

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	24-CR-494 (CKK)
	:	
VEER CHETAL,	:	UNDER SEAL
Defendant.	:	
	:	

**GOVERNMENT’S *EX PARTE* MOTION FOR REVOCATION OF DEFENDANT’S
RELEASE AND REQUEST THAT THE COURT ISSUE A BENCH WARRANT**

The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, respectfully files this *ex parte* request that the Court issue a bench warrant for defendant Veer Chetal based on information recently learned by the government, which establishes that the defendant committed additional crimes while cooperating with the government and hid those crimes from the government in violation of his plea agreement. The government has also learned that the defendant lost his visa, withdrew from university, and plans to leave the country. The government requests that the Court temporarily seal this motion, the proposed order, and proposed bench warrant to prevent the defendant’s flight. After the defendant is arrested, the government requests that the Court hold a hearing, pursuant to 18 U.S.C. § 3142(f), formally revoke his release conditions, and order him detained pending sentencing.

I. BACKGROUND

A. Procedural History

On August 18, 2024, victim R.W. was defrauded out of over 4,100 Bitcoin (“BTC”). The FBI executed a search warrant at the defendant’s New Jersey apartment on or about September 9, 2024. Defendant agreed to cooperate with law enforcement and began providing information regarding his co-conspirators. He was appointed counsel during the week of September 9, 2024.

His co-conspirators, Malone Lam and Jeandiel Serrano, were arrested on September 18, 2024. The prosecution team met with the defendant through video conferences on several occasions met in person with Mr. Chetal on September 26, 2024 as well as on November 13, 2024.

On November 13, 2024, the defendant entered a guilty plea to a two-count Information charging him with conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 and conspiracy to engage in money laundering in violation of 18 U.S.C. § 1956(h). *See ECF Doc. 9.* Defendant was permitted to remain on pre-trial release as he attempted to provide assistance to the Government in this and other investigations.

B. Facts Regarding the Defendant and the Scheme

As part of his plea agreement with the government, the defendant admitted to the following facts before the Court during his plea hearing. *See ECF Doc. 8.*

Chetal met co-conspirators Malone Lam (“Lam”) and Jeandiel Serrano (“Serrano”) playing the game Minecraft online. From in or around November 2023 and continuing through at least September 2024, Chetal, Lam, and Serrano, and others (“the conspirators”) agreed to participate in a conspiracy designed to steal virtual currency from unwitting victims. The conspirators caused multiple wire communications to be transmitted in interstate commerce, including into the District of Columbia, to further the object of the conspiracy.

The conspirators utilized social engineering techniques to trick victims into providing private information over the telephone that allowed the conspirators to steal victims’ virtual currency holdings. Social engineering is a term used to describe a fraud scheme where criminal actors impersonate employees from trusted companies, send spoofed emails and websites, or employ related techniques designed to convince a victim to disclose valuable personal information that can be exploited for profit.

Lam's role in the conspiracy was to obtain breached databases containing lists of high net-worth subjects who would be targeted by the conspirators for social engineering schemes. Lam would further the scheme by causing "account access attempt" notifications to be sent to victims in order to make them believe there had been unauthorized attempts to access their online accounts.

Chetal and Serrano participated in the conspiracy, by among other things, calling potential victims on the telephone and pretending to be representatives from security or technical support teams at major companies such as Google and Yahoo!. Chetal served in this role, in furtherance of the conspiracy, on approximately 50 separate occasions. Chetal and Serrano would convince the victims of their legitimacy and then cause them to click on Lam's account access request notifications that were masked to appear as if they were originating from the victim's home IP address.

Once the victims were convinced to click on prompts allowing account access, Lam used the access to scour the accounts for virtual currency seed phrases, wallet addresses, and additional information relating to their financial currency holdings.

The conspirators then either transferred victim assets themselves, or caused the victims to transfer their virtual currency, into wallet addresses controlled by the conspirators. The conspirators then used virtual currency exchanges and professional money launderers to conceal and disguise the origin and ownership of the stolen virtual currency.

Victim R.W.

On or about August 18, 2024, the conspirators used social engineering techniques to defraud victim R.W. out of approximately \$245,093,239.00 in Bitcoin ("BTC").

In the days leading up to the theft, Lam caused Google account access attempt

notifications to be sent to R.W. The purpose of these notifications was to give more legitimacy to the next step in the scheme.

On August 18, 2024, Chetal called R.W. at his home in Washington, D.C. and claimed to be a Google representative following up on unauthorized account access attempts. Chetal convinced R.W. that he was assisting R.W. in securing his Google account against these unauthorized access attempts. In reality, Chetal and Lam were communicating through Discord and Telegram during this interaction and strategizing about ways to gain access to R.W.'s Google account, including his OneDrive.

Chetal used the Discord display name "Swag," and the Telegram display name "Wiz," or "W."

Lam used the Discord display name "Anne Hathaway," and the Telegram display name "\$ \$ \$" and "Ms. Jackson."

Lam quickly searched R.W.'s emails and saved files to locate victim R.W.'s virtual currency holdings once they gained access to R.W.'s Google accounts. Lam discovered files indicating that R.W. held a significant amount of virtual currency with the Gemini virtual currency exchange and custodial bank. Chetal ended the phone call with R.W. after this discovery and Chetal and Lam reached out to Serrano to continue the scheme.

The conspirators joined two group chats, on Telegram and on Discord, and agreed to continue the fraud scheme against R.W. Chetal and Lam continued using the same screen names and Serrano began using the Discord display name "VersaceGod," and the Telegram display name "!" and "@SkidStar."

Serrano proceeded to call R.W. and claim to be a representative of Gemini's security team calling to alert R.W. about a malware attack affecting his virtual currency wallet. Serrano, with

the real-time support and advice of Chetal and Lam over Telegram and Discord, convinced R.W. to provide private keys to a portion of his virtual currency holdings. Lam used this information to transfer an initial tranche of R.W.'s virtual currency assets into his control.

Serrano, with the support and advice of Lam and Chetal, then convinced R.W. to download a remote desktop connection program that allowed the group to view a mirrored image of R.W.'s desktop computer as he navigated through personal files and virtual currency private keys. Lam used this access to transfer an additional tranche of R.W.'s assets into his control.

In total, the conspirators defrauded R.W. out of approximately 4123.71908099 BTC valued at approximately \$245,093,239.00 on August 18, 2024.

The conspirators successfully defrauded numerous victims in the same manner. At times, Lam would send spoofed webpages or "panels" to victims to trick the victims into loading passwords and other sensitive information into a panel that would transmit the information directly back to Lam. The conspirators would then exploit the information for financial gain.

Money Laundering Conspiracy

From in or around November 2023 and continuing through at least September 2024, the conspirators (including Chetal, Lam, Serrano, and others) agreed to divide the proceeds of their fraud scheme and to launder those proceeds so as to conceal and disguise the nature, location, source, ownership, and control of the proceeds so that the conspirators could convert the proceeds into "clean" fiat currency that could be freely spent on goods including jewelry, purses, cars, rental homes, and nightclub services. This was accomplished through common cryptocurrency laundering techniques, such as changing Bitcoin in the XMR Monero, using peel chains, pass through wallets, and cryptocurrency exchange platforms that do not require detailed know your customer ("KYC") information. The conspirators also enlisted the assistance of professional

money launderers operating on darknet markets.

The conspirators further agreed and intended that, to effectuate the laundering and to enjoy the proceeds, they would engage in transactions in such proceeds of the fraud in amounts well above \$10,000. The conspirators used trusted professional money launderers to assist them in completing transactions in excess of \$10,000 when the transactions involved the proceeds of the specified unlawful activity.

In furtherance of that conspiracy, in August 2024, Lam transferred R.W.'s assets into a wallet address that was not readily attributable to the conspirators, including in amounts over \$10,000 per transaction. Lam then divided the proceeds in five equal parts, between Lam, Serrano, Chetal, and two other individuals identified as "Meech" and "~ ~". "Meech" and "~ ~" had previously assisted the conspirators in other social engineering schemes.

Chetal laundered his funds through multiple virtual currency exchanges that did not require extensive, or any, KYC information. Members of the conspiracy also laundered his stolen funds through a Russian money laundering network operating on the dark-web forum Exploit.in. The conspirators' purpose of this laundering was to make it difficult or impossible to trace their virtual currency back to the initial theft from R.W.

Chetal used his portion of the laundered virtual currency to make several purchases in excess of \$10,000. The items included watches, designer clothes, and multiple luxury automobiles. Chetal used a Los Angeles-based money launderer, Austin Fine, to turn this stolen virtual currency into fiat currency and luxury goods. Fine charged a 10% fee for the conversion. Fine shipped watches and fiat currency across the country to Chetal. Fine shipped fiat cash across the country hidden in stuffed animals.

On September 9, 2024, agents with the Federal Bureau of Investigation ("FBI") executed

a search warrant at Chetal's rental home in Brunswick, New Jersey. Chetal was in possession of approximately \$37,000,000 in stolen virtual currency, obtained through the R.W. theft. Chetal transferred the \$37,000,000 into the custody of the FBI.

Overall, Chetal began engaging in social engineering fraud schemes with Lam, Serrano, and others beginning in or around November 2023. Chetal was involved in defrauding approximately 50 victims during this time that resulted in over \$3,000,000 in personal proceeds, before and in addition to the \$245,093,239.00 from R.W. The conspirators accomplished the objects of the conspiracy by transmitting wires in interstate and foreign commerce.

C. Conditions of Release

The plea agreement contained the following language regarding the defendant's release:

Your client acknowledges that, although the Government will not seek a change in your client's release conditions pending sentencing, the final decision regarding your client's bond status or detention will be made by the Court at the time of your client's plea of guilty. The Government may move to change your client's conditions of release, including requesting that your client be detained pending sentencing, if your client engages in further criminal conduct prior to sentencing or if the Government obtains information that it did not possess at the time of your client's plea of guilty and that is relevant to whether your client is likely to flee or pose a danger to any person or the community. Your client also agrees that any violation of your client's release conditions, any misconduct by your client, or any inability or failure on the part of your client to continue your client's cooperation with the Government, may result in the Government filing an ex parte motion with the Court requesting that a bench warrant be issued for your client's arrest and that your client be detained without bond while pending sentencing in your client's case. *ECF Doc. 9, ¶ 8.*

The Government is now in possession of information that was not in its possession at the time of the defendant's guilty plea regarding the defendant's criminal activity. Defendant has now failed to cooperate with law enforcement in providing truthful information and may be preparing to leave the United States. This is the type of "misconduct" and "failure on the part of [defendant] to continue [his] cooperation with the Government" that is contemplated by the plea agreement

and justifies an *ex parte* motion for a bench warrant. Additionally, failing to disclose his involvement in another crime occurring during the period of his cooperation, in which he was involved, may be considered obstruction of justice in violation of 18 U.S.C. § 1512 or false statements in violation of 18 U.S.C. § 1001. For these reasons, the Government requests a bench warrant to arrest the defendant and have him detained pending a full detention hearing and sentencing.

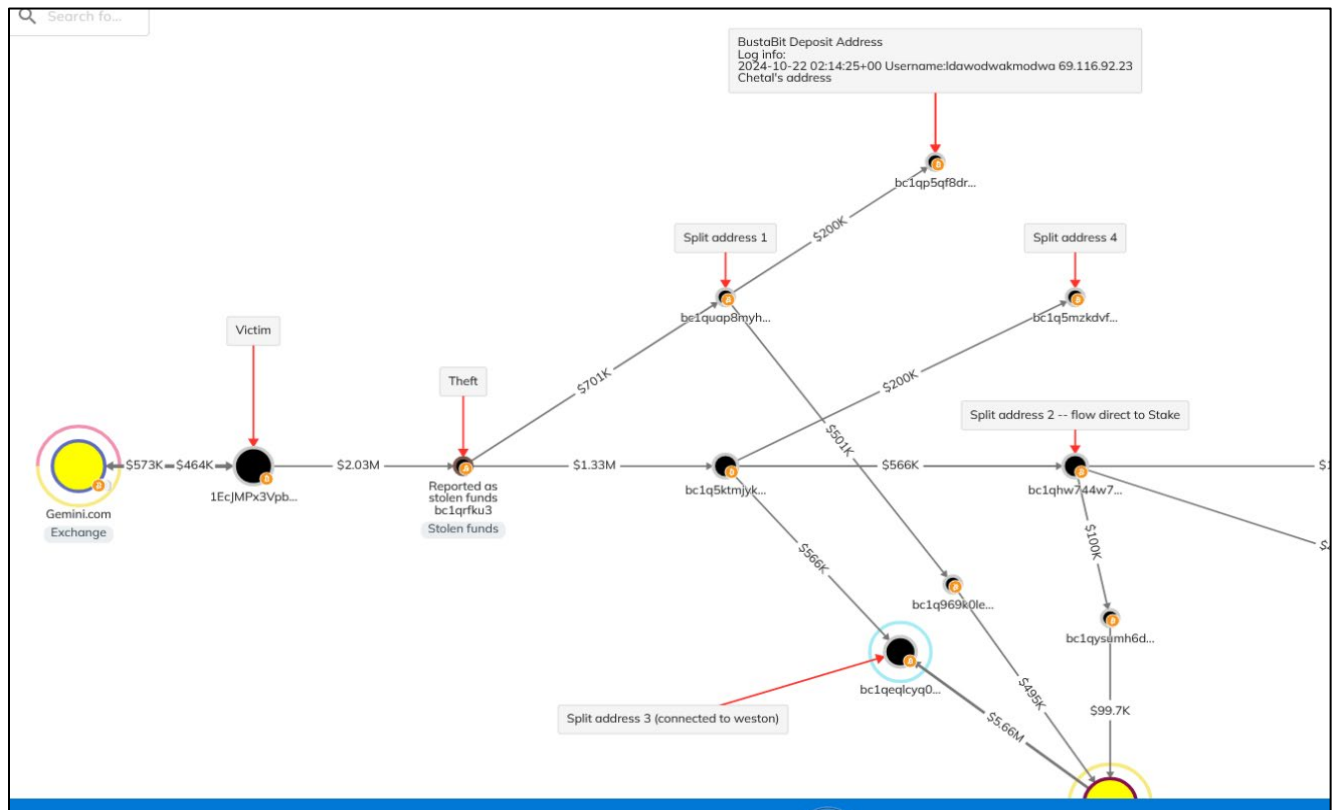
D. Newly Discovered Criminal Conduct

The FBI and IRS-CI have continued to investigate this and other cryptocurrency social engineering schemes victimizing citizens throughout the United States. To that end, the IRS-CI contacted victim M.D., a New Jersey resident who was the victim of a social engineering attack on October 21, 2024.¹ This attack will sound eerily familiar to the Court as it involves the same *modus operandi* as the defendant's prior criminal conduct. M.D. explained that the fraud started when she received a phone call from someone claiming to be a support team member from Google. She subsequently received a phone call from someone purporting to be from the Gemini cryptocurrency exchange support team. The callers informed M.D. that her Gemini account was compromised and that the hackers were moving funds from her bank account to her Gemini account. The caller further convinced M.D. that in order to secure her funds, she needed to provide the "seed phrases" to her cryptocurrency wallet where other funds were stored. The caller sent M.D. a web link to input her private seed phrases. M.D., convinced of the callers' legitimacy, input

¹ This attack occurred one month after the defendant began cooperating with the FBI and approximately three weeks before the defendant formally entered his guilty plea with the Court. Defendant has been given every opportunity to voluntarily disclose his involvement in this October offense and has declined to do so through multiple interviews.

her seed phrases into the website. Later that day, approximately \$2,000,000 in cryptocurrency was stolen from her cryptocurrency wallet without her consent.

IRS-CI tracked the stolen cryptocurrency through recognized and reliable blockchain tracing tools. The blockchain tracing showed the initial \$2,000,000 in stolen funds being split into two transactions of \$701,000 and \$1,300,000 arriving in two separate addresses. The address receiving the \$701,000 then withdrew \$200,000 to an online cryptocurrency gambling account with BustaBit and sent the remaining \$501,000 to the eXch cryptocurrency exchange, which is a well-recognized exchange used by money launderers and criminals due to its complete lack of KYC requirements and refusal to engage with law enforcement. Portions of the stolen funds also arrived at one of the same cryptocurrency addresses used during the R.W. theft, indicating the same actors were involved in both attacks.



The online gambling company, BustaBit, provided records for the account that received the \$200,000 in stolen funds. The username is listed as “ldawodwakmodwa” with an email address of customerhelp1@proton.me. The account was opened on October 22, 2024 shortly after the theft. The account received \$200,000 in stolen funds approximately eight minutes after being created.

The account was accessed six different times during its existence over the course of less than an hour. On five of the six times, the owner used a virtual private network to disguise their identity. On one of the six occasions, within 40 minutes of account opening and 30 minutes of receiving the stolen funds, the account VPN network “failed” and the true IP address leaked.

A	B	C	D
timestamp	user	ip_address	
2024-10-22 01:46:58+00	ldawodwakmodwa	188.241.176.223	
2024-10-22 01:47:15+00	ldawodwakmodwa	188.241.176.223	
2024-10-22 01:53:48+00	ldawodwakmodwa	188.241.176.223	
2024-10-22 02:14:25+00	ldawodwakmodwa	69.116.92.23	
2024-10-22 02:15:20+00	ldawodwakmodwa	188.241.176.223	
2024-10-22 02:15:22+00	ldawodwakmodwa	188.241.176.223	

The above image shows the IP addresses from which the account was accessed. The IP address 69.116.92.23 is registered to Yaana Technologies. Yaana Technologies in turn identified the subscriber for the IP address as Sushil Chetal, the defendant’s mother. The Defendant’s New Jersey address is also the listed residential address for the IP address used to access the BustaBit account receiving the stolen cryptocurrency.

56390-ALUS-Subscriber Information Printout	
Target:	<ul style="list-style-type: none"> • Subscriber with IPV4 Address 69.116.92.23
Account Number:	07875-467428-05
Subscriber:	SUSHIL CHETAL
Service Address:	236 PARK LANE DUNELLEN, NJ 08812
Telephone #(s):	(203)512-2232
Account Activation date:	06/29/2024 to present
MAC Address:	944E5B6B5460
Email Address:	sushilchetal@yahoo.com

In summary form, \$2 million in cryptocurrency is stolen from M.D. on October 21, 2024, over a month after the defendant began “cooperating” with law enforcement through a nearly identical scheme as the R.W. theft detailed in the defendant’s plea agreement. The stolen cryptocurrency is divided through split addresses and at least \$200,000 ends up in an online gambling account created minutes after the M.D. theft. Additional funds end up in one of the same addresses used in the R.W. theft. The gambling account containing the stolen funds is then accessed from the IP address registered to the defendant’s home. Nine minutes later the account gambles away the stolen funds in one bet.

On January 10, 2025, the prosecution team obtained a search warrant to acquire historical cell tower information for the defendant’s cell phone, to determine whether he was present at his New Jersey home when the October 21, 2024 theft occurred and the BustaBit account was accessed from his residential IP address (25-SC-16). Records produced by T-Mobile place the defendant’s cell phone at his home in New Jersey at the time of the offense and at the time the account was created and accessed.

Finally, on January 21, 2024, the prosecution team met with the defendant and his attorney to ask the defendant if he was aware of any additional criminal activity or social engineering schemes not previously detailed in several interviews. The defendant denied knowledge of any criminal activity since the arrest of his co-conspirators on September 18, 2024. He denied engaging

in any cryptocurrency transactions, he denied receiving any cryptocurrency from unknown sources, and he denied engaging in any additional criminal activity since he was first interviewed by the FBI in September. He denied knowing of any additional social engineering schemes. He also stated that he lives alone and no one else has access to his home.

E. Flight Risk Factors

Defendant is not a United States citizen. He was present in the United States on his father's work visa. The government recently learned that his father lost his job, and in turn, his work visa. Defendant has now withdrawn from Rutgers University and is no longer attending college.

Within the last two weeks, a law enforcement source informed the prosecution team that the defendant was gathering high school documents so that he could apply for colleges in Dubai. For context, multiple members of this cyber-crime social engineering community are currently located in Dubai and reside there due to the country's favorable extradition laws.

Upon learning this information, undersigned counsel immediately contacted the pre-trial services agency to inquire whether they possessed the defendant's passport, which they do not.²

During the January 21, 2024 meeting, the prosecution team asked the defendant what he intended to do in the United States now that he has withdrawn from college. Defendant informed the participants that he intends to move back to India with his parents and look for a university in India. As an initial matter, international travel is strictly prohibited. As a supplemental matter, defendant denied his intent to travel to Dubai for school.

Because the Defendant is facing a Guidelines sentencing range of 235 -293 months, is in possession of his passport, no longer has ties to the community, and is planning international travel,

² As of January 24, 2025 he has not turned in his passport. Pre-trial services was notified that he plans to overnight mail his passport on Monday, January 27, 2025.

he was not directly confronted with his concealed criminal conduct committed while ostensibly cooperating with law enforcement. Put plainly, defendant has every incentive to flee the country if given notice that the government has discovered his additional criminal conduct and the breach of his plea agreement and the government made a calculated assessment not to arouse suspicion.

II. APPLICABLE LAW

The Bail Reform Act “requires that detention be supported by ‘clear and convincing evidence’ when the justification is the safety of the community.” *United States v. Simpkins*, 826 F.2d 94, 96 (D.C. Cir. 1987). A determination that an individual is a flight risk must be supported by a preponderance of the evidence. *United States v. Vortis*, 785 F.2d 327, 328–29 (D.C. Cir. 1986) (per curiam).

D.C. Circuit precedent permits the Government to proceed by way of proffer at a detention hearing. See *United States v. Smith*, 79 F.3d 1208, 1209-10 (D.C. Cir. 1996); see also *United States v. LaFontaine*, 210 F.3d 125, 131 (2d Cir. 2000) (“proffers are permissible both in the bail determination and bail revocation contexts.”).

The four factors that the Court must consider under section 3142(g) are (1) the nature and circumstances of the offense; (2) the weight of the evidence; (3) the history and characteristics of the defendant, including her criminal history, and (4) the nature and seriousness of the danger to any person or the community posed by the defendant’s release. 18 U.S.C. § 3142(g). The Section 3142(g) factors all warrant the defendant’s detention under 18 U.S.C. § 3142(e).

III. ARGUMENT

Defendant’s Newly Discovered Criminal Conduct Demands his Arrest and Detention.

Had the government known of the defendant’s October 2024 criminal activity while “cooperating” with law enforcement, it would not have agreed to his release pending sentencing.

Considering his lack of community ties, lack of candor regarding criminal activity, and intention for international travel, the Court should now have similar concerns regarding his pre-trial release.

A. The factors in section 3142(g) support the defendant's detention under section 3142(e)(1).

The Nature and Circumstances of the Offense

The nature of defendant's previously admitted conduct is serious. He engaged in a long-running scheme to steal vast amounts of cryptocurrency from private citizens across the country. His scheme operated on fraud and deceit, fooling victims into believing his representations that he was working for Google and calling to assist them through a cyber intrusion. Defendant began the scheme in the end of 2023, continued it through the R.W. theft, and even after he was confronted by law enforcement and began "cooperating" with the FBI. Defendant spent millions of dollars on expensive automobiles, private jets, and jewelry, and gambled away \$200,000 in victim M.D.'s money in a single wager after the theft in between proffer interviews with the government and his attorney.

As a result, he faces a Guidelines range of 235 to 293 months based on an offense level of 38. This factor weighs in favor of detention.

Weight of the Evidence

Defendant has already admitted to his pervasive and long-running conduct. Now the government has discovered that he continued to commit this conduct while cooperating with law enforcement and then hid the information during multiple interviews. The M.D. \$2,000,000 theft was executed in the same manner as the R.W. theft. The money moved through one of the same addresses as the R.W. theft, and \$200,000 of the stolen funds was deposited into the defendant's gambling account, accessed from his residential IP address where only he lives. This factor weighs in favor of detention.

History and Characteristics of the Defendant

Defendant is not a United States citizen, has no job, is not enrolled in school, and has plans to leave the country. He has no ties to the United States. The vast majority of his time as an adult has been spent defrauding innocent victims out of their cryptocurrency holdings. This factor weighs in favor of detention.

Nature and Seriousness of the Danger to any Person or the Community

The defendant has demonstrated that even after beginning to cooperate with law enforcement, he will continue to commit crimes. He was approached by the FBI in early September 2024 and began providing the FBI with useful information that led to the arrest of his co-conspirators on September 18, 2024. Within a month of this arrest, the defendant was involved in another substantial theft of \$2,000,000. The government now has little confidence that the community can remain safe while the defendant remains at large. The government has no confidence that any set of conditions, or combinations of conditions can protect the safety of the community.

Risk of Flight

Defendant contacted his local high school and asked for graduation documents, citing his intent to apply for university in Dubai. Defendant told the prosecution team something completely different this week and cited his intent to move back to India for school. Either way, the Court is now presented with a defendant lacking citizenship, a visa, a job, college enrollment, or any ties to the United States whatsoever. He has no incentive to stay in the United States and every incentive to flee. This risk of flight is heightened considering that he has not yet turned in his passport.

B. The Court should issue a bench warrant for the Defendant's Arrest and Seal this Motion until the Defendant is arrested.

The defendant explicitly agreed to the following terms in her plea agreement.

The Government may move to change your client's conditions of release, including requesting that your client be detained pending sentencing, if your client engages in further criminal conduct prior to sentencing . . . Your client also agrees that any violation of your client's release conditions, any misconduct by your client, or any inability or failure on the part of your client to continue your client's cooperation with the Government, may result in the Government filing an ex parte motion with the Court requesting that a bench warrant be issued for your client's arrest and that your client be detained without bond while pending sentencing in your client's case. *ECF Doc. 9, ¶ 8.*

Plea Agreement, Section 8 (Conditions of Release) at p. 6.

Defendant's recent untruthful statements to the government regarding this October 21, 2024 fraud may be considered obstruction of justice in violation of 18 U.S.C. § 1512 or false statements made to the government in violation of 18 U.S.C. § 1001 causing the Court to issue an arrest warrant pursuant 18 U.S.C. § 3148. At an absolute minimum, this constitutes misconduct and an inability for him to continue his cooperation with the government in the current posture and provide a basis for the issuance of a bench warrant as contemplated by the plea agreement.

The government submits that under *Washington Post v. Robinson*, 935 F.2d 282, 289, n.10 (D.C. Cir. 1991), compelling reasons exist to seal this filing until law enforcement agents arrest the defendant. If the defendant is made aware of this filing prior to her arrest, he may attempt to flee the country or delete incriminating electronic evidence. Notwithstanding this sealing request, the government seeks permission to share documents with any agencies that can help effectuate the defendant's arrest.

CONCLUSION

WHEREFORE, the government respectfully requests that the Court issue an arrest warrant for defendant Veer Chetal and seal this motion, the proposed order, and the arrest warrant until law enforcement effectuates the arrest of the defendant.

Respectfully submitted,

EDWARD MARTIN JR.
United States Attorney
D.C. Bar No. 481866

By: /s/ Kevin Rosenberg
KEVIN ROSENBERG
OHIO BAR 0081448
Assistant United States Attorney
Fraud, Public Corruption, and Civil Rights Section
601 D Street, N.W. | Washington, D.C. 20530
Kevin.Rosenberg@usdoj.gov | 202-809-5351