UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 26-CR-20065-KMM

UNITED STATES OF AMERICA

vs.

ANGELO MARTINO,

_____/

FACTUAL PROFFER

The United States of America (the "United States") and defendant Angelo Martino (the "defendant") agree that, were this case to proceed to trial, the United States would prove beyond a reasonable doubt the following facts, among others, which occurred in the Southern District of Florida and elsewhere:

BlackCat/ALPHV Ransomware

Ransomware is malicious software that encrypts and steals data from vulnerable computer networks to extort a ransom payment in exchange for unlocking the network and/or not publishing sensitive stolen data. BlackCat/ALPHV ("BlackCat") is a variant of ransomware that was used to attack institutions around the world, including entities engaged in interstate commerce in the Southern District of Florida.

The BlackCat ransomware variant was developed and managed by a BlackCat administrator, or "admin," who granted BlackCat "affiliates" access to the application programming interface, or panel, used to deploy the ransomware pursuant to an agreement that any ransoms paid in virtual currency would be split, typically with 20 percent going to the admin and 80 percent going to the affiliate. Each BlackCat affiliate had their own unique login to the BlackCat panel through which they managed their attacks. After an affiliate deployed BlackCat

ransomware on a victim's system and encrypted and/or stole the victim's data, the victim was directed by the ransom note left on the victim's system to their own dedicated panel with a "live chat" tab to negotiate a ransom payment for the encrypted and stolen data. BlackCat actors threatened victims through messages stating that sensitive data on a victim's network was downloaded, that quick action was needed to prevent the publication of sensitive data, and that attempts by the victim to modify encrypted data will result in permanently lost or inaccessible data.

Typically, the victim was given an initial ransom demand and an opportunity to negotiate a ransom payment amount, sometimes reaching an agreement to pay an amount less than the initial demand. If the victim paid the ransom, they were provided with a "decryptor," a decryption key to render their encrypted data readable and usable to the victim. In cases where sensitive victim information was stolen, the ransom payment was typically paid in exchange for a promise by the BlackCat actors to not publish stolen victim data on a publicly-viewable data leak site. If a victim did not pay the ransom, their stolen data would be published on the data leak site.

The Conspiracy to Assist BlackCat Negotiators

In 2022 and 2023, the defendant was employed as a ransomware negotiator at Company 1, a U.S.-based cyber incident response company. Company 1 offers customers services that include ransomware negotiation in response to a live ransomware attack resulting in the encryption or exfiltration of victim data. These negotiations included responsibility for facilitating communications and negotiations with ransomware threat actors on a customer's behalf and, if necessary, facilitating payment to a threat actor to procure the tools needed to decrypt data.

During the relevant period, the defendant worked remotely on a company-issued laptop. As part of his duties, the defendant was provided with details regarding the attack and information

regarding the ransom demand and typically the victim's applicable insurance coverage and negotiating strategy. In his role as an employee of Company 1, the defendant negotiated with threat actors associated with multiple ransomware variants, including actors using the BlackCat ransomware variant, on behalf of the company's clients. Concerning the victims identified below, the defendant used the live chat tab in the BlackCat panel to negotiate the ransom payment (hereinafter the "negotiation chat"). Copies of these chats were typically saved and provided to Company 1 and the victim.

Beginning in or around April of 2023, the defendant began communicating with BlackCat actors through the messaging platform Tox and in a separate "intermediary chat" tab of the BlackCat panel. The intermediary chat was only accessible to the defendant and the BlackCat negotiators and affiliates. In the intermediary chat, the defendant provided confidential information regarding specific Company 1 clients and instructions without those clients' knowledge, while simultaneously communicating with BlackCat actors in his capacity as a ransomware negotiator employed by Company 1. This confidential information was provided before the victim and threat actor reached agreement regarding the amount of a particular ransom payment.

The purpose of these intermediary chat communications was to maximize the ransom payments paid by those victims to the BlackCat actors. This information provided by the defendant without the victims' knowledge included the victims' insurance policy limits and internal negotiation positions. In exchange for providing confidential information, the defendant received a portion of the ransomware payments in digital currency. Company 1 and their clients were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat or Tox messenger that are described or referred to herein.

Victim 1

In or around September 2023, a BlackCat affiliate attacked Victim 1, a U.S.-based hospitality company engaged in interstate commerce. The BlackCat affiliate used this ransomware to make an unauthorized copy of certain data contained in servers used by Victim 1 as well as encrypting those servers. They demanded a ransom payment to provide a decryptor to Victim 1 and not expose its data on the Internet. The attack caused Victim 1 to fear financial loss from the theft and encryption of their data. Victim 1 hired Company 1, and the defendant conducted the ransom negotiations on behalf of Victim 1.

During the negotiation, the defendant accessed the intermediary chat and advised the BlackCat actor to search Victim 1's stolen data for insurance policy information and provided direction regarding specific steps that should be taken by the BlackCat actor. The defendant explained that:

> the [insurance] carrier is only approving small amounts- keep denying our offers and i will let you know once i find out the max the[y] want to pay. Next msg we send- feel free to say we know you have money and mention [named insurer] and the cyber policy like you mentioned before.

In the negotiation chat that was visible to Company 1 and Victim 1, the defendant then wrote separately:

> We are being serious. We don't know how you came up with your demand but we are losing money operationally and all of our loans are going to turnover on us this year at double the interest rates. $17 million would put us out of business. Also we were only able to get so much on a bitcoin exchange before banks closed. We are able to give you $1 million now- which is a very serious offer.

The BlackCat actor then followed the defendant's instructions and replied in the negotiation chat:

> Well- you can keep that for the penalties and law suits which are coming your way in case we expose you. Time is ticking- we know how much you can pay. Contact your insurance. We know about them also.Stop wasting time.

In addition to other messages, the defendant thereafter stated in the intermediary chat:

> just a heads up- im working on this with a team member. So I will sign in here when I can. I did show the client the private leak. This client absolutely needs the decryptor so maybe focus on threatening deletion of the decryptor. The Client wants to keep increasing the amount but the [insurance] carrier is just being a dick.

The defendant provided this and other information and directions to the BlackCat actor prior to the victim and the BlackCat actor reaching agreement on a ransom payment. Victim 1 eventually paid a ransom payment in virtual currency worth approximately $16,484,000 at the time of payment for the decryptor and for a commitment from the BlackCat actor to forego publication of the copied data on the leak site.

In exchange for the information and directions provided to the BlackCat actors, the defendant received financial compensation from the BlackCat actors. Company 1 and their client were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat.

Victim 2

In or around April 2023, a BlackCat affiliate attacked Victim 2, a U.S.-based nonprofit company engaged in interstate commerce. The BlackCat affiliate stole Victim 2's data and encrypted their servers. They demanded a ransom payment in order to provide a decryptor to Victim 2 and not expose their data on the leak site. The attack caused Victim 2 to fear financial loss from the theft and encryption of their data. Victim 2 hired Company 1, and the defendant conducted the ransom negotiations on behalf of Victim 2. At the same time that defendant was conducting negotiations on behalf of Victim 2, the defendant separately communicated with BlackCat actors to provide confidential information and directions to assist the BlackCat actors in maximizing the ransomware payment paid by the victim. The defendant provided this information and these directions to the BlackCat actor prior to the victim and the BlackCat actor reaching agreement on a ransom payment. Victim 2 paid a ransom payment in virtual currency worth

approximately $26,793,000 at the time of payment for the decryptor and for a commitment from the BlackCat actor to forego publication of the copied data on the leak site.

In exchange for the information and directions provided to the BlackCat actors, the defendant received financial compensation from the BlackCat actors. Company 1 and their client were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat.

Victim 3

In or around October 2023, a BlackCat affiliate attacked Victim 3, a U.S.-based financial services company engaged in interstate commerce. The BlackCat affiliate stole Victim 3's data and encrypted their servers. They demanded a ransom payment in order to provide a decryptor to Victim 3 and not expose their data on the leak site. The attack caused Victim 3 to fear financial loss from the theft and encryption of their data. Victim 3 hired Company 1, and the defendant conducted the ransom negotiations on behalf of Victim 3. At the same time that defendant was conducting negotiations on behalf of Victim 3, the Defendant communicated using the intermediary chat without the knowledge of Company 1 or Victim 3, in order to provide confidential information and directions to assist the BlackCat actor in maximizing the ransomware payment. The defendant provided this information and these directions to the BlackCat actor prior to the victim and the BlackCat actor reaching agreement on a ransom payment. Victim 3 paid a ransom payment in virtual currency worth approximately $25,660,000 at the time of payment for the decryptor and for a commitment from the BlackCat actor to forego publication of the copied data on the leak site.

In exchange for the information and directions provided to the BlackCat actors, the defendant received financial compensation from the BlackCat actors. Company 1 and their client

were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat.

Victim 4

In or around October 2023, a BlackCat affiliate infected Victim 4, a U.S.-based retail company engaged in interstate commerce, and encrypted their servers. The attack caused Victim 4 to fear financial loss from the theft and encryption of their data. Victim 4 hired Company 1, and the defendant conducted the ransom negotiations on behalf of Victim 4. At the same time that defendant was conducting negotiations on behalf of Victim 4, the Defendant used the intermediary chat and the Tox messaging platform that were not known to Company 1 or Victim 4 to provide confidential information and directions to assist the BlackCat actor in maximizing the ransomware payment. The defendant provided this information and these directions to the BlackCat actor prior to the victim and the BlackCat actor reaching agreement on a ransom payment. Victim 4 paid a ransom payment in virtual currency worth approximately $6,100,000 at the time of payment for the decryptor and for commitments from the BlackCat actor, including an agreement to forego publication of the copied data on the leak site.

In exchange for the information and directions provided to the BlackCat actors, the defendant received financial compensation from the BlackCat actors. Company 1 and their client were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat.

Victim 5

In or around October 2023, a BlackCat affiliate attacked Victim 5, a U.S.-based medical company engaged in interstate commerce, and encrypted their servers. The attack caused Victim 5 to fear financial loss from the theft and encryption of their data. Victim 5 hired Company 1, and

the defendant conducted the ransom negotiations on behalf of Victim 5. At the same time that defendant was conducting negotiations on behalf of Victim 5, the Defendant used simultaneous communications that were not known to Company 1 or Victim 5 to provide confidential information and directions to assist the BlackCat actor in maximizing the ransomware payment. The defendant provided this information and these directions to the BlackCat actor prior to the victim and the BlackCat actor reaching agreement on a ransom payment. Victim 5 paid a ransom payment in virtual currency worth approximately $213,000 at the time of payment for the decryptor and for a commitment from the BlackCat actor to forego publication of the copied data on the leak site.

In exchange for the information and directions provided to the BlackCat actors, the defendant received financial compensation from the BlackCat actors. Company 1 and their client were not aware of and did not approve the disclosures of confidential information by the defendant in the intermediary chat.

The *Conspiracy to Deploy Ransomware as a BlackCat Affiliate*

Beginning in or around 2022, the defendant, Co-conspirator 1 and Co-Conspirator 2, began using ransomware to conduct ransomware attacks against victims. During the times relevant to this conspiracy, Co-conspirator 1 was an employee at Company 1 and resided in Texas, and Conspirator 2 was an employee at a separate incident response company ("Company 2") and resided in Georgia. In May of 2023, the defendant obtained affiliate access to the BlackCat panel that he shared with Co-conspirators 1 and 2. After the defendant obtained affiliate access, the defendant, Co-conspirator 1, and Co-Conspirator 2 agreed to, and did use the BlackCat ransomware and platform to attack and extort victims and share the ransom proceeds amongst themselves and with the BlackCat admin.

Victim 6

In or around May 2023, the defendant, Co-Conspirator 1, and Co-Conspirator 2 used BlackCat ransomware to attack Victim 6, a U.S.-based medical device company engaged in interstate commerce. Victim 6's servers were encrypted and the defendant, Co-conspirator 1 and Co-Conspirator 2 demanded a $1.38 million dollar ransom payment to decrypt their servers. The attack caused Victim 6 to fear financial loss from the theft and encryption of their data. Victim 6 paid the defendant, Co-conspirator 1 and Co-conspirator 2 a ransom payment in virtual currency worth approximately $1,274,000 at the time of payment for the decryptor and for their data not to be published on the Internet. Consistent with the agreement with the BlackCat administrator to receive affiliate access to the BlackCat panel, the defendant, Co-conspirator 1, and Co-Conspirator 2 paid the BlackCat admin a percentage of the ransom.

Victim 7

In or around November 2023, the defendant, Co-Conspirator 1, and Co-Conspirator 2 used BlackCat ransomware to attack Victim 7, a U.S.-based manufacturer of unmanned aerial systems engaged in interstate commerce. The defendant, Co-Conspirator 1, and Co-Conspirator 2 demanded a $300,000 ransom payment to decrypt their servers. The defendant, Co-Conspirator 1, and Co-Conspirator 2 intended to cause Victim 7 to fear financial loss from the theft and encryption of their data, and therefore to pay the ransom. Victim 7 did not pay the ransom, and the defendant, Co-Conspirator 1, and Co-conspirator 2 did not provide a decryptor to Victim 7. Victim 7 nevertheless suffered damages.

Victim 8

In or around October 2023, the defendant, Co-Conspirator 1, and Co-Conspirator 2 used BlackCat ransomware to attack Victim 8, a U.S.-based engineering company engaged in interstate commerce. The defendant, Co-Conspirator 1, and Co-Conspirator 2 demanded a $1,000,000 ransom payment to decrypt their servers. The defendant, Co-Conspirator 1, and Co-Conspirator 2 intended to cause Victim 8 to fear financial loss from the theft and encryption of their data, and therefore pay the ransom. Victim 8 did not pay the ransom. The defendant, Co-Conspirator 1, and Co-conspirator 2 did not provide a decryptor to the Victim. Victim 8 nevertheless suffered damages.

Victim 9

In or around May 2023, the defendant, Co-Conspirator 1, and Co-Conspirator 2 used BlackCat ransomware to attack Victim 9, a U.S.-based pharmaceutical company engaged in interstate commerce. The defendant, Co-Conspirator 1, and Co-Conspirator 2 demanded a ransom payment to decrypt their servers. The defendant, Co-Conspirator 1, and Co-Conspirator 2 intended to cause Victim 9 to fear financial loss from the theft and encryption of their data, and therefore pay the ransom. Victim 9 did not pay the ransom. The defendant, Co-Conspirator 1, and Co-conspirator 2 did not provide a decryptor to the Victim. Victim 9 nevertheless suffered damages.

Victim 10

In or around June 2023, the defendant, Co-Conspirator 1, and Co-Conspirator 2 used BlackCat to attack Victim 10, a doctor's office engaged in interstate commerce. The defendant, Co-Conspirator 1, and Co-Conspirator 2 demanded a $5,000,000 ransom payment to decrypt their servers. The defendant, Co-Conspirator 1, and Co-Conspirator 2 intended to cause Victim 10 to fear financial loss from the theft and encryption of their data, and therefore pay the ransom. Victim

10 did not pay the ransom. The defendant, Co-Conspirator 1, and Co-conspirator 2 did not provide a decryptor to the Victim. Victim 10 nevertheless suffered damages.

Cryptocurrency Proceeds

The defendant received millions of dollars in cryptocurrency as proceeds from the above conspiracies. He used the proceeds to purchase two houses: one located at 2305 Bayshore Road Nokomis, FL 34275, and the second at 236 Tracino Terrance Nokomis FL 34275. Using the proceeds, the defendant also purchased a 1999 Nissan skyline vehicle (VIN: BNR34-006236), a 2023 boat (VIN: BKFBL100K123), a 2024 Polaris vehicle VIN: 3NSRMD2K5RG333271 and a 2023 food truck (VIN: 4DJAB3031PA001316). On April 3, 2025, the FBI seized the following cryptocurrency from the defendant's residence, which are proceeds of the above conspiracies:

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

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

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

iv. approximately 50.35937019 BTC, seized from cryptocurrency address ending -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 0.0000693 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; and

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

The parties agree that these facts, which do not include all facts known to the United States and the defendant, are sufficient to prove Count 1 of the Information.

JASON A. REDING QUIÑONES
UNITED STATES ATTORNEY

Date: 4/14/26

THOMAS HAGGERTY
Assistant United States Attorney

Date: 4/14/26

for CHRISTEN GALLAGHER
JORGE GONZALEZ
Trial Attorneys
Computer Crime and Intellectual Property Section

Date: 4-14-26

LINDA JULIN MCNAMARA
Attorney for the Defendant

Date: 4-14-26

ANGELO MARTINO
Defendant