UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Case No. 24-cr-417 (CKK)**
	:	
MARLON FERRO, also known as "Marlo," and "GothFerrari,"	:	
	:	

GOVERNMENT'S MEMORANDUM IN AID OF SENTENCING

Defendant Marlon Ferro (hereinafter, "the defendant") was a vital cog in the social engineering ("SE") enterprise that successfully defrauded several victims out of millions in cryptocurrency holdings throughout 2024. The defendant was tasked with conducting home invasions of individuals thought to possess millions worth of cryptocurrency on unhosted, hardware wallets which would have otherwise been inaccessible to the social engineers. Furthermore, once his co-conspirators in the enterprise were able to successfully steal cryptocurrencies from their victims, the defendant assisted them in spending and laundering their ill-gotten gains. Finally, the defendant continued to assist the leader of the enterprise, co-defendant Malone Lam, long after the latter was arrested in September 2024 by using fraud proceeds to pay Lam's prior attorneys, providing luxury goods to Lam's paramour, and selling off Lam's clothing and shoe collection among other things. In light of the foregoing, and particularly in light of the defendant's resorting to home invasions to assist the enterprise, the United States believes that a substantial carceral sentence is warranted and recommends that the defendant be sentenced to 78 months' incarceration to be followed by 36 months of supervised release.

I. FACTUAL AND PROCEDURAL HISTORY

On April 30, 2025, a federal grand jury sitting in Washington, D.C. returned a Superseding Indictment against multiple individuals, including the defendant, charging him specifically with

one count of Conspiracy to Participate in a Racketeer Influenced and Corrupt Organization, in violation of 18 U.S.C. § 1962(d), one count of Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1343, and one count of Conspiracy to Launder Monetary Instruments in violation of 18 U.S.C. § 1956(h). Law enforcement arrested the defendant on May 13, 2025, and the defendant later appeared in United States District Court for the District of Columbia on May 19, 2025, where he was arraigned on the Superseding Indictment. On October 17, 2025, the defendant pled guilty to Count One of the Superseding Indictment pursuant to a written agreement with the government. In support of the guilty plea, the defendant agreed to and acknowledged the following factual proffer under oath:

The Social Engineering Enterprise

The Social Engineering Enterprise ("SE Enterprise") was made up of a group of individuals based in California, Connecticut, New York, Florida, and abroad. The SE Enterprise began on a date unknown but by no later than October of 2023 and continued through at least in or around March 2025. Members and associates of the SE enterprise served different roles and held different responsibilities. The roles included database hackers, organizers, target identifiers, callers, money launderers, and residential burglars targeting hardware virtual currency wallets. Ferro was a residential burglar and money launderer for the SE Enterprise. The purposes of the SE Enterprise included, but were not limited to, stealing virtual currency from victims throughout the United States through fraudulent pretenses; disguising, concealing, and obfuscating the source and ownership of the stolen funds through the use of virtual currency laundering techniques; and converting laundered virtual currency into fiat currency and wire transfers for use at nightclubs, for the purchase of exotic cars, jewelry, luxury handbags, clothing, private jet rentals, and rental mansions in Los Angeles, the Hamptons, and Miami.

Members and associates of the SE Enterprise used stolen virtual currency to purchase, among other things, (1) nightclub services ranging up to $500,000 per evening, (2) luxury handbags valued in the tens of thousands of dollars which were given away at nightclub parties, (3) luxury watches valued between $100,000 up to over $500,000, (4) luxury clothing valued in the tens of thousands of dollars, (5) rental homes in Los Angeles, the Hamptons, and Miami, (6) private jet rentals for travel, (7) a team of private security guards, and (8) a fleet of exotic cars, ranging in value from $100,000 up to $3,800,000.

On or around February 23, 2024, Ferro agreed with another cybercriminal to commit a residential home burglary in Winnsboro, Texas from victim T.C. Ferro was provided money for travel, an address and location, and the code to the victim's safe. Ferro's goal was to steal a hardware wallet from the victim believed to contain

approximately 100 bitcoin ("BTC"), then valued at over $5,000,000. Ferro traveled to Winnsboro, Texas, broke into the victim's home, and stole the hardware wallet containing the 100 BTC. Ferro and the other cybercriminal then transferred the funds through various cryptocurrency exchanges to disguise the origin, source, and ownership of the funds. Ferro received a large percentage of the stolen funds for his role in the residential burglary.

Ferro met the SE Enterprise members when he moved to California in early 2024 following this Texas burglary. Ferro met Hamza Doost ("Doost") and Austin Fine ("Fine") when he moved to California and needed crypto-to-cash services to convert his stolen cryptocurrency. Upon his arrival in California, he began using Doost to launder stolen cryptocurrency into fiat cash for use at Los Angeles nightclubs.

Ferro ingratiated himself in the SE Enterprise and became close friends with Fine and Malone Lam ("Lam"). Ferro offered Lam and others his residential burglary services for cryptocurrency thefts as part of the SE Enterprise.

In or around July 2024, Ferro agreed to travel to New Mexico from California to execute a home break-in to search for a virtual currency hardware wallet. Lam and Veer Chetal ("Chetal") asked Ferro to perform this home break-in because they believed that the victim held approximately $30,000,000 in virtual currency on his hardware wallet. Ferro arrived in New Mexico and positioned a cell phone in front of the victim's home for surveillance. Lam also tracked the victim's location by logging into his iCloud account. When the group believed the victim had departed the residence, Ferro entered the rear of the home, broke into the home by smashing a window with a brick, entered the home, and scoured the home for the hardware wallet. Ferro took various digital devices but was unable to find the target hardware wallet. Ferro was captured on the victim's surveillance camera breaking into his home.

Ferro solicited additional home break-in targets from Chetal in August 2024. On August 31, 2024, Ferro sent Chetal a series of messages stating, "I'm getting surgery so if you need targ[et]s hit lmk [let me know] before those days." Ferro sent Chetal a message on September 7, 2024, stating, "Need licks," referring to robbery targets.

Ferro also assisted members of the SE Enterprise in purchasing luxury goods with stolen cryptocurrency. On August 31, 20245, Ferro sent Chetal a message with his year-to-date spending on Amiri clothing, which showed $255,060 in purchased clothing by Ferro on behalf of Chetal. Ferro then used Joel Cortes ("Cortes") to ship designer clothes to Chetal after Ferro purchased the clothing in Los Angeles with stolen cryptocurrency.

Ferro learned that Lam, Chetal, Jeandiel Serrano ("Serrano") and others stole approximately $248,000,000 from Victim-7 almost immediately after the theft occurred. Ferro was with Lam for portions of the crime. Ferro openly discussed the theft with Chetal on Telegram, criticizing Serrano for his rush to launder his cut of the stolen money. Ferro stated, through several messages, "John [Serrano] is so fucking stupid. It fucking hurts. Why can't anything just go too plan. What's so hard about waiting too clean 50 MILLION. Dollors. Why is he so impatient knowing he has trusted people cleaning it. Like what was the point of Malone sweating his ass off cleaning John shit little by little. Bro. He just

fumbled. 250m. Lick. Just by being. Stupid."

Ferro also procured fraudulent know-your-customer documents from a Lithuanian individual and used them to open a RedotPay digital payment-card account to be used by members of the SE Enterprise to spend their stolen cryptocurrency at physical retail locations and nightclubs. Redotpay provides digital payment cards that can be stored on mobile telephones and used to pay for goods and services in person. Users transfer cryptocurrency to their Redotpay account and draw down on the account balance through purchases, like a debit card. Redotpay account registration is geo-blocked in the United States and the United States is listed as a restricted location on the Redotpay website. Ferro used these foreign identification documents to create the account so that SE Enterprise members including Chetal, Lam, and Serrano could use the account to spend their stolen cryptocurrency. Ferro arranged for cryptocurrency stolen by Chetal, Lam, and Serrano to be loaded onto the Redotpay account through him. Ferro then shared the account access with Chetal, Lam, and Serrano. Members of the SE Enterprise then used this account to purchase luxury goods at retail stores and nightclub services, throughout Miami and elsewhere. Ferro used the identification documents of a Lithuanian individual, instead of his own, so as to mask the source, location, and ownership of the account and the spending occurring through the account. Many of the transactions involved purchases over $10,000 in proceeds of the specified unlawful activity.

Following Lam's arrest in September 2024, Ferro collected funds from other SE Enterprise members to pay for Lam's attorneys knowing that the funds were proceeds of specified unlawful activity. Specifically, Ferro received hundreds of thousands of dollars in cryptocurrency, converted it into different types of cryptocurrencies, then converted it into fiat cash through illicit crypto-to-cash services. He converted the funds to wires and used the funds to pay for Lams attorneys. Ferro also facilitated and organized the purchase and shipment of Hermes Birkin bags on behalf of Lam for his Miami girlfriend while Lam was incarcerated.

Ferro was arrested on May 13, 2025, and possessed a fake identification document and two firearms.

Ferro agrees that it was reasonably foreseeable to him that at least $3.5 million in cryptocurrency would be stolen by members of the SE Enterprise in furtherance of the objects of the SE Enterprise. Ferro also agrees that he was assisting other members of the SE Enterprise to spend their stolen cryptocurrency and disguise and conceal the nature, location, source, ownership, and control of the stolen cryptocurrency.

See ECF No. 226. As the Statement of Facts makes clear, it "does not purport to be an inclusive recitation of everything that the Defendant heard, knew, or witnessed concerning the illegal activities committed by Defendant and others. It is intended to represent sufficient information for the Court to find a factual basis for accepting the Defendant's guilty plea." *Id.*

II. DISCUSSION AND APPLICATION OF U.S. SENTENCING GUIDELINES AND 3553(a) FACTORS

A. Generally Applicable Legal Principals

When determining the appropriate sentence, the district court should consider all of the applicable factors set forth in 18 U.S.C. § 3553(a). See *United States v. Gall*, 128 S. Ct. 586, 596 (2007). The listed factors in 18 U.S.C. § 3553(a) include the following:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed –
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> > (B) to afford adequate deterrence to criminal conduct;
> > (C) to protect the public from further crimes of the defendant; and
> > (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
>
> (3) the kinds of sentences available;
>
> (4) the kinds of sentence and the sentencing range established for –
>
> > (A) the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines –
> >
> > > (i) issued by the Sentencing Commission ...; and
> > >
> > > (ii) that, . . . are in effect on the date the defendant is sentenced; ...
>
> (5) any pertinent policy statement –
>
> > (A) issued by the Sentencing Commission ... and
> >
> > (B) that, . . . is in effect on the date the defendant is sentenced.

> (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
>
> (7) the need to provide restitution to any victims of the offense.

With respect to the U.S. Sentencing Guidelines, while they are no longer binding, they should inform the Court's approach to fashioning a sentence that will effectuate the aforementioned goals in § 3353(a). This is so because, as the Supreme Court has recognized, the Guidelines themselves "seek to embody the § 3553(a) considerations, both in principle and in practice." *See Rita v. United States*, 551 U.S. 338, 350, (2007). As the Court elaborated, given the difficulties in balancing the "abstract and potentially conflicting nature of § 3553(a)'s general sentencing objectives, and the differences of philosophical view among those who work within the criminal justice community as to how best to apply general sentencing objectives, it is fair to assume that the Guidelines, insofar as practicable, reflect a rough approximation of sentences that might achieve § 3553(a)' s objectives." *Id.*

B. Guidelines Calculations

Turning to 3553(a)(4)(A), upon reviewing the Pre-Sentence Investigation Report (hereinafter, "PSR"), the government agrees with the calculations of U.S. Probation regarding the defendant's Final Offense Level under the U.S. Sentencing Guidelines (hereinafter, "Guidelines" or "USSG") as well as USPO's calculation of his criminal history. As such, the parties agree about the ensuing USSG range.

1. Offense Level

The Guideline for a violation of 18 U.S.C. § 1962(d) is found at § 2E1.1, which provides that the base offense level for this charge is the greater of either 19 or the base offense level for the underlying racketeering activity. *See* USSG § 2E1.1. As the PSR correctly notes, when there is more than one underlying offense, each offense is to be treated as a separate count of conviction

and the rules regarding grouping apply. *Id.* Here there are two groups of offenses that underly the defendant's conviction on Count One – Conspiracy to Commit Wire Fraud and Laundering Monetary Instruments. *See* PSR at ¶¶ 43-44. Under the terms of the plea agreement as well as the relevant Guidelines provisions, these two categories are grouped together under USSG § 3D1.2(c). *Id*. at ¶ 45. Under USSG § 3D1.3(a), the highest offense level of the "counts" in the group applies to the entire group as a whole. Here that would be § 2S1.1, the guideline for Laundering Monetary Instruments. With respect to that Guideline, the base offense level for § 2S1.1 is the offense level for the underlying offense from which the funds were derived if the defendant committed the underlying offense (or would otherwise be held accountable for it) and the offense level for that can be determined. *See* USSG § 2S1.1(a)(1). Here, the underlying offense would be Wire Fraud, which is governed by § 2B1.1. Under § 2B1.1, the base offense level begins at 7 and because the intended loss was more than $3,500,000 but less than $9,500,000, that is then increased by 18 levels to 25. An additional two levels are added because the offense involved a substantial financial hardship to one or more victims pursuant to § 2B1.1(b)(2)(A)(iii) (though, for purposes of § 4C1.1 the government has agreed that the defendant did not personally cause the hardship), while a further two levels are added because of the defendant's engagement in sophisticated means to accomplish the fraud under § 2B1.1(b)(10)(C). As such the base offense level is 29. Given that the defendant would have been convicted under 18 U.S.C. § 1956, there is a two-level increase as dictated by § 2S1.1(b)(2)(B). Furthermore, because the offense involved sophisticated laundering, there is a further two-level increase. *See* § 2S1.1(b)(3). The Adjusted Offense Level, therefore, is 33.

Because the defendant has accepted responsibility early in the pendency of this case, he is ultimately entitled to a three-level decrease under § 3E1.1. Furthermore, the government does not

contest that he meets the criteria for Zero Point Offender status set forth in § 4C1.1(a)(1)-(11).[1] As a result, his offense level is reduced by a further two levels, leading to a Final Offense Level of 28.

2. Criminal History

The government agrees that the defendant has no criminal convictions and thus his total criminal history score is zero and he falls within Criminal History Category ("CHC") I. *See* PSR at ¶ 60.

3. USSG Range

At a Total Offense Level of 28, in CHC 1, the defendant's resulting Guidelines range is 78-97 months, within Zone D. In Zone D, the only Guidelines-compliant sentence is one of incarceration. *See* USSG § 5C1.1(f).

C. Recommendation

The United States believes that a sentence of 78 months' incarceration – the bottom of the defendant's properly calculated Guidelines range – is sufficient but not greater than necessary to effectuate the purposes of 18 U.S.C. § 3553(a). The defendant was a key member of the enterprise, conducting a home invasion to access hardware wallets that other members of the enterprise could not otherwise socially engineer and hack their way into. Furthermore, once the enterprise had obtained their ill-gotten gains, the defendant facilitated their expenditure of the stolen cryptocurrency, *even after multiple individuals had been arrested, charged, and were being preventatively detained in local jails*. Against these factors, which might otherwise augur in favor of a top-of-the-Guidelines sentence, the defendant was only 18 at the time of the offense, has no

[1] As will be explained *infra* at II.C.1, while the defendant did admit to burglarizing at least two residences as part of his Statement of Offense, neither involved the use of physical force against another or the use of firearms or other dangerous weapons.

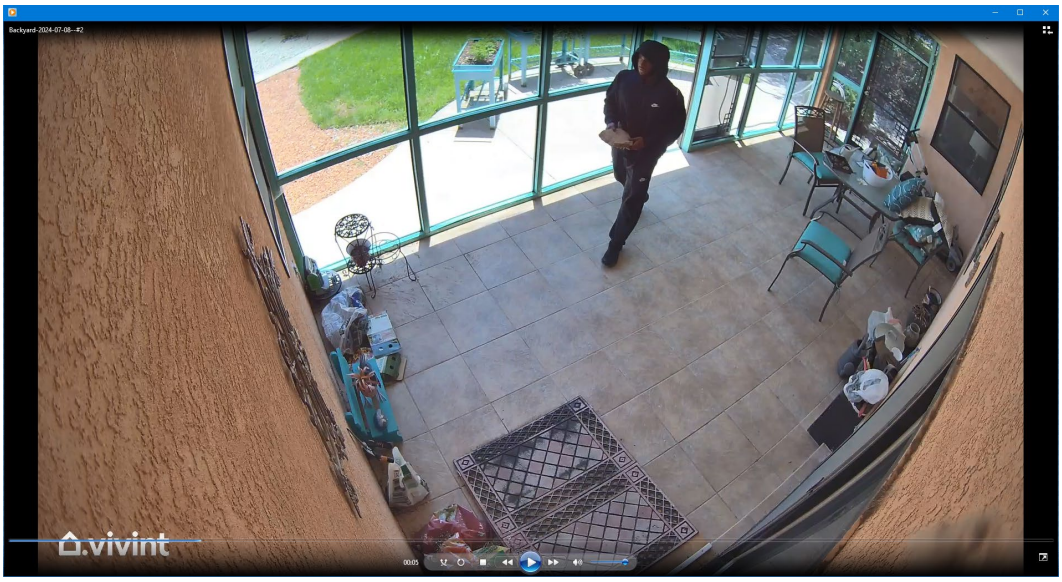
prior criminal history, and quickly accepted responsibility within mere months of being charged with his participation in a complex racketeering conspiracy. As such, a low-end Guideline sentence adequately accounts for his role within the conspiracy and the actions he undertook as a member of the enterprise, while appropriately reflecting his age, lack of criminal history, and acceptance of responsibility.

1. Nature and Circumstances of the Offense

The defendant was an active and critical contributor to the charged social engineering enterprise that successfully stole more than $250,000,000 from victims throughout the United States. He broke into one residence on behalf of the charged enterprise (and a separate home on behalf of another), helped launder the proceeds of their large-scale thefts to enable them to spend the victims' cryptocurrencies on various luxury expenses, and provided vital assistance to co-defendant Lam after his arrest, charging, and pre-trial detention. To begin, while typically, as this Court knows, the conspirators typically stole cryptocurrency through calling victims whom they had identified as likely having significant digital assets and socially engineering them to the point where they gained access to their personal email accounts and later their software wallets, this was not always the case. Rather, some of the victims kept their cryptocurrency holdings not in software wallets that could be accessed via the internet, usually on a virtual currency exchange, such as Coinbase or Gemini, but in hardware wallets. Hardware wallets are physical, removable devices that store a user's private keys and can be connected to a computer when the user wishes to use the private keys store on the wallet for virtual currency transactions. *See* Second Superseding Indictment, ECF No. 229, at ¶ 9. To access these devices, members of the charged enterprise would need to send someone to the location where the device was being held and steal it. This is where the defendant came in.

As the Statement of Offense makes clear, the defendant had already performed at least one

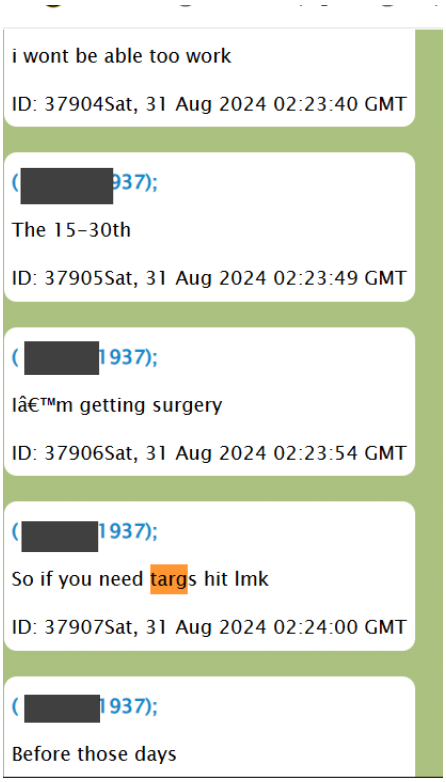
home invasion at the behest of another cybercriminal. Much like the instant matter, the purpose of the defendant's break-in was to steal a hardware wallet from the victim, believed to contain bitcoin, which he did successfully, before ultimately teaming with the cybercriminal to launder the funds through various cryptocurrency exchanges. In the course of his laundering of the proceeds of his home invasion and crypto-theft, the defendant connected with a member of the charged SE enterprise who assisted the defendant in converting his digital assets into fiat currency for things like nightclub services. Thereafter, he gradually ingratiated himself into the charged SE enterprise and offered his home invasion services to co-defendant Lam. Things came to a head in July 2024, when the defendant agreed with other members of the enterprise to fly to New Mexico to steal a hardware wallet belonging to V-4, who the SE enterprise had identified as having significant holdings of digital assets in hardware wallets after having successfully socially engineered V-4 into giving them access to his e-mail account. The defendant went about his usual process, flying out and casing the location for several days, putting a cell phone in front of the residence to monitor V-4's whereabouts and develop a rough pattern of life, and then coordinating with other members of the enterprise to time the break-in when V-4 had left his home as the defendant's co-conspirators had access to V-4's iCloud and could track his whereabouts. When the group believed the victim had departed the residence, the defendant broke into the home by smashing a window with a brick, entered, and began scouring the home for the hardware wallet. The defendant took various digital devices but was unable to find the target hardware wallet. The foregoing was captured on a Ring home surveillance camera V-4 had set up at his residence. *See* Gov. Ex. 1.



Still from Gov. Ex. 1.

Ultimately, the defendant took the digital devices he stole to his rental unit where he attempted to access them, but was unsuccessful and eventually discarded them.

The unsuccessful home invasion, however, did little to deter the defendant. He reached out to other members of the SE enterprise to see if they needed any help with additional "targs" or locations to burglarize. In the exchange below, the defendant plans with a coconspirator in advance of a medical procedure. He tells the coconspirator to let him know about any "targs" or targets in advance, because he will be unable to victimize targets during a two-week period.



Screenshot of the defendant's text message with CC-1

He followed-up with CC-1 approximately one week later and stated that he needed "licks."

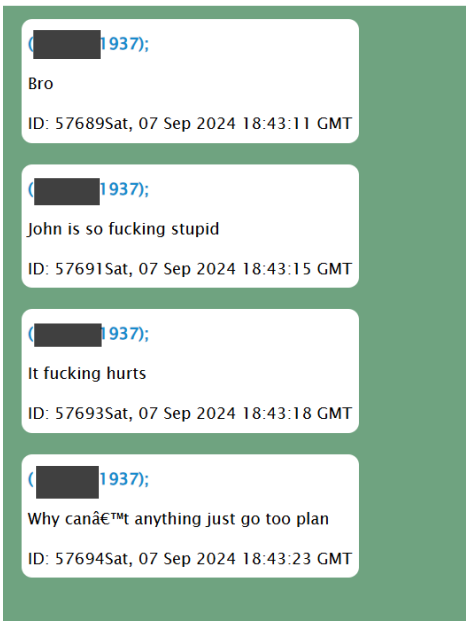
Yet the defendant was not simply the proverbial muscle for the SE enterprise, breaking into residences to steal hardware wallets from unwitting victims. He also played a key role in laundering the proceeds of the enterprise's various crimes. Upon stealing cryptocurrency from other victims, including V-7, the defendant and his co-conspirators spent it by using a digital payment card provided by Company # 1. Company # 1 provides users with physical and digital cards that can store cryptocurrency and allow it to be spent at participating physical retail locations. U.S.-based users cannot access and complete account registration paperwork for this website as it is geo-blocked. To circumvent this restriction, the defendant provided fraudulent identification documentation he obtained from a foreign national to register with Company # 1 (and comply with

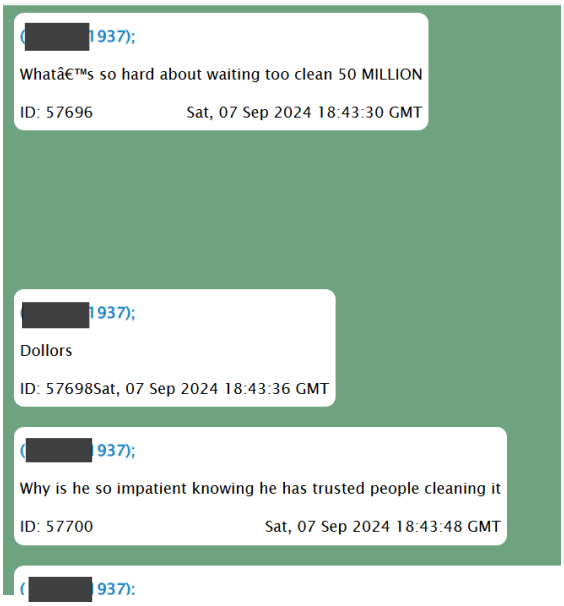
the "Know Your Customer" provisions) and obtain a digital payment card on which to store and ultimately spend stolen cryptocurrency. Once the card was in hand, the defendant coordinated with other co-conspirators on transferring digital assets to the card.

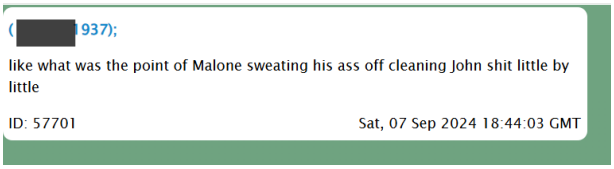
He also counseled other members of the conspiracy on how to use the card properly, particularly in order to avoid Company # 1 freezing funds due to money laundering concerns. In one exchange from September 16, 2024, the defendant had the following exchange with a fellow-co-conspirator.

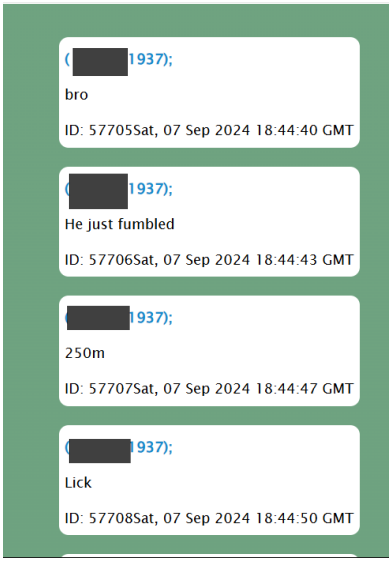
FERRO: If you are going to pay don't use Ethereum… Malone sent 200k and it's still pending on eth…Tether only…Usdt
CC-2: Yeah bro I told him I think it's 100k per right?
* * *
CC-2: Yeah Jesus bro the thing is the 200k he sent was my 200k… Yeah bro defo cause it's above 99k … It fcked it
FERRO: I just hope they don't ask for kyc… I deleted my old tele with my kyc guy

In addition, he spoke frequently about how other co-conspirators were laundering additional proceeds from their criminal activity. In the below-message, for example, from August 2024, he complained that co-defendant Jeandiel Serrano was not waiting to launder his money till co-defendant Lam finished the laundering process for his cut. He then lamented at how Serrano was jeopardizing the "250m" "lick," or the theft from Victim-7 in August 2024 in which co-defendants Serrano and Lam stole approximately $240,000,000 worth of bitcoin.









And then, even after co-defendants Lam and Serrano were apprehended on September 18, 2024 – with the defendant being present at the former's arrest – the defendant did not attempt in any way to distance himself from the charged enterprise. If anything, his role was elevated within

it. Once co-defendant Lam was detained, the defendant served as his primary conduit to the outside world and members of the charged enterprise. As the government previously set forth in its Emergency Motion for *De Novo* Review of the Magistrate's Release Order, ECF No. 67, co-defendant Lam directed the defendant to contact additional criminals and collect money on his behalf.

Date/Time	Facility	Direction	Other Party	Person Of Interest	Subject	Message
12/04/2024 05:32 PM	VA - Alexandria Detention Center VA	Outgoing	Marlon Ferro (Disconnected)	MALONE LAM	RE: Hello	Get me in contact with 41, tell him I want to speak to him. Ask Ethan what he did with Jae's watch, tell him I'm the one asking. Get me in contact with Gerred, ask around for it, tell him I want to speak to him.
12/05/2024 10:11 PM	VA - Alexandria Detention Center VA	Outgoing	Marlon Ferro (Disconnected)	MALONE LAM	RE: Hello	Tell that nigga 41 to stop talking about what I tell him / don't tell anyone what I tell him, not Ethan, not Cody, nobody
12/07/2024 03:52 PM	VA - Alexandria Detention Center VA	Incoming	Marlon Ferro (Disconnected)	MALONE LAM	Hello	41 Said " No response"
12/07/2024	VA -	Incoming	Marlon Ferro	MALONE	RE: call	Bet let me text him

"41" is a well-known hacker working with the group. "Ethan" is a reference to co-defendant Ethan Yarally, who at the time was a fugitive in the United Arab Emritaes. "Gerred" is a reference to another social engineer caller working with the enterprise.

The defendant also assisted Lam in using Lam's leftover remaining stolen cryptocurrency to purchase luxury handbags for his Miami girlfriend. The purses, Hermes Birkins, retail for multiple tens of thousands of dollars, a picture of which is below:

Additionally, the defendant would discuss how to budget the stolen proceeds that still remained with the enterprise and how co-defendant Lam would spend them. On December 10, 2024, for example, Lam asked "What's the word with the Chanel bag and do you have someone that can wrap it as Christmas presents and send it away? I want the Chanel stuff and Birkin wrapped and I want a bouquet of roses all sent together too." Ferro responded "XMR is down SO much i'm gonna send you a pic, you wont be able to afford both. I say you get her two or 3 purses that are channel and then later we get her the Birkin… I sent you the screen shots showing proof of the xmr, I would cover but i also have to get liz and my parents things. I don't spawn in 10 million a week." Lam responded "isn't Conor [Flansburg] sending money? I'm so confused… And Ethan [Yarally] sent you 55k, you said I had 25k too." Lam continued by saying "bro what? firstly its not 10? to swap xmr to tether and secondly the 55k dropped to 42k, I still had money, that's just money from Ethan [Yarally] wtf are you saying lol." Ferro responded with "10% to change it into cash lol," referencing the fee charged for unlicensed crypto-to-cash exchangers. Lam replied, "stop fucking telling me this and that you had so much of my $ that Gerred gave, not just from Ethan [Yarally]." This is another conversation where Lam discusses how Ferro received a significant

amount of money from the cybercriminal "Gerred" on Lam's behalf, in addition to $55,000 from co-defendant Yarally.

***

In sum, the defendant was a committed member of the social engineering enterprise that stole hundreds of millions of dollars from innocent victims across the United States. He was deeply embedded in its workings and fully cognizant of the scale of its operations. While this fact, in and of itself, underscores just how serious this offense is, the defendant was not any ordinary member of the enterprise, he was the person they relied to conduct home break-ins of potential victims, the person they trusted to coordinate and facilitate the spending of the stolen proceeds, and the person that co-defendant Lam confided in once he was in jail for these offenses. This conduct alone warrants a significant carceral sentence.

2. History and Characteristics

While the defendant lacks any criminal history, the government does not believe that factor should be assigned significant weight given that he was only 18 at the time of the charged conduct in this case, giving him insufficient opportunity to accumulate a serious criminal history. Furthermore, within a month of turning 18, he was resorting to home break-ins on behalf of cybercriminals, as the defendant acknowledged in his Statement of Offense. More concerningly, the PSR reveals precious little about what would have impelled the defendant into this type of activity. The defendant grew up in a stable, loving family in Las Vegas, Nevada, *see* PSR at ¶¶ 64-66, where he graduated from high school, *see id.* at ¶ 78, and ultimately continued to pursue additional educational opportunities thereafter, *id.* at ¶ 79.

Nevertheless, by his own admission, the defendant was in "deep" with the enterprise quickly after he turned 18. And as stated above, the defendant persisted in his activity with the SE enterprise even after multiple co-conspirators were arrested. Furthermore, as the government

alluded to in its filings regarding the defendant's potential pre-trial detention, *see* ECF Nos. 67, 98, at the time he was arrested in May 2025, law enforcement found multiple firearms, magazines, and ammunition in his California home as shown below.

9-millimeter black rifle taken from defendant's

Glock 19 9-millimeter firearm bearing Serial Number 0710USMC

Partially loaded 9-millimeter magazine

Additionally, marijuana and Adderall were also found in the apartment, along with fake identification. Consequently, even by the time of his arrest, the defendant was engaged in further criminal activity.

3. Need for Sentence Imposed

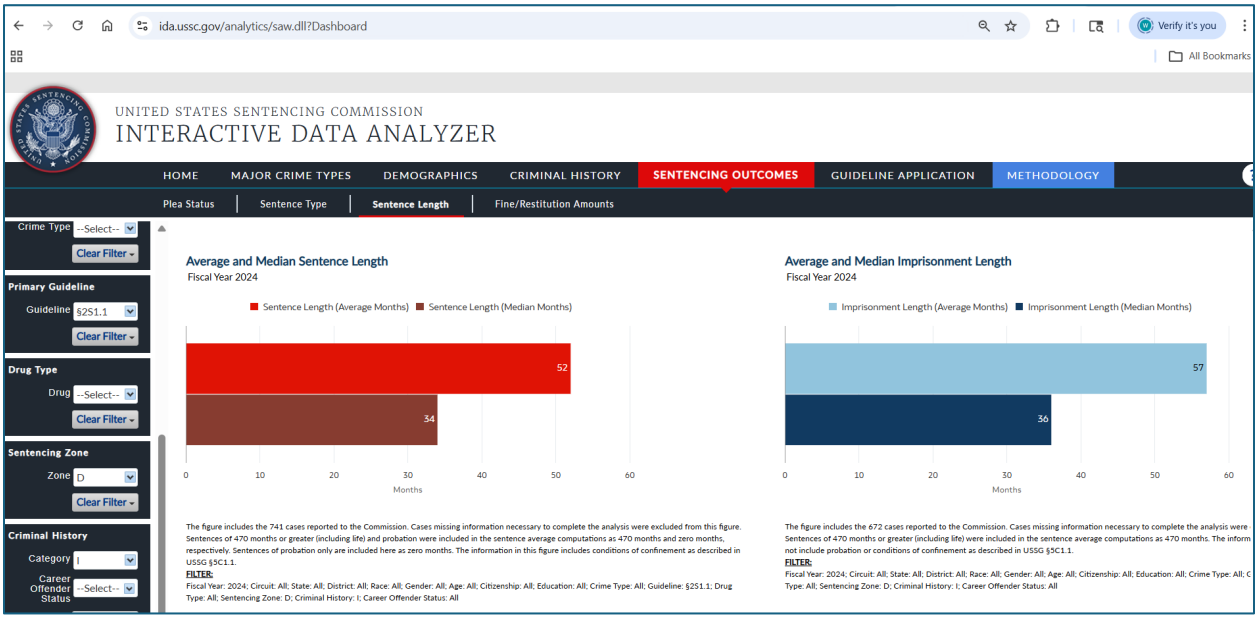
The government believes that its proposed sentence will best effectuate the purposes of sentencing as set forth in 3553(a)(2)(A)-(D), that is, for the sentence imposed to reflect the seriousness of the offense, promote respect for the law, and provide just punishment for the offense; afford adequate deterrence of criminal conduct; protect the public from further crimes of the defendant; and provide the defendant with training, treatment, and other type of care he may require. Only a sentence with a significant period of incarceration would accomplish these goals. The defendant was a key member of a sprawling criminal conspiracy that affected countless victims and took it upon himself to conduct home invasions on behalf of the enterprise to access virtual currency wallets that it could not otherwise access by virtue of online social engineering.

He then helped launder the stolen millions in cryptocurrency and facilitated his co-conspirators' dissipation of victim funds on items such as luxury handbags. Only a Guidelines-compliant sentence could underscore the severity of the conduct at issue here and adequately punish the defendant for his various crimes committed on behalf of the enterprise. Furthermore, the sentence the Court hands down must have a significant deterrent effect. Social engineering scams to fleece unwitting cryptocurrency holders out of their holdings are proliferating. *See, e.g.,* Anas Hassan, "Victim Loses $282M in Bitcoin and Litecoin to Hardware Wallet Scam," Yahoo! Finance, Jan. 26, 2026, *available at* https://finance.yahoo.com/news/victim-loses-282m-bitcoin-litecoin-185821837.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAA9QtYFxHjJa-ZUH9PautBMpQh1LQchb0ls__93EUyPAvoKF3D0w-xUpxbFxPKrsrBPKGxL2E-GgsHfl5E9-RhNrUwk6E7qLQf490OndCX2yz8QxRJO32yxbZAieCe95-8i8ecnew-PSR3tPKCkCT5t5DcKU1rM33JJAPpn8jyi5. A significant carceral sentence within the Guidelines range communicates the message that these offenses – particularly where individual residences are being invaded – will be punished severely. While admittedly there are certain mitigating factors at play, most notably the defendant's youth and lack of criminal history as well as his swift acceptance of responsibility, these are sufficiently taken into account by the government's recommendation of a sentence at the very bottom of his Guidelines range.

4. *Avoiding Unwarranted Sentencing Disparities*

The government's sentencing recommendation is sufficiently proximate to sentences imposed for similar conduct for defendants in the same criminal history category. As the below chart from the U.S. Sentencing Commission's Interactive Data Analyzer demonstrates, for

defendants in Criminal History Category I, sentenced with § 2S1.1 as their primary guideline, the average imprisonment length was 57 months.



As the PSR points out, the Judiciary Sentencing Information ("JSIN"), includes data suggesting that for defendants with a primary sentencing Guideline of 2S1.1 and a Final Offense Level of 28, the average length of imprisonment was 65 months and the median was 68 months. *See* PSR at ¶ 111. The government's recommendation is slightly higher, but again, is within the range prescribed by the Guidelines, which themselves are meant to guard against unwarranted disparities. *See United States v. Bartlett*, 567 F.3d 901, 908 (7th Cir. 2009) ("The best way to curtail 'unwarranted' disparities is to follow the Guidelines, which are designed to treat similar offenses and offenders similarly."); *see also Molina-Martinez v. United States,* 578 U.S. 189, 193 (2016) ("Uniformity and proportionality in sentencing are achieved, in part, by the Guidelines' significant role in sentencing."). Furthermore, while the government's recommendation is slightly higher than the average based on the JSIN data, this appropriately reflects significant aggravating factors in the defendant's conduct, including the fact that to steal cryptocurrency, his job was to surveil targets'

homes and break into their residences to steal their prized assets. Consequently, any disparity between the government's recommendation and the median / average length of similarly situated defendants would not be unwarranted.

III. CONCLUSION

WHEREFORE, the government recommends that the defendant be sentenced to a term of imprisonment of 78 months, to be followed by a period of 36 months of supervised release.

Respectfully submitted,

JEANINE FERRIS PIRRO
UNITED STATES ATTORNEY

WILL HART
Assistant United States Attorney
U.S. Attorney's Office for the
District of Columbia
D.C. Bar No. 1029325
601 D. St., N.W.,
Washington, D.C. 20530
William.hart@usdoj.gov
(202)-252-7877