UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**No. 24-cr-417 (CKK)-1**
	:	
MALONE LAM,	:	
	:	
Defendant.	:	

STATEMENT OF OFFENSE IN SUPPORT OF GUILTY PLEA

I. Summary of the Plea Agreement

As set forth in the attached plea agreement, Defendant Malone Lam (hereinafter referred to as "the defendant") agrees to accept responsibility and plead guilty to Count One of the Second Superseding Indictment, charging him with Conspiracy to Participate in a Racketeer Influenced and Corrupt Organization ("RICO Conspiracy"), in violation of 18 U.S.C. § 1962(d).

II. Elements of the Offenses

Count One, RICO Conspiracy

The essential elements of the offense of RICO Conspiracy, in violation of Title 18, United States Code, Section 1962(d), each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

1. That the defendant knowingly agreed to conduct or participate, directly or indirectly, in the conduct of the affairs of the charged enterprise through a pattern of racketeering activity.
2. That an enterprise would be established as alleged in the indictment.
3. That the enterprise would be engaged in, or its activities would affect, interstate or foreign commerce.
4. That the defendant would be employed by, or associated with, the enterprise.

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 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, target identifiers, callers, money launderers, and residential burglars targeting hardware virtual currency wallets. The defendant played multiple roles within 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 as well as 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.

Wire Fraud

The defendant met co-conspirators and fellow members of the SE Enterprise Jeandiel Serrano ("Serrano") and Veer Chetal ("Chetal") playing the game Minecraft online while the defendant was living in Singapore. The defendant traveled to the United States from Singapore in or around October 2023 to live with Serrano, Connor Flansburg ("Flansburg") and others in Texas. From in or around October 2023 and continuing through at least September 2024, the defendant, Serrano, Chetal, Flansburg, and several others ("the conspirators") agreed to participate in a conspiracy designed to steal virtual currency from unwitting victims. The conspirators furthered the goals of the conspiracy by serving in various roles and in different combinations throughout the life of the conspiracy, but all with the same goal of unlawfully taking 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 purposes of the SE Enterprise.

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 criminals impersonate employees from trusted companies, send spoofed emails and websites ("panels") to victims, or employ related techniques designed to convince a victim to disclose valuable personal information that can be exploited for profit.

The defendant's role was to obtain breached cryptocurrency related databases containing lists of high net-worth subjects who would be targeted by the conspirators for social engineering schemes. The defendant analyzed the stolen data of the potential targets. The defendant also furthered the scheme by causing "account access attempt" push notifications to be sent to potential victims in order to make them believe there had been unauthorized attempts to access their online accounts. After co-conspirators convinced victims to provide personal account information, the defendant accessed the victims' accounts and searched for valuable information including cryptocurrency accounts, passwords, and seed phrases.

Additional conspirators / members of the SE Enterprise were involved in obtaining stolen databases, organizing the data, and then targeting victims. These conspirators included, but were not limited to, Flansburg, and others the defendant only knows through their online aliases such as "41" or "Qwervy," Chen ("~_~" or "Squiggly"), Danish or Danny Zulfiwar ("Meech"), Ibrahim Mustafa ("Krust") and Nicholas Dellecave ("Nic" or "Soulja").

Serrano and Chetal participated in the enterprise, 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, Yahoo!, or major cryptocurrency exchanges such as Coinbase or Gemini. Serrano and Chetal served in this role, in furtherance of the conspiracy, on numerous occasions. Serrano and Chetal would convince the victims of their legitimacy and then

cause the victims to disclose account access codes, which the defendant and others would use to access victim accounts and scour the accounts for virtual currency seed phrases, wallet addresses, and additional information relating to their financial currency holdings.

The conspirators, in various combinations, then either transferred victim cryptocurrency assets themselves, or caused the victims to transfer their virtual currency into wallet addresses controlled by the conspirators, under the belief that the funds were being transferred to secure wallets with their cryptocurrency exchange. The conspirators then used virtual currency exchanges, instant exchanges, and professional money launderers to conceal and disguise the origin and ownership of the stolen virtual currency.

A New Zealand-based conspirator and member of the SE Enterprise, Aakash Anand, whom the defendant knew through the online aliases "Dark" and "Light," also assisted in the laundering of stolen assets through cryptocurrency exchanges. Additional conspirators assisted in converting stolen virtual currency into fiat cash and luxury items such as watches, vehicles, and rental homes, including, but not limited to, Austin Fine ("Fine"), Hamza Doost ("Doost"), Joel Cortez ("Cortez"), Evan Tangeman ("Tangeman"), and Kunal Mehta ("Mehta" or "Neil")

Another conspirator, Marlon Ferro ("Ferro"), created an account with RedotPay to assist in spending stolen funds. RedotPay is a company that provides crypto payment cards, allowing customers to load cryptocurrency onto physical or digital cards and then use the card for purchases like a traditional credit or debit card. The card can be loaded onto a cellular telephone. Ferro created the account with fake identification documents because Redotpay does not support US-based registration. Ferro shared access to the card with the defendant and others so that they could load stolen cryptocurrency onto the account and use the digital card for purchases.

Victim K.W.

In furtherance of the conspiracy, the defendant and others targeted Victim K.W. for a social engineering cryptocurrency theft. In or around June/ July of 2024, the defendant and Chetal were able to access K.W.'s iCloud account through social engineering and determined that he held a significant amount of cryptocurrency on his cold storage wallet. Unable to access the wallet through the internet, the defendant and Chetal agreed to send Ferro to break into K.W.'s home in New Mexico. In or around July 2024, Ferro traveled to New Mexico and surveilled K.W.'s home while the defendant simultaneously monitored K.W.'s location through K.W.'s iCloud account. On July 8, 2024, Ferro broke into K.W.'s home and stole various electronic devices to access K.W.'s cold storage cryptocurrency wallets. Members of the SE Enterprise were ultimately unable to access Victim K.W.'s cryptocurrency following the home break-in.

Victim M.C.

In furtherance of the SE Enterprise, the defendant and others targeted Victim M.C. while M.C. was located in California. In or around June 23, ~~2023~~ 2024 CKK 9/8/26, members of the conspiracy contacted M.C. and claimed to be from Google, assisting M.C. with an unauthorized intruder accessing his email account. Through their social engineering scheme, members of the conspiracy were able to access M.C.'s private files and steal approximately $800,000 in virtual currency from M.C. The defendant participated in this theft with Squiggly and another conspirator he knew as "Gerred."

Victim S.P.

In furtherance of the conspiracy, the defendant and others targeted Victim S.P. while S.P. was located in Washington State. On July 23, 2024, members of the conspiracy, including the

defendant and Dellecave, executed a social engineering scheme on Victim S.P. They convinced Victim S.P. that they worked for Google and convinced Victim S.P. to download an application on his telephone for his security. Members of the conspiracy then used this application to access Victim S.P.'s private files and credentials and used this information to steal approximately $14,000,000 in virtual currency. Following this theft, the defendant used Neil to change a portion of the stolen cryptocurrency into fiat currency for a fee. Neil hand delivered a duffle bag containing $500,000 in US dollars to the defendant in Los Angeles in exchange for a portion of the stolen cryptocurrency.

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, the defendant 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 the defendant were communicating through Discord and Telegram during this interaction and strategizing about ways to gain access to R.W.'s Google account, including his Google OneDrive.

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

The defendant used the Discord display name "Anne Hathaway," and the Telegram display name "$ $ $" and "Ms. Jackson."

The defendant was able to access R.W.'s Google account and searched victim R.W.'s emails and Google OneDrive files to locate his virtual currency holdings once they gained access to his Google OneDrive accounts. The defendant discovered files in R.W.'s Google OneDrive accounts indicating that R.W. held a significant amount of virtual currency with the Gemini virtual currency exchange and custodial bank ("Gemini"). Chetal ended the phone call with R.W. after this discovery and Chetal and the defendant 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 with additional calls to R.W. Chetal and the defendant continued using the same screen names and Serrano began using the Discord display name "VersaceGod," and the Telegram display name "!" and "@SkidStar." Chen ("Squiggly) and Zulfiqar ("Meech") were also monitoring the access to R.W.'s Google account and the communications among the conspirators.

Chetal was in Connecticut during this series of calls. Serrano and the defendant were in Los Angeles at separate locations. Ferro was present with the defendant during the calls and observed the scheme unfolding on the defendant's computer. Meech was in Dubai at the time of these calls.

At one point Serrano called R.W. and claimed 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 the defendant over Telegram and Discord, convinced R.W. to provide the private keys to a portion of his virtual currency holdings. Chen

(Squiggly) used this information to access R.W.'s virtual currency assets and transfer an initial tranche of R.W.'s virtual currency assets to defendant, which were eventually laundered and divided evenly among the five conspirators.

Serrano, with the support and advice of the defendant and Chetal, then convinced R.W. to download a remote desktop connection program ("AnyDesk") that allowed the conspirators to view a mirrored image of R.W.'s desktop computer as he navigated through personal files and virtual currency private keys held in a cold storage wallet. The defendant and his other conspirators used this access for Chen to transfer an additional tranche of R.W.'s assets to defendant and into the control of the conspirators.

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

Money Laundering

From in or around October 2023 and continuing through at least September 2024, the conspirators (including the defendant, Serrano, Chetal, Meech, Squiggly, 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 into XMR Monero, using peel chains, pass through wallets, instant exchanges, and cryptocurrency exchange platforms that do not require 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, the defendant transferred R.W.'s assets into wallet addresses that were not readily attributable to the victim or conspirators, including in amounts over $10,000 per transaction. The defendant and his conspirators eventually divided the proceeds from R.W.'s virtual currency wallet into five equal parts (each worth more than $49 million), among the defendants, Serrano, Chetal, Meech, and Squiggly. Meech and Squiggly had previously assisted the conspirators in other social engineering schemes, including assistance in obtaining stolen cryptocurrency related databases used by the defendant, Chetal, and Serrano to identify and target victims, including R.W.

The defendant laundered his funds – including the funds from the theft/fraud on R.W. as well as other victims of the Wire Fraud Conspiracy – through multiple virtual currency exchanges that did not require extensive, or any, KYC information. Members of the conspiracy also laundered their 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 victim R.W.

Between at least October 2023 through September 2024, the defendant used his portion of the laundered virtual currency from the theft/fraud on R.W. as well as other victims to make

several purchases in excess of $10,000. The items included watches, designer clothes, private jet travel, rental homes in Los Angeles and Miami, nightclub services, and multiple luxury automobiles. On various occasions between at least January 2024 and September 2024, the defendant used Los Angeles-based money launderers Fine, Neil, and Cortez to turn his stolen virtual currency into fiat currency and luxury goods. Fine, Neil, and Cortez were aware that the virtual currency represented proceeds of a specified unlawful activity and continued to assist the defendant and others with this service. Fine, Neil, and Cortez typically charged a 10% fee for the cash conversions and luxury goods purchases.

The defendant used Doost, a San Jose based money launderer, to convert stolen cryptocurrency into fiat cash. Doost also assisted in obtaining private jet travel, Miami mansion rentals, and night club services.

During the course of the conspiracy, the defendant frequented various Los Angeles nightclubs operated by the h.Wood group. h.Wood did not accept payment in cryptocurrency. As a workaround, the defendant used an individual he knew as "Buster" and Will Markquart ("Markquart") to pay his nightly bills, sometimes in excess of $500,000 per evening. Buster used his credit card to pay the invoices. Buster and Markquart then accepted the defendant's stolen cryptocurrency and charged him an additional 10 - 20% fee for using their credit cards because Buster and Markquart needed to convert the cryptocurrency into fiat currency to pay their credit card bills. The crypto-to-cash conversions were often facilitated through Fine who charged his own fee.

Markquart also sold the defendant and the conspirators hundreds of Adderall pills and accepted well over $10,000 in cryptocurrency in exchange for the Adderall pills.

The defendant acquired dozens of luxury automobiles with stolen cryptocurrency. He primarily acquired these through two dealerships, the Exotic Car Factory and TBFTW. The defendant worked with Neil to broker automobile purchases with Sean DeSilva ("DeSilva") at the Exotic Car Factory. The defendant also worked with Zach Ersoff ("Ersoff") at TBFTW in Los Angeles and Miami to acquire at least 31 luxury automobiles, to include the following, all of which were purchased with stolen cryptocurrency:

- 2017 Rolls-Royce Dawn, VIN SCA666D58HU107052
- 2024 Porsche 911 Turbo, VIN WP0CD2A95RS257974
- 2024 The Lamborghini Revuelto, VIN ZHWUC1ZM9RLA00502
- 2024 The Lamborghini Urus, VIN ZPBUC3ZL8RLA28270
- 2020 The Lamborghini Aventador, VIN ZHWUN6ZD4LLA09485
- 2023 Rolls Royce Ghost, VIN SCATD6C01PU218443
- 2022 Ferrari, VIN ZFF99SLA5N0286515
- 2024 Ferrari Purosangue, VIN ZSG06VTA9R0308458
- G Mercedez Benz, VIN WDB4632761X308913 (invalid vin)
- 2021 The Lamborghini Urus, VIN ZPBUA1ZL9MLA15711
- 2020 The Lamborghini Aventador, VIN ZHWUM6ZD4LLA09411
- 2023 Mercedez-Benz Metris, VIN W1XV0CEY9P4259188
- 2024 Rolls-Royce Phantom, VIN SCATT6C09RU222911
- 2023 The Lamborghini Urus, VIN ZPBUC3ZL2PLA21277
- 2022 Mercedez-Benz G-Class, VIN W1NYC8AJ4NX448250
- 2021 The Lamborghini Urus, VIN ZPBUA1ZL8MLA14985
- 2024 Porsche 911, VIN WPOAD2A97RS252394
- 2023 Mercedez-Benz G-Class, VIN W1NYC7HJ7PX468026
- 2024 BMW M3, VIN WBS43AYO6RFS40948
- 2023 BMW M4, VIN WBS63AZ08PCM06345
- 2023 Ferrari 296 GTB, VIN ZFF99SLA5P0296996
- 2023 McLaren GT, VIN SBM22GCA8PW002500
- 2022 Mercedez-Benz Metris, VIN W1YVOCEY5N3976394
- 2024 Porsche 911, VIN WP0AD2A9ORS253399
- 2014 Pagani Huayra, VIN ZA9H11UAXESF76028
- 2023 Mercedes-Benz S-Class, VIN W1K6X7GBXPA191975
- 2024 Porsche 911, VIN WPOAF2A99RS272656
- 2024 BMW X6, VIN 5UX33EXOXR9U94401

Ersoff communicated with the defendant through Telegram and Signal, two encrypted

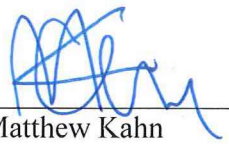
messaging platforms. Ersoff accepted millions of dollars in cryptocurrency from the defendant in exchange for these automobiles. Ersoff also helped the defendant disguise the true ownership of the automobiles by creating a Montana LLC, Crypto Administration LLC, and registering the automobiles in the name of the shell company. The defendant told Ersoff on multiple occasions that the defendant obtained the virtual currency he used to purchase the luxury automobiles from fraud. Ersoff was aware that the virtual currency represented proceeds of a specified unlawful activity and continued to assist the defendant and others with obtaining luxury automobiles.

As a member of the SE Enterprise, the defendant agreed that members of the SE Enterprise would commit at least two racketeering acts as defined by Title 18, United States Code, Section 1961. The defendant agrees that, based on his involvement and knowledge of the SE Enterprise, it was reasonably foreseeable to him that at least $250,000,000 would be stolen through wire fraud in furtherance of the conspiracy.

The defendant, together with his co-conspirators, personally obtained $245,093,239 in digital assets from different victims of their fraud. The defendant further admits that some of the proceeds the SE Enterprise obtained described above have been dissipated and cannot be located upon the exercise of due diligence; have been transferred or sold to, or deposited with, a third party; and/or have been placed beyond the jurisdiction of the Court. Finally, the defendant also agrees that the items listed in the Consent Preliminary Order of Forfeiture are property that he obtained directly or indirectly as a result of the SE Enterprise's racketeering activity in violation of 18 U.S.C. § 1962.

Respectfully Submitted

JEANINE FERRIS PIRRO
United States Attorney

By: 

Matthew Kahn
Deputy Chief
Fraud, Public Corruption, & Civil Rights

Christopher R. Howland
David Liss
Assistant United States Attorneys
Fraud, Public Corruption, & Civil Rights

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, John Pierce, 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: 8th September 2026

Malone Lam

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: 9/8/26

John Pierce, Esq.
Attorney for Malone Lam