UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
26-CR-20065-BLOOM/ELFENBEIN
CASE NO. _____
18 U.S.C. § 1951(a)
18 U.S.C. § 981(a)(1)(C)

UNITED STATES OF AMERICA

vs.

ANGELO MARTINO,

Defendant.
_____/

INFORMATION

The United States Attorney charges that:

GENERAL ALLEGATIONS

At times material to this Information:

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 at least 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 Defendant and his Co-Conspirators

4. **ANGELO MARTINO** resided in Land O' Lakes, Florida, and was employed as a ransomware negotiator at Company 1, a cyber-incident response company based in Chicago, Illinois.

5. Ryan Clifford Goldberg resided in Watkinsville, Georgia.

6. Kevin Tyler Martin resided in Roanoke, Texas.

The Defendant and his Co-Conspirators' Victims

7. Victim 1 was a hospitality company based in the United States that was engaged in interstate commerce.

8. Victim 2 was a nonprofit company based in the United States that was engaged in interstate commerce.

9. Victim 3 was a financial services company based in the United States that was engaged in interstate commerce.

10. Victim 4 was a retail company based in the United States that was engaged in interstate commerce.

11. Victim 5 was a medical company based in the United States that was engaged in interstate commerce.

12. Victim 6 was a medical device company based in Tampa, Florida, with employees in the Southern District of Florida that was engaged in interstate commerce.

13. Victim 7 was a manufacturer of unmanned aerial systems based in Virginia that was engaged in interstate commerce.

14. Victim 8 was an engineering company based in California that was engaged in interstate commerce.

15. Victim 9 was a pharmaceutical company based in Maryland that was engaged in interstate commerce.

16. Victim 10 was a doctor's office based in California that was engaged in interstate commerce.

CONSPIRACY TO INTERFERE WITH INTERSTATE COMMERCE BY EXTORTION
(18 U.S.C. § 1951(a))

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

ANGELO MARTINO,

did knowingly and willfully combine, conspire, confederate, and agree with Ryan Clifford Goldberg, Kevin Tyler Martin, and others, both known and unknown to the United States Attorney, 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 the conspirators, and induced by fear, including fear of economic loss and harm.

PURPOSE OF THE CONSPIRACY

18. It was the purpose of the conspiracy for the defendant and his 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 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 **ANGELO MARTINO** and his co-conspirators sought to accomplish the object and purpose of the conspiracy included, among others, the following:

19. **ANGELO MARTINO** and his co-conspirators accessed victims' networks or computers and deployed ALPHV BlackCat ransomware. **MARTINO** also provided confidential information regarding ransomware negotiations to ALPHV BlackCat co-conspirators while employed at Company 1 as a ransomware negotiator.

20. For example, in or around May 2023, **ANGELO MARTINO**, Ryan Clifford Goldberg, and Kevin Tyler Martin used ALPHV BlackCat ransomware to attack Victim 6. **MARTINO**, Goldberg, and Martin encrypted Victim 6'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. The attack caused Victim 6 to fear financial loss from the theft and encryption of its data. Victim 6 paid **MARTINO**, Goldberg, and Martin a ransom in virtual currency worth approximately $1,274,000 at the time of payment.

21. In or around May 2023, **ANGELO MARTINO**, Ryan Clifford Goldberg, and Kevin Tyler Martin used ALPHV BlackCat ransomware to attack Victim 7. **MARTINO**, Goldberg, and Martin encrypted Victim 7'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 7's servers, the co-conspirators intended to cause Victim 7 to fear financial loss from the theft and encryption of its data.

22. In or around July 2023, **ANGELO MARTINO**, Ryan Clifford Goldberg, and Kevin Tyler Martin used ALPHV BlackCat ransomware to attack Victim 8. **MARTINO**,

Goldberg, and Martin encrypted Victim 8'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 8's servers, the co-conspirators intended to cause Victim 8 to fear financial loss from the theft and encryption of their data.

23. In or around October 2023, **ANGELO MARTINO**, Ryan Clifford Goldberg, and Kevin Tyler Martin used ALPHV BlackCat ransomware to attack Victim 9. **MARTINO**, Goldberg, and Martin encrypted Victim 9'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 9's servers, the co-conspirators intended to cause Victim 9 to fear financial loss from the theft and encryption of their data.

24. In or around November 2023, **ANGELO MARTINO**, Ryan Clifford Goldberg, and Kevin Tyler Martin used ALPHV BlackCat ransomware to attack Victim 10. **MARTINO**, Goldberg, and Martin encrypted Victim 10'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 10's servers, the co-conspirators intended to cause Victim 10 to fear financial loss from the theft and encryption of their data.

25. As noted, **ANGELO MARTINO** also provided, as a ransomware negotiator, confidential information to his ALPHV Blackcat co-conspirators. For example, in or around September 2023, a co-conspirator encrypted Victim 1's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. The attack caused Victim 1 to fear financial loss from the theft and encryption of its data. Victim 1 hired Company 1, and **MARTINO** conducted the ransom negotiations on behalf of

Company 1. During the ransom negotiations, **MARTINO** provided direction and confidential information to co-conspirators in order to maximize the ransom payment and in exchange for a portion of the ransom payment. Victim 1 paid the co-conspirators a ransom payment in virtual currency worth approximately $16,484,000 at the time of payment.

26. In or around April 2023, a co-conspirator encrypted Victim 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. The attack caused Victim 2 to fear financial loss from the theft and encryption of its data. Victim 2 hired Company 1, and **ANGELO MARTINO** conducted the ransom negotiations on behalf of Company 1. During the ransom negotiations, **MARTINO** provided direction and confidential information to co-conspirators in order to maximize the ransom payment in exchange for a portion of the ransom payment. Victim 2 paid co-conspirators a ransom payment in virtual currency worth approximately $26,793,000 at the time of payment.

27. In or around October 2023, a co-conspirator encrypted Victim 3's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. The attack caused Victim 3 to fear financial loss from the theft and encryption of its data. Victim 3 hired Company 1, and **ANGELO MARTINO** conducted the ransom negotiations on behalf of Company 1. During the ransom negotiations, **MARTINO** provided direction and confidential information to co-conspirators in order to maximize the ransom payment in exchange for a portion of the ransom payment. Victim 3 paid co-conspirators a ransom payment in virtual currency worth approximately $25,660,000 at the time of payment.

28. In or around October 2023, a co-conspirator encrypted Victim 4's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not

to publish the stolen information. The attack caused Victim 4 to fear financial loss from the theft and encryption of its data. Victim 4 hired Company 1, and **ANGELO MARTINO** conducted the ransom negotiations on behalf of Company 1. During the ransom negotiations, **MARTINO** provided direction and confidential information to co-conspirators in order to maximize the ransom payment in exchange for a portion of the ransom payment. Victim 4 paid co-conspirators a ransom payment in virtual currency worth approximately $6,100,000 at the time of payment.

29. In or around October 2023, a co-conspirator encrypted Victim 5's servers and demanded a ransom payment to decrypt the affected data and in exchange for a commitment not to publish the stolen information. The attack caused Victim 5 to fear financial loss from the theft and encryption of its data. Victim 5 hired Company 1, and **ANGELO MARTINO** conducted the ransom negotiations on behalf of Company 1. During the ransom negotiations, **MARTINO** provided direction and confidential information to co-conspirators in order to maximize the ransom payment in exchange for a portion of the ransom payment. Victim 5 paid co-conspirators a ransom payment in virtual currency worth approximately $213,000 at the time of payment.

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

FORFEITURE ALLEGATIONS

30. The allegations of this Information 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 the defendant, **ANGELO MARTINO**, has an interest.

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

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

32. The property directly subject to forfeiture as a result of the alleged offenses includes the following:

i. approximately 0.71173674 Bitcoin (BTC), seized from cryptocurrency address ending in 0xcjq;

ii. approximately 26.14495476 BTC, seized from cryptocurrency address ending in dx3p;

iii. approximately 13.10297733 BTC, seized from cryptocurrency address ending in yw55;

iv. approximately 50.35937019 BTC, seized from cryptocurrency address ending in 7fxt;

v. approximately 5000.9997 Monero (XMR), seized from cryptocurrency address ending in smhvo;

vi. approximately 0.00006936 XMR, seized from cryptocurrency address ending in b4Rpz;

vii. approximately 590 XMR, seized from cryptocurrency address ending in Uhkvc;

viii. approximately 653 XMR, seized from cryptocurrency address ending in 93T96;

ix. approximately 1360.99982688 XMR, seized from cryptocurrency address ending in y6pGA

x. approximately 187.872523112871 XMR, seized from cryptocurrency address ending in 2tPBs;

xi. approximately 204.99995 XMR, seized from cryptocurrency address ending in Jtiyn8;

xii. approximately 0.99996932 XMR, seized from cryptocurrency address ending in 8HCJF;

xiii. approximately 0.00003072 XMR, seized from cryptocurrency address ending in jmHoe;

xiv. approximately 0.0006932 XMR, seized from cryptocurrency address ending in ZnKdh;

xv. approximately 0.9999081 XMR, seized from cryptocurrency address ending in Ebk1B;

xvi. approximately 0.00006924 XMR, seized from cryptocurrency address ending in uMsVQ1;

xvii. approximately 10 Ripple (XRP), seized from cryptocurrency address ending in EkThx6;

xviii. approximately 56,174.152377 XRP, seized from cryptocurrency address ending in EkThx6;

xix. approximately 52.355385712 Solana (SOL), seized from cryptocurrency address ending in HbXXhs;

xx. approximately 10 Stellar (XLM), seized from cryptocurrency address ending in 5RJ3BD;

xxi. approximately 39750.7927306 XLM, seized from cryptocurrency address ending in 5RJ3BD

xxii. one motor vehicle, 1999 Nissan Skyline VIN# BNR34-006236;

xxiii. one motor vehicle 2024 Polar RZR-24 PRO VIN# 3NSRMD2K5RG333271;

xxiv. real property located at 2305 Bayshore Road, Nokomis, Florida 34275;

xxv. real property located at 236 Tracino Nokomis, FL 34275;

xxvi. one 2023 Crazy Manson Trailer VIN# 4DJAB3031PA001316, License Plate AL71SM; and

xxvii. one 2023 Vessel VIN# BKFBL100K123, Length: 28' 10".

All pursuant to Title 18, United States Code, Section 981(a)(1)(C) and the procedures set forth in Title 21, United States Code, Section 853, as incorporated by Title 28, United States Code, Section 2461(c).

JASON A. REDING QUIÑONES
UNITED STATES ATTORNEY

THOMAS HAGGERTY
ASSISTANT UNITED STATES ATTORNEY

for CHRISTEN GALLAGHER
JORGE GONZALEZ
TRIAL ATTORNEYS
COMPUTER CRIME AND
INTELLECTUAL PROPERTY SECTION

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA

v.

ANGELO MARTINO

_____/
Defendant.

CASE NO.: 26-CR-20065-BLOOM/ELFENBEIN

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 0 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) No
   If yes, Judge _____ Magistrate Case No. _____
8. Does this case relate to a previously filed matter in this District Court? (Yes or No) Yes
   If yes, Judge K. Michael Moore Case No. 25-CR-20443
9. Defendant(s) in federal custody as of _____
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
15. 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
16. 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
17. 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: ANGELO MARTINO

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

***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.**

AO 455 (Rev. 01/09) Waiver of an Indictment

UNITED STATES DISTRICT COURT

for the

United States of America
v.
Angelo Martino
Defendant

Case No. **26-CR-20065-BLOOM/ELFENBEIN**

WAIVER OF AN INDICTMENT

I understand that I have been accused of one or more offenses punishable by imprisonment for more than one year. I was advised in open court of my rights and the nature of the proposed charges against me.

After receiving this advice, I waive my right to prosecution by indictment and consent to prosecution by information.

Date: _____

_____
Defendant's signature

_____
Signature of defendant's attorney

_____
Printed name of defendant's attorney

_____
Judge's signature

_____
Judge's printed name and title