Ransomware's Inside Job: How Two Men Made Millions Extorting U.S. Companies While They Worked For Cybersecurity Vendors

Ryan Clifford Goldberg and Kevin Tyler Martin worked as affiliates for ALPHV BlackCat, demanding ransoms while they worked for Cybersecurity companies.

Ryan Clifford Goldberg and Kevin Tyler Martin worked for a Ransomware company but they also helped run one of the most damaging ransomware operations to hit American businesses in recent years.

During their time at the company, they also worked for ALPHV BlackCat, a ransomware strain that terrorized hundreds of companies worldwide starting in late 2021.

The Criminal Franchise

The indictment offers a window into how ransomware gangs actually operate. ALPHV BlackCat worked like a criminal franchise. Developers created and maintained the malicious software, then recruited affiliates like Goldberg and Martin to find victims and carry out attacks.

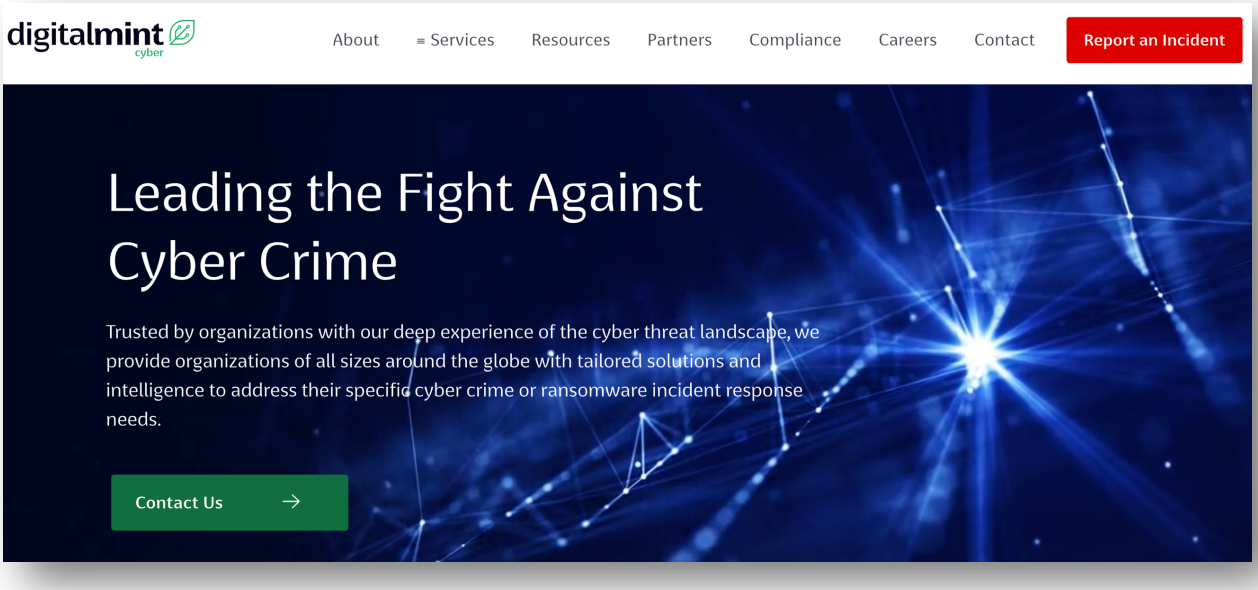
The affiliates got access to the ransomware through a password-protected panel on the dark web, customized for each affiliate's use. The two men worked with a third conspirator based in Land O'Lakes, Florida, attacking at least five companies between May 2023 and April 2025.

Their victims ranged from a Tampa medical device company to a Virginia drone manufacturer. In their most successful attack, prosecutors say, they extracted $1.27 million from the Tampa company after encrypting its servers and threatening to publish stolen data.

The Twist was They Were Employees Of Cybersecurity Companies

At the time of the attacks, they were both employees of ransomware companies.

Martin was a ransomware threat negotiator for River North-based DigitalMint at the time of the alleged conspiracy. A suspected accomplice who wasn't indicted



Ryan Clifford Goldberg, an incident response manager for the multinational company Sygnia Cybersecurity Services. Sygnia said Goldberg no longer works for the company and it “is not the target of this investigation, however we continue to work closely with law enforcement.”

How the Attacks Worked

"They would gain access to the victim's network to steal data and deploy the ransomware to encrypt data and leave a ransom note," the indictment states. Victims were then directed to the ALPHV BlackCat panel where they could negotiate with the attackers.

The Tampa medical device company attack in May 2023 shows how the scheme worked. Goldberg, Martin and their co-conspirator encrypted the company's servers and demanded roughly $10 million to decrypt the data and promise not to publish the stolen information.

The company, fearing the financial damage from lost data, paid about $1.27 million in cryptocurrency. For the attackers, it was simple math: steal the data, lock the computers, then offer a solution to the problem they created.

A String of Victims Across America

Not every attack succeeded. When the group hit a Maryland pharmaceutical company that same month, demanding a ransom to decrypt servers and keep data private, the company apparently didn't pay.

Same with a California doctor's office they attacked in July 2023, where they sought $5 million. An engineering firm in California faced a $1 million demand in October 2023. A drone manufacturer got hit with a $300,000 ransom demand in November 2023.

The ransomware attacks caused tens of millions of dollars in cryptocurrency ransom payments across all ALPHV BlackCat victims, along with major disruptions to business operations and large losses of private information. More than twenty companies in South Florida alone fell victim to ALPHV BlackCat attacks, according to prosecutors.

Read the Indictment

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

25-CR-20443-MOORE/D'ANGELO
CASE NO. _____

18 U.S.C. § 1951(a)
18 U.S.C. § 1030(a)(5)(A)
18 U.S.C. § 982(a)(2)(A)

UNITED STATES OF AMERICA

vs.

RYAN CLIFFORD GOLDBERG and
KEVIN TYLER MARTIN,

Defendants.
_____/

INDICTMENT

The Grand Jury charges:

GENERAL ALLEGATIONS

At times material to this Indictment:

1. Ransomware is malicious software that cybercriminals use to encrypt and steal data from vulnerable computer networks to extort a ransom payment in exchange for unlocking the network and/or not publishing sensitive stolen data, both of which can cause significant economic harm to a victim.

2. ALPHV – also known as BlackCat and, jointly, "ALPHV BlackCat" – was a strain of ransomware that cybercriminals used beginning in or around late 2021 to attack and extort hundreds of institutions around the world, including a university and a corporation in the Southern District of Florida that were both engaged in interstate commerce. Other ALPHV BlackCat victims included medical facilities, school districts, law firms, and financial firms. There were over twenty ALPHV BlackCat ransomware victims in the Southern District of Florida. The ransomware attacks

caused tens of millions in cryptocurrency ransom payments, major disruptions in ongoing operations, and large losses of proprietary information.

3. Most ALPHV BlackCat attacks had a similar structure. ALPHV BlackCat's "developers," who created and updated the ransomware, first recruited and vetted an "affiliate," who would identify and attack victims using the ransomware. In the ransomware context, an affiliate refers to an individual or group that is allowed to use a ransomware variant to attack victims in exchange for a payment or percentage paid to the developer or administrator of the variant. ALPHV BlackCat's developers then provided the affiliate with the ransomware through a password-protected "panel" available on the dark web and customized to that affiliate. The affiliate then gained access to the victim's network to steal data and deploy the ransomware to encrypt data and leave a ransom note. The victim was directed to the ALPHV BlackCat panel hosted on the dark web where the victim could communicate with the ransomware group to negotiate the ransom. Once the victim agreed to pay, the ALPHV BlackCat actors provided a Bitcoin or Monero cryptocurrency address for the payment. The ransom payment was often split up when received and moved into various cryptocurrency addresses through multiple transactions to obscure the source of the proceeds before it reached the point of cashing out for fiat currency.

The Defendants and Co-Conspirator 1

4. **RYAN CLIFFORD GOLDBERG** resided in Watkinsville, Georgia.

5. **KEVIN TYLER MARTIN** resided in Roanoke, Texas.

6. Co-Conspirator 1 resided in Land O'Lakes, Florida.

The Co-Conspirators' Victims

7. Victim Company 1 was a medical device company based in Tampa, Florida, that was engaged in interstate commerce.

8. Victim Company 2 was a pharmaceutical company based in Maryland that was engaged in interstate commerce.

9. Victim Company 3 was a doctor's office based in California that was engaged in interstate commerce.

10. Victim Company 4 was an engineering company based in California that was engaged in interstate commerce.

11. Victim Company 5 was a drone manufacturer based in Virginia that was engaged in interstate commerce.

COUNT 1
Conspiracy to Interfere with Interstate Commerce by Extortion
(18 U.S.C. § 1951(a))

1. The General Allegations section of this Indictment is re-alleged and incorporated by reference as though fully set forth herein.

2. From in or around May 2023, and continuing through in or around April 2025, in Miami-Dade County, in the Southern District of Florida, and elsewhere, the defendants,

RYAN CLIFFORD GOLDBERG and
KEVIN TYLER MARTIN,

did knowingly and willfully combine, conspire, confederate, and agree with each other, Co-Conspirator 1, and others, both known and unknown to the Grand Jury, to obstruct, delay, and affect commerce and the movement of articles and commodities in commerce, by means of extortion, as the terms "commerce" and "extortion" are defined in Title 18, United States Code, Sections 1951(b)(2) and (b)(3), in that the conspirators did plan to obtain cryptocurrency from

persons and companies within the United States, with their consent, not due **GOLDBERG** and **MARTIN**, and induced by fear, including fear of economic loss and harm.

PURPOSE OF THE CONSPIRACY

3. It was the purpose of the conspiracy for the defendants, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and their co-conspirators to unlawfully enrich themselves by, among other things, (a) accessing victims' networks or computers without authorization; (b) stealing victims' data; (c) installing and executing ALPHV BlackCat ransomware on victims' computers resulting in the encryption of the data on those computers; (d) extorting victims by demanding a cryptocurrency ransom in exchange for a decryption key for the encrypted data and a promise not to publicize or publish the victims' stolen data; and (e) collecting ransom payments from victims and dividing those payments among themselves and their co-conspirators.

MANNER AND MEANS OF THE CONSPIRACY

The manner and means by which **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, Co-Conspirator 1, and their co-conspirators sought to accomplish the object and purpose of the conspiracy included, among others, the following:

4. **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 accessed victims' networks or computers and deployed ALPHV BlackCat ransomware, thereby stealing victim data and encrypting data on victim computers.

5. On or about May 13, 2023, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 used ALPHV BlackCat ransomware to attack Victim Company 1. **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 encrypted Victim Company 1's servers and demanded an approximate $10,000,000 ransom payment to decrypt the affected data and in

exchange for a commitment not to publish the stolen information.

6. The attack caused Victim Company 1 to fear financial loss from the theft and encryption of their data. Victim Company 1 paid **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 a ransom in virtual currency worth approximately $1,274,000 at the time of payment.

7. In or around May 2023, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 used ALPHV BlackCat ransomware to attack Victim Company 2. **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 encrypted Victim Company 2's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. By stealing data and encrypting Victim Company 2's servers, the co-conspirators intended to cause Victim Company 2 to fear financial loss from the theft and encryption of its data.

8. In or around July 2023, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 used ALPHV BlackCat ransomware to attack Victim Company 3. **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 encrypted Victim Company 3's servers and demanded an approximate $5,000,000 ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. By stealing data and encrypting Victim Company 3's servers, the co-conspirators intended to cause Victim Company 3 to fear financial loss from the theft and encryption of its data.

9. In or around October 2023, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 used ALPHV BlackCat ransomware to attack Victim Company 4. **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 encrypted Victim Company 4's servers and demanded an approximate $1,000,000 ransom payment to decrypt the affected data and in

exchange for a commitment not to publish the stolen information. By stealing data and encrypting Victim Company 4's servers, the co-conspirators intended to cause Victim Company 4 to fear financial loss from the theft and encryption of its data.

10. In or around November 2023, **RYAN CLIFFORD GOLDBERG**, **KEVIN TYLER MARTIN**, and Co-Conspirator 1 used ALPHV BlackCat ransomware to attack Victim Company 5. **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 encrypted Victim Company 5's servers and demanded an approximate $300,000 ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. By stealing data and encrypting Victim Company 5's servers, the co-conspirators intended to cause Victim Company 5 to fear financial loss from the theft and encryption of its data.

All in violation of Title 18, United States Code, Section 1951(a).

COUNT 2
Interference with Interstate Commerce by Extortion
(18 U.S.C. § 1951(a))

1. Paragraphs 1 through 7 of the General Allegations section of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about May 13, 2023, in Miami-Dade County, in the Southern District of Florida, and elsewhere, the defendants,

RYAN CLIFFORD GOLDBERG and
KEVIN TYLER MARTIN,

did knowingly and willfully, in any way, obstruct, delay, and affect commerce and the movement of articles and commodities in commerce, by means of extortion, as the terms "commerce" and "extortion" are defined in Title 18, United States Code, Sections 1951(b)(2) and (b)(3), in that **GOLDBERG**, **MARTIN**, and Co-Conspirator 1 obtained from Victim Company 1 approximately $1,274,781.23 in cryptocurrency, with its consent, not due **GOLDBERG** and **MARTIN**, and

induced by fear, including fear of economic loss and harm, in violation of Title 18, United States Code, Sections 1951(a) and 2.

COUNT 3
Intentional Damage to a Protected Computer
(18 U.S.C. § 1030(a)(5)(A))

1. Paragraphs 1 through 7 of the General Allegations section of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about May 13, 2023, in Miami-Dade County, in the Southern District of Florida, and elsewhere, the defendants,

RYAN CLIFFORD GOLDBERG and
KEVIN TYLER MARTIN,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, that is, Victim Company 1's servers and computers, and as a result of such conduct, caused loss to one or more persons during a one-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), and 2.

FORFEITURE ALLEGATIONS

1. The allegations of this Indictment are hereby re-alleged and by this reference fully incorporated herein for the purpose of alleging forfeiture to the United States of America of certain property in which any of the defendants, **RYAN CLIFFORD GOLDBERG** or **KEVIN TYLER MARTIN** has an interest.

2. Upon conviction of a violation, or conspiracy to commit a violation, of Title 18, United States Code, Section 1951, as alleged in this Indictment, the defendants shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds

traceable to the violation to such offense, pursuant to Title 18, United States Code, Section 981(a)(1)(C).

3. Upon conviction of a violation of Title 18, United States Code, Section 1030, the defendants shall forfeit to the United States:

a. any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and/or 1030(i)(1)(B); and/or

b. any personal property used or intended to be used to commit or to facilitate the commission of such violation, pursuant to Title 18, United States Code, Section 1030(i)(1)(A).

4. If any of the property subject to forfeiture, 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;

the United States shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p).

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), and 1030(i)(1), and the procedures set forth in Title 21, United States Code, Section 853, as

incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), and Title 28, United States Code, Section 2461(c).

A TRUE BILL,

[redacted]

Foreperson

JASON A. REDING QUIÑONES
UNITED STATES ATTORNEY

THOMAS HAGGERTY
ASSISTANT UNITED STATES ATTORNEY

CHRISTEN GALLAGHER
JORGE GONZALEZ
TRIAL ATTORNEYS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA

v.

RYAN CLIFFORD GOLDBERG and
KEVIN TYLER MARTIN,

_____/
Defendants.

CASE NO.: 25-CR-20443-MOORE/D'ANGELO

CERTIFICATE OF TRIAL ATTORNEY

Superseding Case Information:
New Defendant(s) (Yes or No) ____
Number of New Defendants _____
Total number of new counts _____

Court Division (select one)
☑ Miami ☐ Key West ☐ FTP
☐ FTL ☐ WPB

I do hereby certify that:

1. I have carefully considered the allegations of the Indictment, the number of defendants, the number of probable witnesses and the legal complexities of the Indictment/Information attached hereto.
2. I am aware that the information supplied on this statement will be relied upon by the Judges of this Court in setting their calendars and scheduling criminal trials under the mandate of the Speedy Trial Act, 28 U.S.C. §3161.
3. Interpreter: (Yes or No) No
   List language and/or dialect: _____
4. This case will take 5 days for the parties to try.
5. Please check appropriate category and type of offense listed below:

(Check only one)		(Check only one)	
I	☑ 0 to 5 days	☐	Petty
II	☐ 6 to 10 days	☐	Minor
III	☐ 11 to 20 days	☐	Misdemeanor
IV	☐ 21 to 60 days	☑	Felony
V	☐ 61 days and over		

6. Has this case been previously filed in this District Court? (Yes or No) No
   If yes, Judge _____ Case No. _____
7. Has a complaint been filed in this matter? (Yes or No) Yes
   If yes, Judge Eduardo I. Sanchez Magistrate Case No. 25-MJ-03805
8. Does this case relate to a previously filed matter in this District Court? (Yes or No) No
   If yes, Judge _____ Case No. _____
9. Defendant(s) in federal custody as of September 22, 2023 - Ryan Goldberg
10. Defendant(s) in state custody as of _____
11. Rule 20 from the _____ District of _____
12. Is this a potential death penalty case? (Yes or No) No
13. Does this case originate from a matter pending in the Central Region of the U.S. Attorney's Office prior to October 3, 2019 (Mag. Judge Jared M. Strauss)? (Yes or No) No
14. Did this matter involve the participation of or consultation with Magistrate Judge Eduardo I. Sanchez during his tenure at the U.S. Attorney's Office, which concluded on January 22, 2023? No
15. Did this matter involve the participation of or consultation with Magistrate Judge Marty Fulgueira Elfenbein during her tenure at the U.S. Attorney's Office, which concluded on March 5, 2024? No
16. Did this matter involve the participation of or consultation with Magistrate Judge Ellen F. D'Angelo during her tenure at the U.S. Attorney's Office, which concluded on October 7, 2024? No

By: _____
Thomas Haggerty
Assistant United States Attorney
FL Bar No. 46136

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: KEVIN TYLER MARTIN

Case No:

Count #: 1

Conspiracy to Interfere with Commerce by Extortion (18 U.S.C. § 1951(a))

* **Max. Term of Imprisonment:** 20 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

Count #: 2

Interference with Commerce by Extortion (18 U.S.C. § 1951(a))

* **Max. Term of Imprisonment:** 20 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

Count #: 3

Intentional Damage to a Protected Computer (18 U.S.C. § 1030(a)(5)(A))

* **Max. Term of Imprisonment:** 10 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

***Refers only to possible term of incarceration, supervised release and fines. It does not include restitution, special assessments, parole terms, or forfeitures that may be applicable.**

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PENALTY SHEET

Defendant's Name: RYAN CLIFFORD GOLDBERG

Case No:

Count #: 1

Conspiracy to Interfere with Commerce by Extortion (18 U.S.C. § 1951(a))

* **Max. Term of Imprisonment:** 20 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

Count #: 2

Interference with Commerce by Extortion (18 U.S.C. § 1951(a))

* **Max. Term of Imprisonment:** 20 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

Count #: 3

Intentional Damage to a Protected Computer (18 U.S.C. § 1030(a)(5)(A))

* **Max. Term of Imprisonment:** 10 years
* **Mandatory Min. Term of Imprisonment (if applicable):** None
* **Max. Supervised Release:** Three years
* **Max. Fine:** $250,000 or twice the gross gain or gross loss for the offense

***Refers only to possible term of incarceration, supervised release and fines. It does not include restitution, special assessments, parole terms, or forfeitures that may be applicable.**