IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. CAMERON ALBERT REDMAN Defendant.	Case No. 1:25-cr-129 Hon. Leonie M. Brinkema

POSITION OF THE UNITED STATES WITH RESPECT TO SENTENCING

Cameron Redman is a serial online fraudster. After being incarcerated for a year for stealing $40 million in a SIM swapping attack, he almost immediately returned to online criminal activities. His next round of sophisticated fraud schemes—the crimes at issue here—resulted in financial losses totaling at least hundreds of thousands of dollars to approximately two hundred victims in a remarkably short period of time. He unsuccessfully sought to target even more victims, failing only due to technical difficulties. A Guidelines sentence of 35 months is necessary and appropriate to reflect the seriousness of the defendant's crimes and deter him from future criminal conduct. Such a sentence will also give the defendant an important opportunity to disconnect from the harmful communities he has found on the internet and take advantage of the Bureau of Prison's services for rehabilitation.

FACTUAL BACKGROUND

The defendant has established himself as a sophisticated, successful, and repeat cybercriminal. In his most recent criminal forays, the defendant was a critical member of two different teams determined to steal non-fungible tokens—a form of cutting-edge digital art

referred to as NFTs—and sell them before anyone realized that a crime had been committed. *See* ECF No. 26, Statement of Facts (SOF), ¶ 5.

The defendant's frauds with CC-2 and CC-3

In May 2022, the defendant formed his first conspiracy when he and co-conspirator 3 (CC-3) compromised Victim 1's X account with the goal of stealing NFTs. *Id.* ¶ 6. To assume control of this account, the defendant gained unauthorized access to X's customer support panel for major users of X's platform, known as the Partner Support Panel. The defendant then submitted a support ticket to X through the Partner Support Panel falsely claiming to be an authorized user of Victim 1's X account. *Id.* The defendant and his co-conspirator successfully persuaded X to change the email address on the account to an email that the defendant and his co-conspirator controlled. *Id.* From there, the co-conspirators were able to submit a password reset request, receive the password change email at the address they controlled, reset the account password, and lock Victim 1 out of his account. *Id.*

Once in control of Victim 1's X account, the co-conspirators posted a link to a fraudulent website. *Id.* ¶ 7. This website encouraged visitors to enter a raffle to win new, unique NFTs that were supposedly created by Victim 1. *Id.* Because this purported raffle was an unusual occurrence that offered the chance to win a potentially valuable digital asset, victims were incentivized to move quickly to avoid missing out on this limited-time opportunity. But when the victims clicked to enter the raffle, they thought they were authorizing a transaction to *receive* NFTs into their digital wallets; in fact, they were authorizing the defendant and his co-conspirators to *remove* all of the cryptocurrency and NFTs from their wallets. *Id.* ¶¶ 8, 11.

When the original website that the defendant and his co-conspirator built had trouble stealing NFTs and cryptocurrency, they expanded their conspiracy. *Id.* ¶ 9. The new co-

conspirator, CC-2, built a new website that mimicked Victim 1's legitimate website and used a more effective tool for stealing funds from victims' digital wallets. *Id.* The co-conspirators promoted this new website—again using the defendant's ill-gotten access to Victim 1's X account—claiming that Victim 1 was releasing a limited number of pieces of new digital art. *Id.* Once again, victims thinking they were receiving NFTs unwittingly authorized the defendant and his co-conspirators to drain all of the cryptocurrency and NFTs from their wallets. *Id.* ¶ 11. CC-2 then sold these NFTs for cryptocurrency. *Id.* ¶ 13.

Victim 1 regained control of his account the same day that the defendant and his co-conspirators launched their attack. *See id.* ¶ 12. Yet even in this short time frame, the co-conspirators defrauded at least 80 victims and made $446,756. *Id.* ¶ 13. Despite the scheme's overall profitability, however, CC-2 did not share the profits with the defendant. *Id.*

The defendant's mentorship of CC-1

After failing to personally profit from an otherwise wildly successful fraudulent scheme, the defendant realized he needed to change his business practices. He therefore sought to sell his access to X's Partner Support Panel, thus ensuring he profited before the rest of the fraud even got off the ground. In pursuit of these guaranteed returns, the defendant agreed to sell CC-1 exclusive access to the Partner Support Panel in June 2022 for a fee of 230 Ether (a cryptocurrency) and a 10 percent cut of the profits from all of CC-1's phishing scams that used the Partner Support Panel. SOF ¶ 15. At the time, 230 Ether was worth approximately $283,411, *id.*; at today's valuation, it is worth upwards of $860,000.

The defendant's involvement in CC-1's scheme did not end with this sale, however. Though CC-1 had general plans to steal NFTs, he did not understand all of the mechanics of how such a fraud would work, and he certainly did not know how to access or use the Partner Support

Panel. The defendant stepped in to mentor CC-1, instructing him on how to put the fraudulent scheme in motion. *See id.* ¶ 16. As he had in the attack on Victim 1, the defendant and his new co-conspirators gained control of victims' X accounts by convincing X customer support to change the email address assigned to a digital artists' account. The co-conspirators would then reset the password and lock the victim out of their account. *See id.* But for the co-conspirators' email change requests to X to be processed in the first place, they needed to be believable. The defendant therefore taught CC-1 how to identify top media companies who would be likely to represent significant digital artists. The defendant instructed CC-1 on how to create email addresses that appeared to be associated with those media companies. *Id.* After that, the defendant showed CC-1 how to access the Partner Support Panel, provided him with a template message to send to X requesting an email account change, and provided instructions on how to avoid detection. *Id.* In other words, without the defendant's tutelage, this fraud scheme would not have gotten off the ground.

But the defendant did not stop there. Instead, he personally participated in the attacks themselves, demonstrating first-hand how to implement the skills and techniques that he had just taught. For example, the defendant identified the first victim for the group to target and walked CC-1 and other co-conspirators through how to gain control of Victim 4's account. *Id.* ¶ 17. After the defendant helped them launch the scheme, the other co-conspirators built the spoof website, stole the victims' NFTs, and sold them online. *Id.* ¶ 18. This scheme netted the group over $24,000 from at least 27 victims in just about one day's time. *Id.* ¶ 23. The defendant personally made $15,000 from this attack. *Id.* ¶ 24.

The defendant similarly directly participated in the attacks on Victims 5, 2, and 3. For the attack on Victim 5, the defendant helped identify not only the victim, but also the media

company that the co-conspirators would impersonate, and he guided another co-conspirator through the process of gaining access to Victim 5's X account. *Id.* ¶ 25. For the attack on Victim 2, the defendant created the email address designed to impersonate the media agency and then personally sent the emails through the Partner Support Panel to gain control of Victim 2's account. *Id.* ¶ 31. For the attack on Victim 3, the defendant again selected the media company to impersonate and assisted with gaining control of Victim 3's X account. *Id.* ¶ 38. In these three attacks alone, the defendant and his co-conspirators stole NFTs from over 100 victims, netting approximately $323,000. *See id.* ¶¶ 28-29, 35-36, 42-43. The defendant himself made approximately $100,000 to $120,000 from these three attacks—well more than the 10 percent he had originally negotiated. *See id.* ¶¶ 29, 26, 43. Overall, the defendant's two conspiracies made over $794,000.[1] The defendant and his co-conspirators also attempted to compromise other victim accounts, but had minimal success with these other efforts, often because they could not compromise the X account in the first instance. *Id.* ¶ 44. Ultimately, the scheme disbanded when the Partner Support Panel stopped working.

Procedural Posture

The defendant was charged by complaint on April 17, 2024. He was arrested in Portugal on December 3, 2024. He arrived in the United States on March 19, 2025, and made his initial appearance in the Eastern District of Virginia on March 20, 2025. The defendant entered a guilty plea on May 8, 2025.

[1] This gain significantly understates the amounts that the victims lost because the co-conspirators would frequently sell NFTs well below their market rate in order to offload them quickly. For example, one victim purchased an NFT in April 2022 for $90,313. The co-conspirators sold it just three months later for only $12,312.

SENTENCING ANALYSIS

I. Statutory Penalties and Guidelines Calculations

As this Court is aware, to determine the appropriate sentence, the Court must consult both the Guidelines and the factors set forth in 18 U.S.C. § 3553(a). Here, the PSR correctly calculated the Guidelines with a total offense level 20, a criminal history category I, and a Guidelines range of 33 to 41 months.[2]

II. Section 3553(a) Factors

After calculating the Guidelines range, a sentencing court must then consider that range, as well as the sentencing factors set forth in 18 U.S.C. § 3553(a) and determine a sentence that is appropriate and reasonable for the individual defendant. *Nelson v. United States*, 555 U.S. 350, 351 (2009). The United States recommends that the defendant be sentenced within the Guidelines to a term of imprisonment of 35 months. Such a sentence is appropriate in light of the defendant's past criminal history, from which he appears to have learned no lessons; reflects the seriousness of the defendant's crime; will provide the defendant an opportunity to take advantage of Bureau of Prison mental health resources; and is necessary for general deterrence.

a. Nature and Characteristics of the Defendant and the Need for Specific Deterrence

The defendant apparently grew up as an awkward kid with a troubled home life. But though the internet is full of myriad communities offering healthy support and beneficial connections, he instead chose instead to immerse himself in the world of cybercrime. Likewise, instead of applying himself to learning in school, he applied himself to learning sophisticated cybercrime techniques. For his first foray into crime (or at least the first foray for which he was

[2] The government moves for the additional one-point reduction in the defendant's offense level based on early acceptance of responsibility.

caught and punished), he executed a complicated SIM-swapping scheme resulting in the theft of approximately $40 million *in one day, from one victim*. ECF No. 29 (PSR) at ¶ 81. Only a small portion of these funds have ever been recovered. *Id.*

Even though he was a juvenile, and even though he was convicted and punished in Canada, he still received a year of incarceration as punishment for this crime. Though one year is a significant sentence for a juvenile, it appeared to have no deterrent effect. Within at least one year of being released, the defendant was camped out in his father's basement looking for—and finding—new ways to profit from crime.

Though the defendant was released from jail in May 2021 and was not re-incarcerated until December 2024, he took no steps during this more than three-and-a-half-year period to meaningfully improve his position or opportunities in life. He has not completed any educational or vocational training. He has not developed any job skills. In fact, it appears he has never held a job and has instead supported himself by gambling and living off of his criminal proceeds. PSR ¶ 107. Similarly, he has no discernible ties to any community.

Notably, the defendant was responsible for the "social engineering" aspects of the fraud schemes. In other words, it was his job to manipulate and deceive others into giving him what he was not otherwise authorized to have. Moreover, though the defendant committed his first crime alone, he stepped up into a mentorship and training role for his second go-round.[3] The defendant taught at least one other cybercriminal—a juvenile—important elements of how to execute complex frauds. Though the defendant's psychological evaluation repeatedly notes his social

[3] The defendant in his reports to probation and his psychologist has emphasized that the publication of his SIM-swapping crime brought hardship to his family. However, in online criminal communities, this public attribution in fact enhanced the defendant's reputation and standing.

isolation and limitations, he in fact appears quite adept at interacting with and reading people when doing so serves his financial interests.

In sum, the defendant has demonstrated that he consistently chooses wrong. He chose the wrong communities online. He chose not to learn any lessons from his prior run-in with the law. He chose not to seek education, job opportunities, or other personal development when he was released, and instead chose to return to the criminal opportunities that were easily available to him. He chose not to pursue mental health treatment or addiction counseling or healthier connections, but instead chose to return to the criminal communities he already knew. A sentence of 35 months is necessary for the defendant to realize that these choices are no longer available to him. A 35-month sentence is necessary to deter him from returning to the unsuccessful and criminal life with which he is most familiar.

b. Seriousness of the Offense and Protecting the Public

With just a few days' work, without any notable physical exertion, and at no particular risk to himself, the defendant and his co-conspirators defrauded over 200 victims and made approximately $794,000, defrauding victims of even more. Moreover, unlike his first crime, the defendant did not act independently. Instead, he partnered with numerous other co-conspirators that he met online. A "conspiracy poses a 'threat to the public' over and above the threat of the commission of the relevant substantive crime—both because the 'combination in crime makes more likely the commission of other crimes' and because it 'decreases the probability that the individuals involved will depart from their path of criminality.'" *United States v. Jimenez Recio*, 537 U.S. 270, 275 (2003) (quoting *Callanan v. United States*, 364 U.S. 587, 593–594 (1961)). This threat was realized in this case, where the defendant's mentoring, guidance, and support

ensured that the crime got off the ground successfully when it otherwise might have failed before it even began.

In addition to being extremely profitable for relatively little work, the defendant's crimes undermined the trust and confidence in the new but growing cryptocurrency and digital art community. He exploited the trust that numerous successful digital artists had built with their followers, capitalizing on their hard-won reputations, carefully curated online presences, and trusting communities to line his own pockets. As one of the victims explained, he viewed himself as a "builder, investor, and active community member" in the NFT community who was "supporting artists, joining digital communities, attending in-person meetups, and forming friendships through shared passion." This fraud "shook [his] trust in the communities [he] loved," leaving him feeling "betrayed, ashamed, and isolated" and with "lingering psychological stress." As he explained, these crimes "aren't just internet hacks," but are "attacks on culture, connection, and livelihood." Crimes like the defendant's are about "broken trust, in the platforms we use, the communities we nurture, and the believe that innovation in digital spaces can be pursued safely."[4]

Thus, a sentence of 35 months' imprisonment is necessary to reflect the seriousness of the offense and the defendant's conduct.

c. Providing the Defendant with Needed Training and Care

The parties appear to agree that the defendant at this point would be best served by pursuing some form of formal education and receiving treatment and care for his mental health and addictions. The defendant's history of failing to seek this care on release indicates he is most likely to receive this support while in a structured setting. The defendant is thus likely to benefit

[4] This victim's impact statement will be provided separately to the court.

from the educational and perhaps vocational opportunities available to him while he is incarcerated. The government also recommends that the defendant be required to obtain counseling and treatment for mental health and addiction while incarcerated.

d. Need to Afford Adequate General Deterrence

The court cannot overlook the need in these cybercrime cases for general deterrence. General deterrence plays a vital role in the protection of society from calculated yet difficult-to-detect crimes. "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. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994). Moreover, because crimes like the defendant's are "more rational, cool, and calculated than sudden crimes of passion or opportunity," these crimes are "prime candidate[s] for general deterrence." *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006); *see also United States v. Morgan*, 635 F. App'x 423, 450 (10th Cir. 2015) ("General deterrence comes from a probability of conviction and significant consequences. If either is eliminated or minimized, the deterrent effect is proportionately minimized."). The Fourth Circuit, as well as Congress, has emphasized the importance of deterrence in difficult to detect crimes:

> [T]he Commission's focus on incarceration as a means of third-party deterrence is wise. The vast majority of such crimes go unpunished, if not undetected. Without 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. Engle, 592 F3.d 495, 502 (4th 2010); *accord* S.Rep. No. 98–225, at 76 (1983), reprinted in 1984 U.S.C.C.A.N. 3182, 3259. Simply put, the Government cannot deter difficult-to-detect criminal schemes like the defendant's unless there is a meaningful punishment for

egregious conduct. The government's sentencing recommendation of 35 months satisfies this need for general deterrence.

III. Restitution

The government requests that the Court impose restitution of $248,257.07. This number is a conservative estimate of the losses incurred by two victims that the government has been able to identify. The government has undertaken extensive efforts to identify and contact other victims, but at this time can only tie specific loss amounts to these two victims. The government has provided documentation regarding these two victims' losses to defense counsel, and the parties will attempt to reach an agreement on restitution prior to sentencing.

The PSR incorrectly indicates a higher restitution number, divided amongst the five victims identified in the Statement of Facts. *See* PSR ¶ 63. However, that total number reflects the total gain to the co-conspirators that the scheme generated for each account hack, not a restitution amount due to any one victim. Additionally, Victims 1 through 5 did not suffer direct financial losses because of the defendant's crimes. Instead, the chart should be read to indicate that, e.g., the defendants made $446,756.92 from the attack on Victim 1's account. The government raised this error with Probation after the PSR was finalized and was advised that Probation would submit an amended PSR following sentencing.

IV. Fine

Section 5E.12 of the Guidelines states that the Court "shall impose a fine in all cases, except where the defendant establishes that he is unable to pay and is not likely to become able to pay any fine." The fine range typically depends upon the offense level, except section 35E.12(c)(4) provides that "limiting the maximum fine, does not apply if the defendant is convicted under a statute authorizing (A) a maximum fine greater than $500,000 . . . In such cases, the court may

impose a fine up to the maximum authorized by the statute." Under 18 U.S.C. § 3571 (b) and (d) the maximum fine that the defendant can receive is the greater of $250,000 or twice the gross gain or loss. Here, the gross gain (and a conservative measure of the gross loss) is $794,263.80, and twice that gain is $1,588,527.60.

The government recommends that the defendant be required to pay a fine of $794,263.80. As an initial matter, the defendant has more than sufficient funds available to pay the maximum fine of twice the gross gain. PSR ¶ 109. So far, the main lesson the defendant appears to have learned from his criminal activities is that crime does, in fact, pay. In light of the defendant's extensive fraudulent conduct, the fact that his wealth appears to derive entirely from this conduct, the limited restitution he appears likely to have to pay, and his ability to pay, the government believes that a fine of the gross gain from the defendant's present offense is necessary and appropriate.

CONCLUSION

For the reasons stated, the United States requests that this Court impose a term of incarceration of 35 months.

Respectfully Submitted,

Erik S. Siebert
United States Attorney

Date: _July 22, 2025_____

_____/s/_____
Zoe Bedell
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Ave
Alexandria, Virginia 22314
Phone: 703-299-3700
Zoe.bedell@usdoj.gov