UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 25-mj-03805-Sanchez

IN RE SEALED COMPLAINT

_____/

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to October 3, 2019 (Mag. Judge Jared M. Strauss)? No

2. 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

3. 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

4. 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

Respectfully submitted,

JASON A. REDING QUIÑONES
UNITED STATES ATTORNEY

By: */s/ Thomas Haggerty*
THOMAS HAGGERTY
Assistant United States Attorney
Southern District of Florida
Fl Bar No. 46136
99 NE 4th Street
Miami, Florida 33132
Tel: (305) 961-9002
Email: thomas.haggerty@usdoj.gov

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America)
v.)
)
Ryan Clifford Goldberg,) Case No. 25-mj-03805-Sanchez
)
)
)

Defendant.

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of between May 2023 and April 2025 in the county of Miami-Dade in the Southern District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1951(a)	Conspiracy to Interfere with Commerce by Extortion;
18 U.S.C. § 1951(a)	Interference with Commerce by Extortion; and
18 U.S.C. § 1030(a)(5)(A)	Intentional Damage to a Protected Computer.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

Complainant's signature

Dominique Dawson, Special Agent FBI
Printed name and title

Attested to by the Applicant in accordance with the requirements of Fed.R.Crim.P. 4.1 by Face Time

Date: September 19, 2025

Judge's signature

City and state: Miami, Florida

Honorable Eduardo I. Sanchez, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Dominique Dawson having been duly sworn, do hereby depose and state:

AGENT BACKGROUND AND INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) having been so employed since February 2022. I am presently assigned to the Miami Field Office. As an FBI Special Agent, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7). I am empowered by law to conduct investigations of, and/or to make arrests for, offenses enumerated in Title 18 of the United States Code. I have received training at the FBI Academy in Quantico, VA where I received training in investigations and in drafting affidavits. I am currently assigned to investigate, among other things, computer intrusion incidents, malware services, cybercriminal infrastructure, and cybercriminal marketplaces. In these investigations, I have been involved in the serving and execution of arrest and search warrants.

2. This Affidavit is based on my personal investigation and investigation by others, including federal and foreign law enforcement officials whom I know to be reliable and trustworthy. The facts contained herein have been obtained by interviewing victims and examining documents obtained during the investigation and through other means. This Affidavit does not include every fact known to me about this investigation, but rather only those facts sufficient to establish probable cause.

3. Your affiant has participated in a criminal investigation into **RYAN GOLDBERG**, a United States citizen and resident of the State of Georgia who is believed to be currently in Europe, Co-Conspirator 1, a United States Citizen and resident of Florida, and Co-Conspirator 2, a United States citizen and resident of Texas. Based on the evidence gathered through this investigation, there is probable cause to believe that from in or around May 2023 through in or

around April 2025, **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2, in violation of Title 18, United States Code, Section 1951(a), did knowingly and willfully combine, conspire, confederate, and agree with each other and others, 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, Section 1951(b)(2), and to obtain cryptocurrency, from companies, with the companies' consent, wrongfully induced by the wrongful use of fear, including fear of economic harm, in violation of Title 18, United States Code, Sections 1951(a) and 2.

4. Based on the evidence gathered through this investigation, there also is probable cause to believe that **RYAN GOLDBERG** did 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 obtained cryptocurrency, from Victim 1, with Victim 1's consent, induced by the wrongful use of fear, including fear of economic harm, in violation of Title 18, United States Code, Sections 1951(a) and 2.

5. Based on evidence gathered through this investigation, there also is probable cause to believe that **RYAN GOLDBERG** did knowingly cause 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, and the offense caused loss to persons during a one-year period from the defendant's course of conduct affecting protected computers 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.

OVERVIEW OF RANSOMWARE AND ALPHV BLACKCAT

6. 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. 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 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.

7. 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.[1] The

[1] The dark web refers to a computer network designed specifically to facilitate anonymous communication over the Internet. The most common darknet network is known as the "Tor Network." In order to access the Tor Network, a user must use free, specialized Tor software which can be downloaded as an add-on to a standard web browser, as a standalone "Tor browser bundle," or as an app for a mobile device. The Tor software anonymizes Internet users' online activities by routing their communications through a globally distributed network of intermediary computers, or proxies, along a randomly assigned path known as a "circuit." The Tor software encrypts both

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.

PROBABLE CAUSE

8. **RYAN GOLDBERG** resided in Watkinsville, Georgia, and was a director of incident response for a multinational cybersecurity company. **GOLDBERG** is, as of the date of this Affidavit, believed to be in Europe.

9. At all times relevant to this complaint, Co-Conspirator 1, an individual whose identity is known to your affiant, was employed as a ransomware negotiator for a cyber-incident response company.

10. At all times relevant to this complaint, Co-Conspirator 2, an individual whose identity is known to your affiant, was employed as a ransomware negotiator for the same cyber-incident response company that employed Co-Conspirator 1.

11. Beginning at least in or around May of 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 began using ransomware to conduct ransomware attacks against victims. Specifically, in May of 2023, Co-Conspirator 1 obtained an affiliate account on

---

the headers and contents of each packet in layers such that no computer in the circuit, including the destination, can associate an originating user's IP address with the contents or routing path of a particular communication. Because of the way the Tor Network routes communications through the proxy computers, traditional IP identification techniques are not effective.

the ALPHV BlackCat panel and shared it with **GOLDBERG** and Co-Conspirator 2. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 agreed to and did use the ALPHV BlackCat ransomware and panel to attack and extort victims and share the ransom proceeds amongst themselves and with the ALPHV BlackCat administrator.

12. On or about May 13, 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 used ALPHV BlackCat ransomware to attack Victim 1, a medical company based in Florida that is engaged in interstate commerce. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 encrypted Victim 1's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not to publicize the stolen information. The attack caused Victim 1 to fear financial loss from the theft and encryption of their data. Because Victim 1's servers were encrypted by **GOLDBERG** and his Co-Conspirators, one or more employees of Victim 1 living and working in the Southern District of Florida were unable to work because their devices could not access data and applications necessary for their jobs, contributing to operational delays and lost business for Victim 1. Victim 1 paid **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 a ransom in virtual currency worth approximately $1,274,781.23 at the time of payment. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 paid the ALPHV BlackCat admin a percentage of the ransom payment and split the remainder amongst themselves.

13. On or about May 10, 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 used ALPHV BlackCat ransomware to attack Victim 2, a pharmaceutical company based in Maryland that is engaged in interstate commerce. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 encrypted Victim 2's servers and demanded a ransom payment to decrypt their servers. By stealing data and encrypting Victim 2's servers, the conspirators intended to cause Victim 2 to fear financial loss from the theft and encryption of their data.

14. In or around July of 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 used ALPHV BlackCat ransomware to attack Victim 3, a doctor's office based in California that is engaged in interstate commerce. **GOLDBERG**, Co-Conspirator 1 and Co-Conspirator 2 encrypted Victim 3's servers and demanded an approximate $5 million ransom payment to decrypt their servers. By stealing data and encrypting Victim 3's servers, the conspirators intended to cause Victim 3 to fear financial loss from the theft and encryption of their data.

15. In or around October of 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 used ALPHV BlackCat ransomware to attack Victim 4, an engineering company based in California that is engaged in interstate commerce. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 encrypted Victim 4's servers and demanded an approximate $1 million ransom payment to decrypt their servers. By stealing data and encrypting Victim 4's servers, the conspirators intended to cause Victim 4 to fear financial loss from the theft and encryption of their data.

16. In or around November of 2023, **RYAN GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 used ALPHV BlackCat ransomware to attack Victim 5, a manufacturer of unmanned aerial systems based in Virginia that is engaged in interstate commerce. **GOLDBERG**, Co-Conspirator 1, and Co-Conspirator 2 encrypted Victim 5's servers and demanded an approximately $300,000 ransom payment to decrypt their servers. By stealing data and encrypting Victim 5's servers, the conspirators intended to cause Victim 5 to fear financial loss from the theft and encryption of their data.

17. On June 17, 2025, the FBI conducted a consensual recorded interview of **RYAN GOLDBERG**. After initially denying being involved in ransomware attacks, **GOLDBERG**

confessed that he was recruited by Co-Conspirator 1 to "try and ransom some companies." **GOLDBERG** told the agents that he, Co-Conspirator 1, and Co-Conspirator 2 successfully "ransomed" Victim 1. **GOLDBERG** told the agents that he, Co-Conspirator 1, and Co-Conspirator 2 conducted attacks on other companies but were unsuccessful. **GOLDBERG** told the agents that they attacked Victim 4, which he described as an engineering company. **GOLDBERG** told the agents that they used ALPHV BlackCat ransomware to conduct the attacks. **GOLDBERG** said that after Victim 1 paid the ransom, they routed the cryptocurrency through a mixing service and then through multiple cryptocurrency wallets. **GOLDBERG** said that they believed that would make the funds harder to trace. **GOLDBERG** told the agents that he conducted the attacks to get out of debt and that he was "going to federal prison for the rest of [his] life."

18. Additionally, **RYAN GOLDBERG** stated that he was contacted by Co-Conspirator 2 after the FBI conducted a search of the residence of Co-Conspirator 1 on or about April 3, 2025. According to **GOLDBERG**, Co-Conspirator 2 was "freaking out about the FBI raiding [Co-Conspirator 1]."

19. An analysis of devices used by **RYAN GOLDBERG** and seized by the FBI on or about June 17, 2025, pursuant to a search warrant, revealed that **GOLDBERG** used a search engine to search Victim 2's name on or about May 4, 2023, approximately six days before the attack on Victim 2. On or about May 5, 2025, **GOLDBERG** also conducted, among other searches, an internet search for Co-Conspirator 1's name followed by "doj.gov."

20. Ten days after he was interviewed by the FBI, on June 27, 2025, **RYAN GOLDBERG** and his wife boarded a flight to Paris, France, from Atlanta, Georgia. The one-way tickets were purchased two days prior to travel, on June 25, 2025. As of the date of this Affidavit,

the FBI believes **GOLDBERG** and his wife are still in Europe. The FBI is unaware of any flights purchased by **GOLDBERG** to return to the United States.

CONCLUSION

21. Based upon the foregoing, your Affiant submits that there is probable cause to believe that **RYAN GOLDBERG** (1) conspired to, and did, obstruct, delay, and affect commerce and the movement of articles and commodities in commerce, by means of extortion, in violation of Title 18, United States Code, Sections 1951(a) and (b); and (2) intentionally caused damage without authorization to a protected computer in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030 (c)(4)(B)(i), and 2.

FURTHER AFFIANT SAYETH NAUGHT.

DOMINIQUE DAWSON
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Attested to by the Applicant in accordance with the requirements of Fed.R.Crim.P. 4.1
by Face Time this 19th day of September 2025.

HONORABLE EDUARDO I. SANCHEZ
UNITED STATES MAGISTRATE JUDGE