UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**No. 24-CR- 494 (CKK)**
	:	
VEER CHETAL,	:	**UNDER SEAL**
	:	
Defendant.	:	

STATEMENT OF OFFENSE IN SUPPORT OF GUILTY PLEA

I. Summary of the Plea Agreement

As set forth in the attached plea agreement, Defendant Veer Chetal (hereinafter referred to as "Defendant" or "Chetal") agrees to accept responsibility and plead guilty to Counts One and Two of the Information, charging Defendant with (Count One) Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349 and (Count Two) Conspiracy to Launder Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h).

II. Elements of the Offenses

Count One, Conspiracy to Commit Wire Fraud

The essential elements of the offense of Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349, each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

(1) Two or more persons, in some way or manner, agreed to try to accomplish a common and unlawful plan to commit a fraud crime listed in Title 18 Chapter 63, as charged in the Indictment, that is, wire fraud; and

(2) The defendant knew the unlawful purpose of the plan and willfully joined in it.

The essential elements of the offense of Wire Fraud, in violation of Title 18, United States Code, Section 1343 are:

(1) That the defendant devised a scheme to defraud or to obtain money or property by materially false or fraudulent pretenses, representations or promises (or willfully participated in such a scheme with knowledge of its fraudulent nature);

(2) That the defendant acted with the intent to defraud; and

(3) That in advancing, furthering, or carrying out the scheme, the defendant transmitted any writing, signal, or sound by means of a wire, radio, or television communication in interstate commerce or caused the transmission of any writing, signal, or sound of some kind by means of a wire, radio, or television communication in interstate commerce.

Count Two, Conspiracy to Launder Monetary Instruments

The essential elements of the offense of Conspiracy to Launder Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h), each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

(1) Two or more people agreed to try to accomplish a common and unlawful plan to violate 18 U.S.C. §§ 1956 or 1957; and

(2) the Defendant knew about the plan's unlawful purpose and voluntarily joined in it.

The essential elements of the offense of Concealment Money Laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i), each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

(1) The defendant conducted or attempted to conduct;

(2) A financial transaction;

(3) Knowing that the property involved in such a financial transaction represented the proceeds of some form of unlawful activity;

(4) Which in fact involved the proceeds of specified unlawful activity;

(5) While acting with the knowledge that the transaction was designed in whole or part to disguise the nature, location, source, ownership, or control of the proceeds of the specified unlawful activity.

The essential elements of Expenditures Money Laundering, in violation of Title 18, United States Code, Section 1957(a), each of which the Government must prove beyond a reasonable doubt to sustain a conviction are:

(1) The defendant knowingly engaged, or attempted to engage in a monetary transaction;

(2) The monetary transaction was of a value greater than $10,000;

(3) The monetary transaction involved criminally derived property;

(4) Criminally derived property was derived from specified unlawful activity; and

(5) The defendant knew that the monetary transaction involved criminally derived property.

II. Statement of Facts

Pursuant to Federal Rule of Criminal Procedure 11, the United States and the Defendant, with the concurrence of Defendant's attorney, stipulate and agree that the following facts are true

and accurate. The following statement of facts does not purport to include all of the Defendant's illegal conduct. It also 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.

The Wire Fraud Conspiracy

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 assistant 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 them 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.

Respectfully Submitted

MATTHEW M. GRAVES
United States Attorney

By: _____
Kevin Rosenberg
Assistant United States Attorney

DEFENDANT'S ACKNOWLEDGMENT

I have read the Statement of Offense setting forth the facts related to my guilty plea. I have discussed this proffer fully with my attorney, Tezira Abe, Esq. I fully understand this proffer and I acknowledge its truthfulness, agree to it and accept it without reservation. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this proffer fully.

Date: 11/13/2024

Veer Chetal

ATTORNEY'S ACKNOWLEDGMENT

I have read each of the pages constituting the Government's proffer of evidence related to my client's guilty plea. I have reviewed the entire proffer with my client and have discussed it with him fully. I concur in my client's agreement with and acceptance of this proffer.

Date: 11/13/2024

Tezira Abe, Esq.
Counsel for Defendant