UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 26-20065-CR-MOORE

UNITED STATES OF AMERICA

v.

ANGELO MARTINO,

Defendant.
_____/

THE UNITED STATES OF AMERICA'S SENTENCING MEMORANDUM

The United States of America hereby files its sentencing memorandum as to Angelo Martino (MARTINO) and requests a sentence that reflects the seriousness of MARTINO's criminal conduct, which the parties agree is properly reflected by a total offense level of 27 and a guidelines range of 70 to 87 months. MARTINO's criminal conduct falls into two related categories.

First, MARTINO was a ransomware negotiator employed by an incident response company (Company 1) to negotiate with cybercriminals to mitigate the ransoms paid by Company 1's clients. Instead, MARTINO provided the cybercriminals with confidential negotiation information to maximize the ransoms in exchange for a portion of the ransom payments. Five of the victims whom MARTINO was supposed to help paid over $75 million dollars to ransomware affiliates, including likely millions of dollars in ransom demands inflated as a result of the confidential information provided by MARTINO.

Second, MARTINO conspired other cybersecurity professionals Ryan Clifford GOLDBERG and Kevin Tyler MARTIN, who was also a ransomware negotiator at Company 1,

to attack at least five victims using ransomware, and obtained over $1,200,000 in cryptocurrency as ransom.

In addition to reflecting the significant damage suffered by MARTINO's victims, the Court should impose a sentence that reflects the seriousness of the offense and the need to deter future cyberattacks, particularly attacks by individuals seeking to abuse specialized skills and positions of trust within the cybersecurity industry.

Accordingly, the Court should impose a sentence within the guidelines range, and the government believes a sentence of at least the mid-point of this range is warranted.

I. BACKGROUND ON RANSOMWARE AND THE BLACKCAT/ALPHV VARIANT

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 BlackCat administrators, or "admins," 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, these ransom payments were divided with 20% going to the admins and 80% going to the affiliate. Each BlackCat affiliate typically 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 with instructions to access a communications platform 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 would 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 also 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.

In December 2023, the Federal Bureau of Investigation successfully disrupted the BlackCat ransomware group by seizing multiple website operated by the organization, developing a decryption capability that was offered to over 500 affected victims, and taking additional steps to degrade that group's ability to conduct ransomware attacks.[1]

II. MARTINO'S CRIMES

MARTINO's crimes represent a profound betrayal of the trust placed in him by ransomware victims during periods of great stress and vulnerability arising from sophisticated cyberattacks. Ransomware victims turn to professional negotiators to act as loyal advocates who work to mitigate the harm inflicted by cyber criminals while preserving their clients' confidences

[1] *See* Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant, *available at* https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant?os=..&ref=app (last visited July 6, 2026).

and sensitive information. The defendant instead exploited that position of trust by secretly feeding confidential negotiation information to the very criminals extorting his clients while being paid by his firm to help them. He was, in effect, a double agent working to maximize the harm to his clients and the financial gain to cybercriminals who paid him a part of the ransom as demonstrated by the fact that authorities have been able to trace certain digital currency payments directly from ransom victims to digital currency addresses controlled by MARTINO.

MARTINO, for example, deliberately exploited this vulnerability by informing attackers in September 2023 that Victim 1 "absolutely need[ed]" the ability to decrypt files while instructing attackers to reject proposed ransom demands until MARTINO could determine the "max the[y] want to pay." The government's investigation has also revealed, for example, that while negotiating on behalf of another victim in October 2023, MARTINO represented to his employer and client that he was making a specific ransom offer, while simultaneously directing the attackers to reject that offer because MARTINO knew that the client would be willing to pay a maximum ransom that was $2,000,000 greater. In this example, the victim did in fact pay a ransom that was more than $2,000,000 greater than the offer which MARTINO initially made on his client's behalf.

This scheme also resulted in significant ransom payments, and affected the ability of victims including companies in the financial services and health industry to provide services to customers. The five victims targeted by this criminal activity paid ransoms of approximately $213,000; $6,100,000; $16,484,000; $25,660,000; and $26,793,000; between April 2023 and September 2023. In each case, these ransom payments were made following negotiations conducted by MARTINO in which he was providing confidential information to the attackers before his client agreed on a payment amount. As explained by statements submitted by those

victims, these victims also incurred significant expenses and losses during the weeks and months required to recover from these attacks.

This was not a crime of opportunity or momentary weakness; it was a sustained abuse of a fiduciary-like relationship driven by a single purpose: greed. The defendant bought cars, boats, and houses with the money extorted from his clients.

Beyond his betrayal as a negotiator, the defendant conspired with other cybersecurity professionals to conduct ransomware attacks against victims in the United States. Beginning in 2022 and continuing through the end of 2023, the Defendant, Goldberg, and Martin planned and executed ransomware attacks against at least five victims in the United States. (During this conspiracy, Martin was hired by MARTINO's employer in mid- 2023 as a ransomware negotiator and Goldberg was a cyber security professional at another company.) Using their specialized skills, the group extorted over $1.2 million dollars in cryptocurrency from a U.S.-based medical device company. The co-conspirators' employment gave them a unique advantage: they understood how victims detect intrusions, how they respond to demands, and how negotiators and insurers evaluate threats.

III. CRIMINAL PROSECUTION

On October 2, 2025, a grand jury returned an Indictment against GOLDBERG and MARTIN (25-CR-20443-KMM). Count 1 of the Indictment charged the defendants with conspiring with each other and MARTINO (identified therein as Co-Conspirator 1) to interfere with interstate commerce by extortion. Count 2 charged them with interference with interstate commerce by extortion for extorting the medical device company, and Count 3 charged them with encrypting the medical device company's servers. MARTIN and GOLDBERG pled guilty to Count 1 of the Indictment, and the Court accepted their guilty pleas on December 29, 2025 (25-

CR-20443-KMM, DEs: 68, 69). On April 30, 2026, this Court sentenced MARTIN and GOLDBERG each to 48 months' imprisonment (25-CR-20443-KMM, DEs: 106,107).

On February 25, 2026, Angelo MARTINO was charged by Information with conspiracy to interfere with interstate commerce by extortion. MARTINO pled guilty, and the Court accepted his guilty plea on April 20, 2026 (DE:30). He is set for sentencing on July 9, 2026 (26-CR-20065, DE:30).

IV. THE DEFENDANT'S GUIDELINES RANGE

The United States submits that MARTINO's Total Offense Level is 27. The correct application of the Guidelines is as follows:

Guideline Section	Level
Base Offense Level § 2B3.2	**18**
Specific Offense Characteristics	
Amount demanded more than $9,500,000: § 2B3.1(b)(7)(H)	**+7**
Damage to computer system used to maintain or operate critical infrastructure § 2B3.2(b)(3)(B)(i)(V)	+3
Abuse of public or private trust or used a special skill: § 3B1.3	+2
Adjusted Offense Level	**30**
Acceptance of Responsibility § 3E1.1	-3
Adjusted Offense Level	**27**

In particular, the United States submits that application of the three-level enhancement pursuant to § 2B3.2(b)(3)(B)(i)(V) is appropriate based on MARTINO's conspiracy in the attacks targeting victims in the financial services and medical industries to enhance the ransoms paid by Victims 3 and 5. The United States further submits that application of the two-level enhancement pursuant to § 3B1.3 is appropriate based both on the direct connection between MARTINO's role as a negotiation on behalf of Victims 1 through 5 and his role in providing direction and

confidential information to the attackers as well as the technical skills which he and his co-conspirators used in conducting ransomware attacks targeting Victims 6 through 10. Pursuant to MARTINO's plea agreement, the parties' agree that these specific offense characteristics as well as § 2B3.1(b)(7)(H) apply to MARTINO's criminal conduct.

With a criminal history category of I, the Defendant's guideline range is 70 to 87 months.

V. THE SECTION 3553(A) FACTORS

While the Guidelines are purely advisory, the Court "must consult those Guidelines" and the factors set forth in 18 U.S.C. § 3553(a) when determining the appropriate sentence. *United States v. Booker*, 543 U.S. 220, 264 (2005).

The sentencing factors set forth in 18 U.S.C. § 3553(a), particularly the nature and circumstances of the offense and history of the defendant, the need for the sentence to reflect the seriousness of the offense, promote respect for the law, and provide just punishment and adequate deterrence, counsel in favor of a substantial sentence.

The Eleventh Circuit has held that white-collar criminals deserve punishments commensurate with the seriousness of their offenses:

> Because economic and fraud-based crimes are "more rational, cool, and calculated than sudden crimes of passion or opportunity," these crimes are "prime candidate[s] for general deterrence." … Defendants in white collar crimes often calculate the financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment.
>
> ***
>
> Indeed, the Congress that adopted the § 3553 sentencing factors emphasized the critical deterrent value of imprisoning serious white collar criminals, even where those criminals might themselves be unlikely to commit another offense. . . .

United States v. Martin, 455 F.3d 1227, 1240 (11th Cir. 2006) (certain internal citations omitted). The Eleventh Circuit also cautioned against sentences that leave the impression that "would-be

white-collar criminals stand to lose little more than a portion of their ill-gotten gains and practically none of their liberty." *Id.*

The government submits that after balancing the above factors, a sentence of imprisonment in the upper range of the guidelines range complies with the goals set forth in 18 U.S.C. § 3553(a) and amounts to a reasonable sentence.

i. Accounting for the Nature and Circumstances of the Offense, the Seriousness of the Offense, and the Need to Provide Just Punishment

MARTINO's sophisticated hacking conduct as an affiliate for BlackCat and abuse of his client's trust in this case by collaborating with BlackCat against his clients resulted in numerous victims paying tens of millions of dollars in ransoms. As a negotiator, he was obligated to advance his client's interests and pursue the best possible outcome for them. Instead, he colluded with the ransomware actors against his clients, maximizing the benefit to the threat actors and himself. Consequently, he was complicit in extorting tens of millions of dollars from those clients who had trusted him in a time of crisis.

MARTINO further used his knowledge of ransomware and connections with ransomware actors to secure an affiliate account for himself, Martin, and Goldberg with ALPHV Blackcat. As an ALPHV Blackcat affiliate, the three men deployed ransomware against five victims, successfully extorting one payment for $1.2 million. Although the other victims did not pay the ransom demand, they nevertheless suffered consequential losses from the attacks. In total, the losses resulting from MARTINO's conduct against numerous victims exceeded $76 million dollars and resulted in criminal gains of at least $10 million for himself. The Guidelines direct the application of the loss table in §2B3.1 for violations of Title 18, section 1951(a), which provides for a maximum loss amount of $9,500,000.

The purpose of his conduct was greed. He abused his clients trust for his own personal gain and conspired with other sophisticated hackers to use their considerable computer skills to extort others. A custodial sentence at the top of the Guidelines is needed to reflect the seriousness of conduct and the intrusions into companies operating in the financial services and health industries providing critical services to customers in the Southern District of Florida and across the country.

ii. The Need for General Deterrence of Hacking Conduct

There is a compelling need for general deterrence in this case. The Court's sentence should send a message to those who might consider hacking companies and extorting victims that such conduct will carry consequences.

The importance of general deterrence here is heightened in at least three respects. First, the choice to engage in sophisticated hacking conduct is typically a calculated decision and therefore particularly well suited to general deterrence. *See United States v. Thompson*, 130 F.4th 1158, 1167 (9th Cir. 2025); *see also United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) ("[b]ecause economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence.") (internal quotation marks and alteration omitted). In this case, MARTINO was motivated by greed and a sense of power from hacking and extorting his victims. Other potential criminals must know that the money or thrill of attacking U.S. companies, particularly those attacks that interfere with the operation of foundational U.S. infrastructure, is simply not worth the severe punishment imposed for such crimes.

Second, for sophisticated ransomware schemes involving the use of anonymous identities online, many crimes go unsolved and therefore unpunished. Without a real possibility of

imprisonment in those circumstances where perpetrators are brought to justice, there would be little incentive for a wavering would-be hacker to forego their contemplated criminal conduct. *See United States v. Engle*, 592 F.3d 495, 502 (4th Cir. 2010) (explaining that because tax evasion offenses are infrequently prosecuted, "[w]ithout a real possibility of imprisonment, there would be little incentive for a wavering would-be evader to choose the straight-and-narrow over the wayward path); *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it."); *United States v. Fitzpatrick*, 126 F.4th 348, 354 (4th Cir. 2025) ("[A] 17-day sentence for the commission of three serious felonies [including the largest English-language data-breach forum ever] signals to would-be criminals that they might get one free pass before facing any serious penalties.").

Finally, MARTINO's actions directly resulted in the continued victimization of the companies for which he was the ransom negotiator. Not only were those companies affected and disrupted by the initial ransomware attack, they did not receive the incident response services for which they paid and were instead forced to pay an increased ransom as a direct result of MARTINO's decision to exploit the information with which he had been entrusted by those victims to enrich himself and the attackers. *E.g.*, *United States v. Radford*, 2026 WL 125737 *9 (11th Cir. 2026).

The public's interest in deterring cybercrime cannot be overstated. The Internet Crime Complaint Center ("IC3"), the FBI unit that receives and tracks cybercrime complaints from victims, received a total of 89,129 complaints of extortion in 2025, with reported losses of over

$122 million.[2] These figures highlight that cyber extortion schemes impose a tremendous cost beyond the cost of any ransom paid because the victim must expend considerable resources to identify the full scope of the breach and fix any vulnerabilities, ensure the protection of sensitive data, notify clients, and, in certain cases, report and respond to federal and state regulatory agencies in the aftermath of a breach.

The public need for general deterrence in computer crimes is also at its zenith because of their ease of commission. No computer system is completely secure and opportunities for hacking are legion. Accordingly, it is vital that would-be hackers see that the potential economic and any reputational benefits of this type of computer intrusion are outweighed by stiff punishment. *See*, *e.g.*, *United States v. Thompson*, 130 F.4th 1158, 1167 (9th Cir. 2025) ("[T]here are some people out there who are looking at the cost-benefit analysis and saying ... if I can get away with credit for time served of 100 days, with the possibility of making a couple hundred million dollars with this, I'm going to take the chance."). Accordingly, the need for general deterrence throughout the community favors a significant custodial sentence that will deter those considering hacking conduct.

iii. Avoiding Unwarranted Sentencing Disparities

Lastly, a sentence at least at the mid-point of the guidelines range, i.e., between 70 and 87 months, would avoid unwarranted sentencing disparities. MARTINO's co-conspirators, Martin and Goldberg received 48-month sentences for their roles in the ransomware attacks targeting Victims 6 through 10. MARTINO's significant additional criminal conduct targeting Victims 1 through 5 should be reflected by a sentence within the guidelines range to account for the increased culpability and harm associated with that conduct.

[2] FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2025 at 7-8, *available at* https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf (last visited July 6, 2026).

VI. CONCLUSION

At the Defendant's sentencing, the Court should impose a sentence within the guidelines range of 70 and 87 months. Specifically, the government believes a sentence of imprisonment of at least the mid-point of this range is appropriate.

JASON A. READING QUINOÑES
UNITED STATES ATTORNEY

BY: */s/ Jorge Gonzalez*
Jorge Gonzalez
Christen Gallagher
Trial Attorneys
1301 New York Avenue, NW
Washington, D.C. 20005
Email: Jorge.Gonzalez3@usdoj.gov
Email: Christen.Gallagher@usdoj.gov

BY: */s/ Thomas Haggerty*
Thomas Haggerty
Assistant United States Attorney
Fla. Bar. No. 46136
99 N.E. 4th Street
Miami, Florida 33132
Email: Thomas.Haggerty@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on July 7, 2026, the undersigned electronically filed the foregoing document with the Clerk of the Court using CM/ECF.

/s/Thomas Haggerty
Thomas Haggerty
Assistant United States Attorney