that:

Overview and General Allegations

At all times relevant to this Indictment:

1. Company A was a Florida-registered LLC that operated as a ransomware response company registered in or around October 2020.

2. Defendant JUAN RICARDO PALACIO ESCOBAR ("PALACIO") and Individual 1 were partners and co-founders of Company A. PALACIO was listed as the Manager of Company A in the Florida business filing and was the Chief Technology Officer of Company A. Individual 1 was the Managing Director of North America for Company A. PALACIO and Individual 1 both resided in Colombia but frequently traveled to the United States.

3. Company A held itself out as providing data recovery services to victims of ransomware attacks. Specifically, in written proposals provided to potential clients, it offered "advanced cryptographic tools to restore 100% of data, servers, systems to their original format and integrity."

4. Company A's website also urged potential customers not to pay ransoms. The website said, "Do not pay the ransom!" In the Company's FAQs on its website, it warned

potential customers of the "serious risks" of paying the ransom. It stated that paying ransom "does not guarantee safe file recovery and may expose you to further extortion attempts;" that "there is no guarantee attackers will provide working decryption keys;" and that "in many cases, organizations that pay still experience secondary attacks once criminals know the victim is willing to pay." Company A's website also warned potential customers that "ransom payments may also violate regulatory or insurance policies."

5. Company A's website also stated that its "decryption experts rely on ransomware removal tools and proprietary, cryptography-based decryptor software" to restore victims' databases and files.

6. As part of its ransomware recovery services, Company A charged customers an initial fee for an assessment that it represented included: malware and ransomware identification; detailed technical report of origin and type of damages; professional ransomware removal; the use of forensic tools to eliminate malware from the system; a recovery cost estimate; an estimated time of recovery; and a 100% data recovery guarantee.

7. Company A explicitly stated to victims that it did not engage with threat actors or make ransom payments. However, rather than using a proprietary technical solution to decrypt encrypted files and recover its customers' data, Company A did in fact engage with threat actors and pay ransoms to obtain decryption keys.

Definitions and Technical Background

8. Ransomware is a form of cyber-attack by which a third party (the "cyber attacker" or "threat actor") covertly installs malicious software ("malware") on one or more computer systems, which encrypts some or all of their data. Distributors of ransomware typically demand a ransom payment, typically in cryptocurrency, in exchange for a decryption key that allows the

victim to decrypt, or restore, the encrypted data. Cyber attackers often operate as part of groups or organizations that are known within the cybersecurity community and use specific types of malware or ransomware. Different types of ransomware require different decryption keys

9. Ransomware threat actors (hereafter "threat actors") typically leave a victim identification number or alphanumeric string in the ransom note left on the victim's encrypted computer or network. The identification number is for the victim to provide to the threat actors to identify themselves.

COUNTS 1-3

(Wire Fraud – 18 U.S.C. § 1343)

Scheme and Artifice to Defraud

10. The allegations contained in paragraphs 1 through 9 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

11. Beginning in approximately October 2020 and continuing through June 2026, in the District of Rhode Island and elsewhere, the defendant

JUAN RICARDO PALACIO ESCOBAR

knowingly devised and intended to devise a scheme and artifice to defraud, and to obtain money and property from victims of ransomware attacks, by means of false and fraudulent pretenses, representations and promises.

Object of the Scheme To Defraud

12. The object of the scheme to defraud was for PALACIO to unlawfully enrich himself and Company A by fraudulently representing to victims of ransomware attacks that Company A had sophisticated decryption tools to unlock their data without paying a ransom to

the threat actors, thereby inducing them to hire his company, and then obtaining payments from victims of ransomware attacks that were in excess of the ransom PALACIO paid to ransomware actors to obtain the decryption key for the victim data.

Manner and Means of the Scheme to Defraud

13. It was part of the scheme and artifice to defraud that PALACIO used Company A to intentionally misrepresent to companies in the United States who were victims of ransomware attacks that Company A could help them decrypt and recover their files without paying a ransom.

14. It was further part of the scheme and artifice to defraud that, contrary to the representations made to victims of ransomware attacks, PALACIO negotiated with and paid ransoms to ransomware actors.

15. It was further part of the scheme and artifice to defraud that a representative of Company A falsely told a software consulting company based in Kansas that was a victim of a a ransomware attack on or about January 11, 2024, that it could recover the victim's network without paying the ransom. After discussions with Individual 1, that victim hired Company A and paid $720,000 for its recovery services to PALACIO's bank account ending in 9746.

16. It was further part of the scheme and artifice to defraud that Individual 1 provided a personally signed "Recovery Certificate" to the victim on behalf of Company A, which stated in part:

> "As requested, we hereby certify that our Company has never contacted, nor entered negotiations with anyone about the agreement or settlement of any fee or ransom payment concerning the incident affecting our client [VICTIM 1] in relation to the [IDENTIFIED RANSOMWARE GROUP] attack suffered on the 12th of February.
>
> Our company specializes in ransomware data recovery solutions for corporate clients. Our cryptography experts use proprietary tools and algorithms to achieve 100% data recovery, all backed by a success rate of over 99%. We never promote, intermediate or pay ransom to threat actors on behalf of our clients."

17. It was further part of the scheme and artifice to defraud that despite these representations, on or about January 20, 2024, PALACIO did pay a ransom to the threat actors of approximately $445,000 in Bitcoin in exchange for the decryption key for Victim 1's data.

18. It was further part of the scheme and artifice to defraud that Company A told another victim of a ransomware attack in or around August 2025, that Company A could help restore the data and would not pay the ransom or negotiate with the threat actors, but despite these representations PALACIO paid the ransom to obtain a decryption key.

19. It was further part of the scheme and artifice to defraud that Company A told victims it could decrypt and recover their network without paying the ransom or negotiating with the threat actor, and that it could create a decryption key without negotiating or making a ransom payment.

20. It was further part of the scheme and artifice to defraud that Company A sent invoices to a victim that included charges for a diagnostic service, a vulnerability analysis report, data recovery including the "use of tools, professional reconstruction and engineering hours to execute the repair and extraction of data affected," as well as an invoice for "recovery service" that included "the use of forensic servers, decryption tools, engineering hours to execute the recovery of data affected by a ransomware attack," when in fact Company A did not perform those services and PALACIO paid the ransom.

21. It was further part of the scheme and artifice to defraud that PALACIO misled his customers to believe he was not paying the ransom while in actuality he used multiple electronic accounts to negotiate with ransomware actors about the "best price" for a decryption key.

Execution of the Scheme to Defraud

22. In April of 2025, a Rhode Island-based security company that was the victim of a ransomware attack paid Company A a fee of $1,250 to conduct an initial assessment of its encrypted files. On or about April 26, 2025, Company A sent a proposal to the victim that stated that it would use 354 "forensic servers," including 350 servers for "calculations," 2 servers for "key extraction," and 2 servers for "key creation and decryption." Company A further claimed that the scope of work included "reverse engineering," "forensic reconstruction of data and cryptography processes," engineering hours to prepare decryption tools and to test and run recovery process, and "24/7 on-going technical support to quick recovery." Company A told the Rhode Island victim it would cost $314,150 to recover its encrypted data.

23. In June 2026, a fictitious Rhode-Island-based victim company (Company 1) represented by an Undercover Employee ("UCE") of the Federal Bureau of Investigation (FBI) contacted Company A and posed as a victim of a ransomware attack. The FBI, additionally acting as a fictitious ransomware group represented to Company A by an FBI Online Covert Employee (FBI OCE), encrypted multiple files on a computer owned by Company 1 and left a ransom note with contact information and a unique victim identification number.

24. During an initial meeting on or about June 8, 2026, and in discussions after that date, Company 1 told Company A that it did not want to pay the ransom. Company A responded to Company 1 that it did not negotiate or make ransom payments to threat actors. Company A also told Company 1 it would charge a fee of $2,750 to conduct an initial forensic assessment.

25. On or about June 10, 2026, Company A, using a remote access and support program, conducted the purported forensic assessment on Company 1's system.

26. On or about June 16, 2026, Company 1 and Company A signed a contract stating that Company A would provide the following services: "IT Data recovery consists of the use of forensic servers, decryption tools, engineering hours to execute the recovery of data affected by a ransomware attack." The contract further stated that, "Company A will use proprietary decryption tools in data recovery only for all data evaluated by our engineers, delivering files, databases, and decrypted data in their original structure, naming, and order, not included any corrupt or damaged files."

27. Attachment D of the contract outlined the fees and payment schedule, and further described the service as "entail[ing] advanced reverse engineering and cryptoanalysis, custom algorithm development, intelligent brute-force and heuristic attacks, proven key extraction methodologies, and digital forensic techniques to structurally decrypt and restore encrypted files, databases, and systems to their original organization, naming, and order, excluding any corrupted or damaged files."

28. These representations were false. On or about June 14, 2026, PALACIO contacted the FBI OCE, acting as the ransomware threat actor, from a Proton Mail account and referenced the unique victim identification number in the ransom note left among Company 1's files. PALACIO requested the "lowest possible price for the decryptor." In response, the FBI OCE attacker proposed .2 Bitcoin, worth approximately $13,000 at the time.

29. On or about June 16, 2026, Individual 1 informed Company 1 that the diagnostic assessment was successful and the cost to decrypt the files would be $13,260. The FBI, posing as Company 1, paid $13,260 to Company A's U.S. bank account to complete decryption of their files.

30. On or about June 17, 2026, PALACIO, using a Proton Mail email account, attempted to negotiate with the FBI OCE to reduce its ransom demand to $4,000 for purchase of the decryption tool, thereby increasing the profit Company A would make on the transaction. The FBI OCE and PALACIO ultimately agreed to a ransom of $6,000 for the purchase of the decryption tool. In response to the FBI OCE's request to provide a Google account to receive the decryption tool, PALACIO provided Google email address using the name erickrmiller10, which was an account owned and used by PALACIO.

31. On or about June 19, 2026, PALACIO paid the FBI OCE approximately .0948 BTC ($6,003 at the time) for the decryption tool.

32. Approximately five days after the FBI OCE provided the decryption tool to PALACIO, Individual 1 confirmed to Company 1 their files were decrypted. The initial $2,750 diagnostic fee plus the full fee of $13,260 was a total of $16,010, less approximately $6,000 paid to the OCE, resulted in Company A ultimately receiving approximately $10,010 in profit.

33. On or about the dates set forth below, in the District of Rhode Island and elsewhere, for the purpose of executing the aforementioned scheme and artifice to defraud to obtain money by means of materially false and fraudulent pretenses, representations and promises, and attempting to do so, the defendant,

JUAN RICARDO PALACIO ESCOBAR

did knowingly transmit and cause to be transmitted by means of wire communication in interstate commerce between Rhode Island and locations outside of Rhode Island, certain writings, signs, signals and sounds, to wit the following wire transmissions:

Count	**Date (on or about)**	**Wire Transmission**
1	April 26, 2025	An email proposal sent by PALACIO to a victim of a ransomware attack located in Rhode Island.

2	June 8, 2026	A wire transfer in the amount of approximately $2,750 sent from Company 1, located within the District of Rhode Island, to PALACIO's bank account ending in 9746, maintained in Florida.
3	June 16, 2026	A wire transfer in the amount of approximately $13,260 sent from Company 1, located within the District of Rhode Island, to PALACIO's bank account ending in 9746, maintained in Florida.

All in violation of Title 18, United States Code, Section 1343.

FORFEITURE ALLEGATIONS

(Wire Fraud)

34. The allegations contained above are realleged and incorporated by reference as though fully set forth herein.

35. The Grand Jury further charges that: upon conviction of one or more of the offenses charged in Counts One through Three of this Indictment in violation of 18 U.S.C. § 1343, Defendant JUAN RICARDO PALACIO ESCOBAR shall forfeit to the United States of America, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) all right, title and interest in any and all property, real or personal, that constitutes, or is derived from, proceeds traceable to the commission of the offenses, including but not limited to:

a. all right, title, and interest of the defendant in the real property located at 16045 NW 87th Ct, Miami Lakes, FL 33018, having been purchased by PALACIO on December 1, 2020, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

b. all right, title, and interest of the defendant in the real property located at 695 Whistling Straits Blvd, Davenport, FL 33896, having been purchased by

Ptolomeo Investments, a Florida-registered LLC owned by PALACIO on October 1, 2021, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

c. all right, title, and interest of the defendant in the real property located at 301 Altara Ave Unit 701, Coral Gables, FL 33146, having been purchased by Ptolomeo Investments, a Florida-registered LLC owned by PALACIO on June 1, 2022, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

d. all right, title, and interest of the defendant in the real property located at 301 Altara Ave Unit 805, Coral Gables, FL 33146, having been purchased by Ptolomeo Investments, a Florida-registered LLC owned by PALACIO on September 1, 2023, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

e. all right, title, and interest of the defendant in the real property located at 1400 Biscayne Blvd, Unit 1801, Miami, FL 33132, having been purchased by Titania Investments, a Florida-registered LLC owned by PALACIO on August 1, 2026, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

f. all right, title, and interest of the defendant in the real property located at 1400

Biscayne Blvd, Unit 3803, Miami, FL 33132, having been purchased by Inversiones Tridente Corp., a Florida corporation owned by PALACIO on August 1, 2026, the acquisition, maintenance, improvement, and/or equity of which was funded, in part, by proceeds traceable to the wire fraud scheme charged in Counts One through Three;

g. the bank account ending in 9746, held in the name of Digital Recovery Group at Citibank, NA that was opened on or around June 5, 2019, with PALACIO as the sole authorized signor;

h. the bank account ending in 9254 held in the name of Reputation Up, LLC, at Citibank, NA, that was opened on or around June 19, 2019, with PALACIO as the sole authorized signor;

i. the bank account ending in 8091 held in the name of PALACIO, at Citibank, NA, that was opened on or around August 29, 2019, with PALACIO as the sole authorized signor;

j. the bank account ending in 4792 held in the name of Ptolomeo Investments LLC, at Citibank, NA, that was opened on or around September 14, 2021, with PALACIO as the sole authorized signor;

k. the bank account ending in 8226, held in the name of Digital Recovery Group at Wells Fargo, that was opened on or around September 13, 2021, with PALACIO as the sole signor.

36. If any of the property described in paragraph 35 hereof as being forfeitable pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(A) and 982(a)(7), and Title 28, United States Code, Section 2461(c), as a result of any act or omission of PALACIO:

a. cannot be located upon the exercise of due diligence;

b. has been transferred to, 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,

the United States shall be entitled to forfeiture of substitute property under 21 U.S.C. § 853(p) as incorporated by 18 U.S.C. § 982(b)(1) and 28 U.S.C. 2461(c). It is further the intention of the United States to seek a money judgment as necessary to cover all fraud losses.

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A) and 982(a) (7), and Title 28, United States Code, Section 2461(c).

A TRUE BILL:

[redacted]

Grand Jury Foreperson

Date: 11/18/2026

JULIANNE KLEIN
Assistant U.S. Attorney

LEE H. VILKER
Assistant U.S. Attorney

CHRISTEN GALLAGHER
Trial Attorney
Computer Crime and Intellectual Property Section

Stacey A. Erickson

STACEY A. ERICKSON
Assistant U.S. Attorney
Criminal Division Chief