

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on January 10, 2025

| | | |
|--|---|-----------------------------------|
| UNITED STATES OF AMERICA | : | CRIMINAL NO. 24-CR-417 (CKK) |
| | : | |
| v. | : | (UNDER SEAL) |
| | : | |
| MALONE LAM, also known as "King | : | |
| Greavys," "7," "\$\$\$," "Kg," and "Anne | : | GRAND JURY ORIGINAL |
| Hathaway," | : | |
| | : | |
| MARLON FERRO, also known as | : | VIOLATIONS: |
| "Marlo," and "GothFerrari," | : | |
| | : | COUNT 1: |
| | : | 18 U.S.C. § 1962(d) |
| HAMZA DOOST, also known as | : | (RICO Conspiracy) |
| "Scyllia," and "ç," | : | |
| | : | |
| CONOR FLANSBURG, also known as | : | COUNT 2: |
| "O O," "Green Room," and "@d0uu0b," | : | 18 U.S.C. § 1349 |
| | : | (Conspiracy to Commit Wire Fraud) |
| | : | |
| KUNAL MEHTA, also known as "Papa," | : | COUNT 3: |
| "The Accountant," "Shrek," and "Neil," | : | 18 U.S.C. § 1956(h) |
| | : | (Conspiracy to Launder Monetary |
| ETHAN YARALLY, also known as | : | Instruments) |
| "Rand," and "15%," | : | |
| | : | |
| CODY DEMIRTAS, also known as | : | COUNT 4: |
| "K O," and "Kody," | : | 18 U.S.C. § 1512(c) |
| | : | (Obstruction of Justice) |
| | : | |
| AAKAASH ANAND, also known as | : | FORFEITURE: |
| "Light," and "Dark," | : | 18 U.S.C. § 1963, |
| | : | 18 U.S.C. § 981(a)(1)(C), |
| EVAN TANGEMAN, also known as "E," | : | 18 U.S.C. § 982(a)(1), and |
| "Tate," and "Evan Exchanger," | : | 28 U.S.C. § 2461(c) |
| | : | |
| JOEL CORTES, also known as "J," | : | |
| | : | |
| FNU LNU-1, also known as "~_~" | : | |
| "Squiggly," and "CHEN," | : | |
| | : | |
| FNU LNU-2, also known as "DANNY," | : | |
| and "Meech," and | : | |
| | : | |
| TUCKER DESMOND, | : | |
| | : | |
| Defendants. | : | |

SUPERSEDING INDICTMENT

The Grand Jury charges that:

GENERAL ALLEGATIONS
The Enterprise

At all times relevant to this indictment:

1. The defendants, **MALONE LAM** (“**LAM**”), also known as “King Greavys,” “\$\$\$,” “7,” “Kg,” and “Anne Hathaway,” **MARLON FERRO** (“**FERRO**”), also known as “Marlo,” and “GothFerrari,” **HAMZA DOOST** (“**DOOST**”), also known as “Scyllia,” and “¢,” **CONOR FLANSBURG** (“**FLANSBURG**”), also known as “O O,” “Green Room,” and “@d0uu0b,” **KUNAL MEHTA** (“**MEHTA**”), also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,” **ETHAN YARALLY** (“**YARALLY**”), also known as “Rand,” and “15%,” **CODY DEMIRTAS** (“**DEMIRTAS**”), also known as “K O,” and “Kody,” **AAKAASH ANAND** (“**ANAND**”), also known as “Light,” and “Dark,” **EVAN TANGEMAN** (“**TANGEMAN**”), also known as “E,” “Tate,” and “Evan | Exchanger,” **JOEL CORTES** (“**CORTES**”), also known as “J,” **FNU LNU-1** (“**CHEN**”), also known as “Chen,” “~_~” and “Squiggly,” **FNU LNU-2** (“**DANNY**”), also known as “Danny,” and “Meech,” and others known and unknown, were members and associates of the Social Engineering Enterprise (the “SE Enterprise”). The SE Enterprise, including its leaders, members, and associates, constituted an “enterprise,” as that term is defined in Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact, although not a legal entity, which engaged in, and the activities of which affected, interstate and foreign commerce. The SE Enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives

of the enterprise.

DEFINITIONS

2. **Bitcoin:** Bitcoin (or “BTC”) is a type of virtual currency. Unlike traditional, government-controlled currencies (*i.e.*, fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin’s software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

3. **Virtual Currency:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (*i.e.*, they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (*e.g.*, online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether (“Eth”), are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a

blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

4. **Monero:** XMR or Monero is a virtual currency which uses a blockchain with privacy-enhancing technology to obfuscate transactions to achieve anonymity and fungibility. It is widely regarded as a privacy coin and believed untraceable by law enforcement.

5. **USDT:** USDT or Tether is a stablecoin cryptocurrency designed to maintain a stable value, pegged to the US dollar (approximately \$1).

6. **Virtual Currency Address:** A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

7. **Virtual Currency Exchange:** A virtual currency exchange (“VCE”), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers’ virtual currency addresses in hosted wallets. VCEs can be centralized (*i.e.*, an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (*i.e.*, a peer-to-peer marketplace where transactions occur directly between parties). Coinbase, Gemini, Thorswap, Tradeogre, and eXch are examples of VCEs.

8. **Virtual Currency Wallet:** A virtual currency wallet (*e.g.*, a hardware wallet, software wallet, or paper wallet) stores a user’s public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

9. **Hardware Wallet:** A hardware wallet is a physical, removable device that stores

a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PINs and passphrases and can be backed up or regenerated with a recovery phrase. Trezor and Ledger are some examples of the types of hardware wallets on the market.

10. **Hosted Wallet:** A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, *e.g.*, a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

11. **Software Wallet:** A software wallet is an internet-connected virtual currency wallet in the form of a software application on a desktop or mobile device or a web-based platform accessible through a web browser. The software will store and usually encrypt the user's public and private keys.

12. **Unhosted Wallet:** An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (*e.g.*, a virtual currency exchange) to facilitate a transaction involving the wallet.

13. **Private Key:** A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password,

which is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

14. **Seed Phrase**: A seed phrase, also known as a recovery phrase or mnemonic phrase, is a list of 12 to 24 randomly generated words that acts as a backup for your cryptocurrency wallet, allowing you to regain access to your funds if you lose access to your wallet or device. A social engineer in possession of a victim's seed phrase can reconstitute the virtual currency wallet and take possession of a victim's virtual currency.

15. **Social Engineering**: Social Engineering is a type of fraud scheme wherein individuals call a potential victim and "socially engineer," or trick them into providing passwords, pins, and other personal information that the callers use to gain unauthorized access to the victim's private accounts, including cryptocurrency accounts, Google drive files, iCloud accounts, and other valuable personal files.

16. **Caller**: A "Caller" or "se'er" is the name commonly used for the individuals involved in social engineering schemes who place calls to potential victims and falsely portray themselves as security technicians from well known email providers such as Google and Yahoo! or representatives from VCEs such as Gemini or Coinbase. Their goal is to give the victim enough confidence in their character that the victim will provide access to their online accounts.

17. **IRL Break-in**: An IRL Break-in or In Real Life Break-in refers to the act of sending a SE Enterprise member to a victim's residence for the purpose of breaking in and stealing the victim's hardware wallet.

18. **Targs**: Targs or Targets are terms used by the SE Enterprise to describe potential victims of social engineering schemes.

19. **DBs**: DBs or databases, are stolen virtual currency related databases shared among

the SE Enterprise and used to develop targets for callers.

20. **Crypto-to-Cash**: Crypto-to-cash exchangers refers to unlicensed money transmitters who receive stolen virtual currency and provide customers with physical fiat US currency. Due to its illegality, the fee charged for this service is exorbitant compared to fees charged by VCEs that perform know your customer (“KYC”) anti-money laundering protocols.

21. **Crypto-to-Wire**: Crypto-to-wire exchangers refers to unlicensed money transmitters who receive stolen virtual currency and bring the currency into the US banking system for the customer through laundering techniques in the form of bank wire transfers. Due to its illegality, the fee charged for this service is exorbitant compared to fees charged by VCEs that perform know your customer (“KYC”) anti-money laundering protocols.

22. **Straw Signer**: A straw signer or straw owner is a person who agrees to hold title to another’s automobile or home, for a fee, in order to disguise and conceal the true owner of the items when the true owner wants to conceal their identity from law enforcement.

BACKGROUND OF THE ENTERPRISE

23. 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.

24. The SE enterprise largely grew from friendships developed among its members and associates through online gaming platforms. The friendships evolved into agreements to commit cyber-enabled criminal offenses throughout the United States and abroad.

25. Members and associates of the SE enterprise served different roles and held different responsibilities. The roles included database hackers, organizers, target identifiers, callers, money launderers, and residential burglars targeting hardware virtual currency wallets.

26. Database hackers were responsible for hacking websites and servers to obtain cryptocurrency related databases or purchasing databases on the dark web. Organizers and target identifiers were responsible for organizing and collating information across various databases to determine the most valuable targets. Callers were responsible for cold-calling victims and convincing them their accounts were the subject of a cyber-attack and the callers were attempting to help secure their accounts against cyber-attacks. Money launderers were responsible for receiving stolen virtual currency and turning the virtual currency into fiat US currency in the form of bulk cash or wire transfer, or providing luxury services such as exotic car purchases, private jet rentals, international vacations, or shipping bulk cash across the United States.

PURPOSES OF THE ENTERPRISE

27. The purposes of the SE Enterprise included, but were not limited to the following:
- a. Stealing virtual currency from victims throughout the United States through fraudulent pretenses;
 - b. Disguising, concealing, and obfuscating the source and ownership of the stolen funds through the use of virtual currency laundering techniques; and
 - c. Converting laundered virtual currency into fiat currency and wire transfers for use at nightclubs, for the purchase of exotic cars, jewelry, luxury handbags, clothing, private jet rentals, along with other items, property, goods, and services, and rental mansions in Los Angeles, the Hamptons, Miami, and elsewhere.

DEFENDANTS' ROLES IN THE ENTERPRISE

28. **CHEN, DANNY, FLANSBURG**, and others served as database hackers on behalf of the SE Enterprise.

29. **LAM, FLANSBURG**, and others served as organizers for the SE Enterprise and

identified targets for callers.

30. **COCONSPIRATOR-1, COCONSPIRATOR-2, YARALLY, DEMIRTAS, ANAND, FLANSBURG,** and others served as callers for the SE Enterprise.

31. **DOOST, MEHTA, CORTES, MONEY EXCHANGER-1, FERRO, TANGEMAN, ANAND,** and others served as money launderers for the SE Enterprise.

32. **FERRO** served as a residential burglar or IRL (in real life) Break-in member of the SE Enterprise.

MEANS AND METHODS OF THE ENTERPRISE

33. The means and methods by which the defendants, and other members and associates of the SE Enterprise, conducted and participated in the conduct of the affairs of the SE Enterprise included, but was not limited to, the following:

- a. Members and associates of the SE Enterprise obtained and collected stolen databases primarily relating to virtual currency assets in order to identify potential victims who held vast amounts of virtual currency across different VCEs.
- b. Members and associates of the SE Enterprise caused unauthorized account access push notifications to be sent to potential victims in the leadup to a social engineering attack in order for the fraudulent “support” call to seem more legitimate.
- c. Members and associates of the SE Enterprise made fraudulent “support” calls in which they called victims and identified themselves as employees from major VCEs or email account providers and tricked victims into providing email account passwords, cloud storage account passwords, seed phrases, private keys,

and VCE logins.

d. Members and associates of the SE Enterprise used victim passwords for email accounts, Google Drive accounts, iCloud accounts, and virtual currency accounts to access victim files and private information and search for seed phrases and private keys.

e. Members and associates of the SE Enterprises used stolen seed phrases and private keys to access victims' virtual currency and transfer the virtual currency into their possession.

f. Members and associates of the SE Enterprise planned and executed home break-ins to recover physical hardware wallets when SE Enterprise members identified substantial virtual currency holdings on cold-storage physical devices.

g. Members and associates of the SE Enterprise stole victim virtual currency and laundered it through off-shore VCEs and converting it to XMR to conceal the ownership and location of the stolen virtual currency.

h. Members and associates of the SE Enterprise sent laundered virtual currency to other members of the SE Enterprise who accepted stolen virtual currency and exchanged the currency for bags of fiat currency and wire transfers.

i. 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.

j. Members and associates of the SE Enterprise used various “nightclub promoters” to pay for their nightclub services in exchange for stolen cryptocurrency and up to a 20% fee for the unlicensed conversions.

k. Members and associates of the SE Enterprise placed their homes and automobiles in the names of straw owners, signers, or shell companies to disguise and conceal their ownership and conceal their identity from law enforcement.

l. Members and associates of the SE Enterprise shipped fiat currency across the country to other members, sometimes hidden in clothing or stuffed animals.

m. Members and associates of the SE Enterprise communicated on encrypted messaging applications such as Telegram and Signal and changed their username on a regular basis to maintain their security.

n. Members and associates of the SE Enterprise obtained firearms for their protection from rival cybercrime enterprises and stored the firearms at their group residences.

o. Members and associates of the SE Enterprise obtained information from off-duty law enforcement officers regarding investigations of the SE Enterprise.

COUNT ONE
(18 U.S.C. § 1962(d))
(RICO Conspiracy)

34. Paragraphs 1 through 33 are re-alleged herein.

OBJECT OF THE CONSPIRACY

35. Beginning on a date unknown to the Grand Jury, but from at least on or about October 2023, and continuing through at least in or around March 2025, in the District of Columbia and elsewhere, the defendants,

MALONE LAM,
 also known as “King Greavys,” “\$\$\$,” “7,” “Kg,” and “Anne Hathaway,”
MARLON FERRO,
 also known as “Marlo,” and “GothFerrari,”
HAMZA DOOST,
 also known as “Scyllia,” and “¢,”
CONOR FLANSBURG,
 Also known as “O O,” “Green Room,” and “@d0uu0b,”
KUNAL MEHTA,
 also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,”
ETHAN YARALLY,
 also known as “Rand,” and “15%,”
CODY DEMIRTAS,
 also known as “K O,” and “Kody,”
AAKAASH ANAND,
 also known as “Light” and “Dark,”
EVAN TANGEMAN,
 also known as “E,” “Tate,” “Evan |Exchanger”
JOEL CORTES,
 also known as “J,”
FNU LNU,
 Also known as “~ ~” “Squiggly,” and “CHEN,” and
FNU LNU,
 Also known as “Danny,” and “Meech,”

and others known and unknown to the grand jury, being persons employed by and associated with the SE Enterprise, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, did knowingly, and intentionally combine, conspire, confederate, and agree to violate Title 18, United States Code, Section 1962(c), that is to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity, as defined in Title 18, United States Code, Sections 1961(1) and (5), consisting of multiple acts indictable under Title 18, United States Code:

- a. Section 1028 (relating to fraud and related activity in connection with identification documents);
- b. Section 1029 (relating to fraud and related activity in connection with access devices);
- c. Section 1343 (relating to wire fraud);
- d. Section 1512 (relating to tampering with a witness, victim, or an informant);
- e. Section 1956 (relating to laundering of monetary instruments);
- f. Section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity);
- g. Section 1960 (relating to illegal money transmitters); and
- h. Section 2314 (relating to interstate transportation of stolen property).

36. It was a further part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

Overt Acts

37. In furtherance of the conspiracy, and to achieve the objectives thereof, each defendant and their co-conspirators committed and caused to be committed the following overt acts, among others, in the District of Columbia, and elsewhere:

- a. In or around October 2023, **LAM**, **FLANSBURG**, and **COCONSPIRATOR-2** moved in together in Texas and began discussing cyberfraud schemes, to include database thefts, social engineering schemes, and

email account intrusions.

- b. In or around October 2023, **LAM**, **FLANSBURG**, and **COCONSPIRATOR-2** began committing social engineering attacks in various combinations.
- c. While in Texas from October 2023 through December 2023, **LAM**, **FLANSBURG**, and **COCONSPIRATOR-2** funded their lifestyles and paid rent with profits from their cybercrime activities, which included social engineering schemes.
- d. While in Texas from October 2023 through December 2023, **COCONSPIRATOR-2** and others used **MONEY EXCHANGER-1** to receive stolen cryptocurrency and exchange it into fiat cash in the form of Cashapp deposits. **MONEY EXCHANGER-1** charged a 10% fee for using his unlicensed money service business.
- e. In or around December 2024, **LAM**, **FLANSBURG**, and **COCONSPIRATOR-2** moved to Los Angeles, California and enlisted the assistance of **MONEY EXCHANGER-1** and **TANGEMAN** to help them obtain short and long-term rental homes paid for with stolen virtual currency in fraudulent names.
- f. In December 2023, **LAM**, **FLANSBURG**, and **COCONSPIRATOR-2** used **MONEY EXCHANGER-1** to illegally convert stolen cryptocurrency into fiat cash in amounts ranging from \$10,000 - \$50,000.
- g. Between in or around December 2023 and September 2024, **TANGEMAN** assisted various coconspirators, including **LAM**, **FLANSBURG**,

COCONSPIRATOR-2, and others in obtaining luxury rental homes in Los Angeles using stolen virtual currency.

- h. Between in or around December 2023 and September 2024, **TANGEMAN** and **MONEY EXCHANGER-1** received stolen cryptocurrency from **LAM**, **COCONSPIRATOR-2**, **FLANSBURG**, and others and used Money Exchanger-2 and **MEHTA** to convert the stolen cryptocurrency into U.S. dollars.
- i. In or around January 2024 and continuing through at least September 2024, on behalf of members of the SE Enterprise, **TANGEMAN** placed various rental homes in false names, listed fictitious tenants, and paid deposits in large cash sums, in excess of hundreds of thousands of dollars, in order to disguise and conceal the true ownership of the rental homes on behalf of the SE Enterprise.
- j. From in or around December 2023 and continuing through around September 2024, **TANGEMAN** charged a fee for his anonymizing services and his crypto-to-cash services.
- k. Between December 2023 and April 2024, **MONEY EXCHANGER-1** assisted **LAM**, **FLANSBURG**, **COCONSPIRATOR-2**, and others with exchanging stolen cryptocurrency for US dollars, in exchange for a 10% fee.
- l. In or around the beginning of 2024, **TANGEMAN** assisted **LAM**, **FLANSBURG**, **COCONSPIRATOR-2**, and others to obtain a rental home located on Clear Valley Drive, Encino, California, a six-bedroom, 11-bathroom, 11,000 square foot home and paid for with stolen cryptocurrency.
- m. In or around the beginning of 2024, **LAM**, **FLANSBURG**,

COCONSPIRATOR-2, and others set up computer terminals at the Clear Valley Drive rental home, in Encino, California for the purposes of executing cybercrime schemes including social engineering attacks.

- n. Beginning in or around January 2024 and continuing through at least September 2024, **LAM**, **COCONSPIRATOR-1**, **COCONSPIRATOR-2**, and **FLANSBURG** began targeting victim Gmail accounts for social engineering attacks.
- o. In or around February 2024, **DOOST** joined the SE Enterprise and offered additional crypto-to-cash money laundering services for a fee. Soon thereafter, **DOOST** and **MONEY EXCHANGER-1** began working together to service the SE Enterprise's need for currency exchanges.
- p. In or around early 2024, **MEHTA** was introduced to the SE Enterprise and offered additional crypto-to-cash money laundering services for a fee, as well as crypto-to-wire money laundering services.
- q. From in or around early 2024 and continuing through at least September 15, 2024, **MEHTA** laundered millions of dollars' worth of virtual currency through a sophisticated virtual currency money laundering ring and received "clean" currency through wire transfers and cash deliveries.
- r. From in or around early 2024 and continuing through at least September 2024, **MEHTA** assisted **FLANSBURG**, **FERRO**, **COCONSPIRATOR-2** and other members of the SE Enterprise in obtaining firearms for their protection against rival cybercrime groups.
- s. In or around early 2024, **CORTES** began assisting various money launderers

with retrieving and delivering bags of fiat cash to members of the SE Enterprise.

- t. In or around early 2024, and continuing until at least September 2024, **CORTES** assisted members of the SE Enterprise in changing stolen virtual currency into fiat currency and shipping the currency across the United States, hidden in squishmallow® stuffed animals, each containing approximately \$25,000 apiece.
- u. In or around early 2024, **MEHTA** began assisting the SE Enterprise in laundering stolen virtual currency so that it could be used to purchase exotic cars from Exotic Car Dealership-1. **MEHTA** also agreed to find straw signers for the automobiles or hold the automobiles in his name in order to disguise and conceal the true ownership of the automobiles.
- v. In or around March 2024, **TANGEMAN** assisted **FLANSBURG**, **COCONSPIRATOR-2**, and others in obtaining another rental home located on Hesby Street, a 7000 square foot, 6 bed, 8 bath single-family home in Encino, California (the “Hesby House”). **FLANSBURG**, **LAM**, **COCONSPIRATOR-2** and others paid for this home through stolen cryptocurrency which **TANGEMAN** received and changed into fiat currency for cash payments to the property owners.
- w. In or around March 2024 **TANGEMAN** arranged the lease documents for **FLANSBURG**, **COCONSPIRATOR-2**, and others at the Hesby House and used fake names and fake identity documents to execute the lease for the purpose of concealing their identities.
- x. In or around March 13, 2024, **LAM**, **COCONSPIRATOR-1**, and another

coconspirator executed a social engineering fraud scheme against Victim-1 and stole over \$600,000 in virtual currency from Victim-1.

- y. In or around May 2024, **DOOST** informed **LAM** that **DOOST** could obtain various private jet rentals for **LAM** and his associates and **DOOST** could arrange air travel for **LAM** and others where they would not need to provide any identification documents to travel on private jets.
- z. On or about May 15, 2024, **COCONSPIRATOR-1**, **YARALLY**, and another coconspirator executed a social engineering fraud scheme against Victim-2 and stole approximately \$2,900,000 in virtual currency from Victim-2.
- aa. In or around June 2024, **CORTES**, **MEHTA**, **MONEY EXCHANGER-1**, the owner of Exotic Car Dealership-1, and others rented a private jet and flew from Los Angeles to the Hamptons for a weekend party thrown by **COCONSPIRATOR-1**, paid for with stolen virtual currency.
- bb. In or around June 2024, **DOOST** and **MEHTA** assisted **COCONSPIRATOR-1** in arranging for a rental mansion in the Hamptons and a fleet of exotic car rentals. **MEHTA** and **DOOST** used **MEHTA**'s crypto-to-wire transfer exchange service to assist **COCONSPIRATOR-1** in paying for these items with stolen virtual currency.
- cc. On or about June 21, 2024, **LAM** informed **COCONSPIRATOR-1** that he was "trying to make \$5m[illion] for us atm [at the moment]."
- dd. On or around June 23, 2024, **LAM**, **CHEN**, and another coconspirator, executed a social engineering fraud scheme against Victim-3 and stole approximately \$870,000 worth of virtual currency.

- ee. In or around July 2024, COCONSPIRATOR-1, MONEY EXCHANGER-1, YARALLY, DEMIRTAS, ANAND, DOOST, and others traveled to Miami as a group. While in Miami, DOOST and MONEY EXCHANGER-1 assisted the group in exchanging hundreds of thousands of dollars in stolen virtual currency for fiat cash through DOOST's network in Miami.
- ff. In or around July 2024, LAM, DANNY, and COCONSPIRATOR-1 executed a social engineering fraud scheme against Victim-4.
- gg. In or around July 2024, LAM accessed Victim-4's Apple iCloud account to monitor Victim-4's location in real time.
- hh. In or around July 2024, FERRO flew to New Mexico to break into Victim 4's home for the purpose of stealing Victim-4's virtual currency hardware wallet.
- ii. In or around July 2024, while in New Mexico, FERRO setup a telephone (which had a video camera) across from Victim-4's home to livestream the home during the break-in so that other enterprise members could alert FERRO if the victim returned during the break-in.
- jj. On July 8, 2024, FERRO, in coordination with LAM and others, broke into Victim Victim-4's home in search of hardware virtual currency devices.
- kk. On or about July 17, 2024, TANGEMAN directed LAM to send \$194,000 in stolen virtual currency to TANGEMAN's "cash guy" so that TANGEMAN could retrieve fiat cash and use it to pay a security deposit at one of LAM's Los Angeles rental homes.
- ll. On or about July 19, 2024, LAM asked TANGEMAN to find him \$300,000

in fiat cash in exchange for stolen virtual currency. **TANGEMAN** responded “Yeah let me see if I can get that much cash tonight might have to be in the morning.”

TANGEMAN later responded to **LAM** that if **LAM** had USDT or ETH, he could obtain the full \$300,000 immediately, but if not, **TANGEMAN** could only obtain \$100,000 that day and \$200,000 the following date.

mm. On or about July 21, 2024, **LAM**, **CHEN**, and another co-conspirator executed a social engineering fraud scheme against Victim-5 and stole approximately \$1,740,000 in virtual currency from Victim-5.

nn. On or about July 24, 2024, **LAM**, **CHEN**, and another coconspirator executed a social engineering fraud scheme against Victim-6 and stole approximately \$14,000,000 in virtual currency from Victim-6.

oo. On a date unknown, but shortly after July 24, 2024, **LAM** sent **MEHTA** over \$500,000 in virtual currency stolen during the Victim-6 theft and **MEHTA** in turn personally delivered a duffel bag containing approximately \$500,000 in US currency to **LAM** and his associates.

pp. In or around August and September of 2024, **FERRO** created a digital payment card on the site ReDotPay using fake documents from **FERRO**’s “KYC guy,” and agreed with **COCONSPIRATOR-2**, **LAM**, and others that he would receive their stolen virtual currency, load it onto the virtual payment card, and allow members of the SE Enterprise to use the card in person at retail stores.

qq. On August 3, 2024, **LAM** asked **CORTES** to get him \$100,000 in fiat cash and **CORTES** responded “bet, bet...I’m getting the cash right now.”

rr. On or about August 19, 2024, **LAM**, **COCONSPIRATOR-1**,

COCONSPIRATOR-2, **CHEN**, and **DANNY** executed a social engineering fraud scheme against Victim-7 while Victim-7 was at his home in Washington, D.C. In doing so, they stole approximately \$245,093,239.00 in virtual currency from Victim-7.

ss. On or about August 19, 2024, **LAM**, COCONSPIRATOR-1, COCONSPIRATOR-2, **CHEN**, and **DANNY** convinced Victim-7 to download a remote desktop connection program onto his computer in Washington, D.C. **LAM**, COCONSPIRATOR-1, COCONSPIRATOR-2, **CHEN**, and **DANNY** then accessed Victim-7's computer during their social engineering fraud scheme.

tt. Following the Victim-7 theft, **LAM**, COCONSPIRATOR-1, COCONSPIRATOR-2, **DANNY**, and **CHEN**, used sophisticated virtual currency laundering techniques to "clean" the stolen currency.

uu. Following the Victim-7 theft, **ANAND** assisted COCONSPIRATOR-1 with laundering the stolen virtual currency on various virtual currency exchanges that are known for not requiring any identity documents for financial transactions.

vv. Between August 19, 2024 and September 10, 2024, **LAM** and his associates spent over \$4,000,000 in stolen virtual currency at Los Angeles nightclubs.

ww. On or about August 23, 2024, **TANGEMAN** assisted **LAM** in securing an additional Los Angeles rental home in exchange for stolen virtual currency. **TANGEMAN** directed **LAM** to send \$337,050 in USDT to **TANGEMAN**'s "exchanger" which included a 7% commission for unlicensed crypto-to-cash services.

- xx. On or about August 25 and 26, 2024, **LAM** used **TANGEMAN** and **MONEY EXCHANGER-1** to launder approximately \$3,000,000 in cryptocurrency in order for **LAM** to obtain a new Los Angeles rental home.
- yy. Between August 25 and 28, 2024, **TANGEMAN** and **MONEY EXCHANGER-1** received \$3,000,000 in stolen virtual currency from **LAM** and worked with **MEHTA** to exchange the virtual currency for fiat cash.
- zz. On August 26, 2024, **LAM** requested to tour the home before paying the full \$3,000,000 but **TANGEMAN** told **LAM** this was not a good idea because the realtor had placed the home under the name of a 55-year old living at the residence with his family, all in an effort to conceal **LAM**'s payment and ownership of the home.
- aaa. On or about August 23, 2024, **MEHTA** agreed to ship **COCONSPIRATOR-1** \$50,000 in fiat cash in exchange for stolen virtual currency and a fee for his services.
- bbb. On or about August 26, 2024, **CORTES** informed **COCONSPIRATOR-1** that he was shipping his fiat cash in the mail. Soon thereafter, **COCONSPIRATOR-1** received squishmallow® stuffed animals filled with \$50,000 in fiat currency.
- ccc. On or about August 26, 2024, **ANAND** asked **COCONSPIRATOR-1** to search four email addresses through the SE Enterprise's virtual currency databases to see if any of the targets were valuable.
- ddd. On or about August 29 and 30, 2024, **ANAND** discussed new social engineering callers who he was recruiting to work directly for them including **DEMIRTAS**. **ANAND** told **COCONSPIRATOR-1** that the callers know what

they're doing because they also work with **FLANSBURG**. **COCONSPIRATOR-1** replied, "if it's for Gmails, I'd have to get Malone [**LAM** because] he signs in[to accounts] and stuff."

eee. On September 3, 2024, **LAM** asked **DOOST** in a sms message "who do you get cash off," and **DOOST** replied "Message me on signal."

fff. In or around September 2024, **LAM** requested that **CORTES** and **DOOST** assist him in exchanging \$400,000 in stolen virtual currency.

ggg. In or around September 2024, **ANAND** traveled to the United States from New Zealand to visit **COCONSPIRATOR-1** and retrieve luxury clothing purchased with stolen virtual currency.

hhh. On or about September 6, 2024, **DOOST** and **COCONSPIRATOR-1** discussed the Victim-7 theft and **DOOST** told **COCONSPIRATOR-1** that "I genuinely think Malone [**LAM**] has a huge chance of getting caught compared to you[,] keep your profile the way that you do." **COCONSPIRATOR-1** responded, "Yeah he's gonna simmer down hopefully." **DOOST** replied and told **COCONSPIRATOR-1** "Bro delete your Tele[gram] chats and setup your new phone."

iii. On or about September 7, 2024, **FERRO** and **COCONSPIRATOR-1** discussed the Victim-7 theft and **COCONSPIRATOR-2**'s involvement. **FERRO** stated "Bro [**COCONSPIRATOR-2**] is so fucking stupid. It fucking hurts...What's so hard about waiting to clean 50 million dollars. Why is he so impatient knowing he has trusted people cleaning it. Like what was the point of Malone [**LAM**]

sweating his ass off cleaning [COCONSPIRATOR-2's] shit little by little...Bro he just fumbled a 250m lick just by being stupid."

jjj. On or about September 7, 2024, **YARALLY** sent COCONSPIRATOR-1 a message stating "just got into a rich Indian bitch...but she signed us out" followed by a screenshot of a an excel spreadsheet from the victim's computer showing all of the victim's virtual currency holdings. **YARALLY** continued on saying that she is "stupid" on the phone and asked how he could bypass a google security feature. **YARALLY** then told COCONSPIRATOR-1 "[w]ere back in...Kody [DEMIRTAS] se'd [social engineered] her for her password...[password redacted]...this is her password btw." **YARALLY** finally sent COCONSPIRATOR-1 a screenshot of his computer screen showing **DEMIRTAS** accessing a victim's Gmail account during a social engineering scheme in real-time.

kkk. On or about September 8, 2024, **LAM** shared approximately 40 organized and stolen cryptocurrency-related databases with **FLANSBURG**, and other co-conspirators for the purpose of using the databases to target victims and committing wire fraud.

lll. On or about September 8, 2024, COCONSPIRATOR-1 and **YARALLY** discussed a profit-sharing agreement for current social engineering victims. COCONSPIRATOR-1 stated "30/30/30/10 is how we're going to do shit. 30 [M]alone [LAM] 30 me 30 you 10 se'r" referring to the social engineer caller. **YARALLY** responded, "I'll take 25 and give ma[il] se'er 15....cus mail se'ers r Ruben and Cody [DEMIRTAS] too."

mmm. On or about September 8, 2024, **LAM** and **FLANSBURG** discussed an

arrangement in a group chat wherein **LAM** agreed to send all of his databases to **FLANSBURG** if **FLANSBURG** agreed that he would send **LAM** and **COCONSPIRATOR-1** 20% of any successful social engineering targets where the theft was over \$10,000,000. **FLANSBURG** agreed and stated “[w]e hackin, all day every day.”

nnn. On September 8, 2024, **COCONSPIRATOR-2** asked **CORTES** if he knew who was sending cash to his Hesby House address. **CORTES** informed him that **DOOST** was having cash delivered there for **LAM** and explained that this was a \$400,000 crypto-to-cash exchange.

ooo. On September 8, 2024, **MEHTA** messaged **COCONSPIRATOR-2** to explain the manner in which he disguises and conceals the true owners of the exotic car purchases and told **COCONSPIRATOR-2** that “[o]ur goal is to cover our tracks in a way that if anything comes back ever we are covered and have no stress.”

ppp. On or about September 9, 2024, **MEHTA** and **CORTES** spoke with **COCONSPIRATOR-2** about paying for his security detail. **MEHTA** asked **COCONSPIRATOR-2** to send the XMR to **CORTES** who would then convert the virtual currency into USDT and send it to **MEHTA** for payment.

qqq. On or about September 9, 2024, **LAM** bragged to **FLANSBURG**, **COCONSPIRATOR-1**, and another coconspirator about successfully stealing virtual currency from Victim-5, Victim-6, and Victim-7. **LAM** stated in part “bro [Victim-6] a dumb fuck too,” “[Victim-5] dumb fuck.” **FLANSBURG** responded “[a]ll these kids that been doing it forever suck.” **LAM** replied “[Victim-7]

shouldn't even of took long. [COCONSPIRATOR-2] and I just played it smart and calm. And extra cautious. But other than that think abt it all big ass licks." **LAM** went on to state "they just stupid, just gotta find the right one." **FLANSBURG** agreed and asked "[h]ow are we all so much better than everyone" and "[h]ow have we surpassed all the kids that have been around for 8 years, in a few months."

rrr. On September 9, 2024 **YARALLY** requested an email target database from **COCONSPIRATOR-1** and **COCONSPIRATOR-1** sent him a document containing emails and identifiers for over 1,000 targets, titled "good ass Yahoos to run." **COCONSPIRATOR-1** then asked **YARALLY** which callers were working for him at the moment and **YARALLY** responded "kody," referring to **DEMIRTAS**.

sss. On or about September 9, 2024, **FLANSBURG** and **LAM** discussed past victims and **FLANSBURG** told **LAM** "100%. We hit the guy for 2160 eth 12 btc. Dumb as shit. Gave us his Gmail pw [password] and input seed within 5 mins basically." **LAM** replied "bro, Conor [**FLANSBURG**], we, not me, we have the most Dbs [databases] in this world, in this community bro." **FLANSBURG** replied "oh ye, it's not even close."

ttt. In or around September 2024, an off-duty law enforcement officer informed **MONEY EXCHANGER-1** that federal law enforcement was investigating members of the SE Enterprise. **MONEY EXCHANGER-1** relayed this information to **COCONSPIRATOR-2** and recommended that **COCONSPIRATOR-2** stay in the Maldives instead of returning to the United States.

uuu. In or around September 2024, **COCONSPIRATOR-2** sent **MEHTA** approximately \$500,000 in stolen virtual currency for **MEHTA** to exchange for fiat

currency and wire transfers that **MEHTA** agreed to launder to COCONSPIRATOR-2's mother in the form of cash, wire transfers, and an automobile.

vvv. In September 2024, COCONSPIRATOR-2 paid **DOOST** in stolen virtual currency to arrange travel for himself and two others to travel to the Maldives. COCONSPIRATOR-2 paid **DOOST** during the trip and during one payment of \$32,200 on September 12, 2024, **DOOST** stated "got KYC on the funds, I just wanna make sure it was clean right?" COCONSPIRATOR-2 replied "Yes the funds were clean brotha."

www. In August and September of 2024, **LAM** purchased over 30 automobiles from Exotic Car Dealership-2 using stolen virtual currency and created a fictitious holding company named Crypto Administration LLC to hold title to the cars, all with the goal of disguising and concealing the true ownership of the automobiles. The automobiles included Ferraris, Lamborghinis, Mercedes G Wagons, Rolls Royce, a McClaren, and a Pagani among several others.

xxx. On or about September 12, 2024, **DOOST** informed COCONSPIRATOR-2 about being "beamed" or robbed of \$400,000 during a crypto-to-cash exchange on behalf of **LAM**. COCONSPIRATOR-2 asked "[t]hat's terrible bro. So you sent them 400k for free?" **DOOST** responded "[y]ou're making me sound dumb but cash people every cash person always requires it first and he's fronted money for me before so it was just a show for me – but a few racks is fine bro. Never been burned in my life and highest I did with these people are like 500k on tx [transaction]."

yyy. On or about September 14, 2024, COCONSPIRATOR-2 and **FLANSBURG** discussed the new cars **LAM** was purchasing with stolen virtual currency. COCONSPIRATOR-2 then asked if the cars were under **MEHTA**'s name. **FLANSBURG** responded "All my cars are chilling. I got all mine under him [**MEHTA**]. I got no clue how he [**LAM**] has his set up."

zzz. On or about September 15, 2024, **MEHTA** informed COCONSPIRATOR-2 that **MEHTA** could assist in exchanging virtual currency to fiat cash and sending it to COCONSPIRATOR-2's mother. **MEHTA** stated "[c]ash exchange we can do here brother. . . [s]ame like always my g. 10%. Since day 1... So \$550k when you ready... If you want I can even wire half to her account and half cash. I'm sure it's going to be easier for her to spend if it's in her account than \$500k cash."

aaaa. On or about September 15, 2024, **MEHTA** informed COCONSPIRATOR-2 that **MEHTA** could funnel \$250,000 in stolen virtual currency to COCONSPIRATOR-2's mother in the form of wire transfers. **MEHTA** informed COCONSPIRATOR-2 that **MEHTA** would insulate them from federal investigators by sending COCONSPIRATOR-2's mother \$30,000 at a time and creating "some kind of work for her and show[ing] that I paid her for that and at the end of the year once she files her taxes I can help her get refund as well." **MEHTA** went on to explain that if COCONSPIRATOR-2 wanted "some cash to give with the [mom's new] car then I think we should do like 250k and rest I can do wires slowly."

bbbb. On or about September 16, 2024, **FLANSBURG** told COCONSPIRATOR-2 "look what I smacked." COCONSPIRATOR-2 responded, "I heard a crazy seed

[phrase].” **FLANSBURG** replied “ended up being 5.8” million. **COCONSPIRATOR-2** replied “Bonkers. . . that must’ve been [a] new car that day for u. New Newport house too. 1 yr lease.” **FLANSBURG** then sent **COCONSPIRATOR-2** a photo of a luxury watch he purchased with the stolen virtual currency.

cccc. On or about September 16, 2024, **FLANSBURG** and **COCONSPIRATOR-2** discussed all of **LAM**’s recent spending, including purchasing over 30 cars, multiple homes in Miami and Los Angeles, a two-million-dollar watch, along with the multiple private jets **LAM** rented to fly friends from Los Angeles to Miami.

dddd. On or about September 16, 2024, **COCONSPIRATOR-2** told **FLANSBURG** that he had spent \$200,000 on his Maldives trip, including \$125,000 on travel and two payments of \$25,000 and \$40,000 to **DOOST** to perform the unlicensed virtual currency exchange to fiat currency with **COCONSPIRATOR-2**’s stolen virtual currency.

eeee. On September 17, 2024, **DOOST** told **COCONSPIRATOR-2** to delete his phone applications before returning from the Maldives because customs could go through his phone and this happened to another associate recently where they discovered \$500,000.

ffff. On or about September 17, 2024, **DOOST** told **COCONSPIRATOR-2** that he could procure iPhones for **COCONSPIRATOR-2** for a fee where the phones would be placed under a fake identity and **COCONSPIRATOR-2** would be notified if the phone numbers were ever the subject of a law enforcement subpoena.

gggg. Throughout September 2024, **LAM**, **DOOST**, and others worked to together to exchange stolen virtual currency to fiat currency that could be used for Nightclub services and bulk cash conversions in Miami, Florida.

hhhh. On or about September 18, 2024, **LAM** obtained information about the investigation of the SE Enterprise originating from an off-duty law enforcement officer, specifically, that law enforcement were on their way to arrest **LAM**.

iiii. On or about September 18, 2024, **LAM** walked to the rear of his Miami rental home and dropped his mobile telephone off the boat dock and into Biscayne Bay to destroy incriminating evidence, after being advised that law enforcement were on their way to arrest **LAM**.

jjjj. Following **LAM**'s arrest on or about September 18, 2024, **TANGEMAN** and others recovered digital devices belonging to **FERRO** and **LAM** in Los Angeles and destroyed the devices for the purpose of obstructing the law enforcement investigation.

kkkk. Following **LAM**'s arrest on September 18, 2024 and continuing through October 2024, **YARALLY** regularly spoke with **LAM** from inside of a Miami jail and relayed messages from various SE Enterprise members to **LAM** and relayed messages from **LAM** to other SE Enterprise members.

llll. On or about September 27, 2024, **YARALLY** executed a three-way phone call for **LAM** to COCONSPIRATOR-1. **LAM** told COCONSPIRATOR-1 "[y]ou know I'm taking this for you right? . . .you know I'm in here and it's not my mistake." **LAM** then said "you're the only people....ya'll have the money. You know how it works, the lawyers care about the money . . . I'm talking about pay the

lawyers.” **LAM** then explained that he had already given his money “back to the feds.” **YARALLY** then informed him not to worry about the lawyers because “I’m getting it right now...We have Hamza [**DOOST**] helping everyone out here too.” **LAM** concluded by telling the group, “we always talked about what it would be like if I were to go down, but never thought it would be this crazy.”

mmmm. On or about September 28, 2024, **YARALLY** informed **LAM** that **FLANSBURG** was selling a car to pay for lawyers. **LAM** responded “Why is he selling [their] M3s...Tell Conor [**FLANSBURG**] not to give back those other cars. It’s fucking 200k, I wipe that shit with my ass. I don’t want that. I want my people to have their shit. . . if he wants me out, tell him to get his money to the lawyers, not by selling cars.”

nnnn. On or about October 2, 2024, **YARALLY** informed **LAM** that law enforcement did not recover all of **LAM**’s cars and **YARALLY** told **LAM** that he didn’t want to identify their location over the recorded line.

oooo. From in or around November 2024 and continuing through at least March 2024, **FERRO** held onto a portion of **LAM**’s funds while incarcerated and used **LAM**’s funds to arrange for the purchase of multiple Hermes Birkin purses for **LAM**’s girlfriend with the assistance of **TANGEMAN** and other coconspirators.

pppp. From in or around November 2024 and continuing through at least March 2024, **FERRO** used the remainder of **LAM**’s stolen virtual currency, and other stolen funds sent to **FERRO** by members of the SE Enterprise, including **YARALLY**, to fund **LAM**’s defense team.

qqqq. In or around November and December 2024, **YARALLY** sent **FERRO** approximately \$55,000 in fraud proceeds to support **LAM**.

rrrr. From in or around November 2024 and continuing through March 2025, **FERRO** regularly passed messages on **LAM**'s behalf inside of jail to members of the SE Enterprise, to include **FLANSBURG**, **YARALLY**, **TANGEMAN**, **DOOST**, and others.

ssss. In or around January 2025, **YARALLY** and **DEMIRTAS** regularly shared their computer screen views with **COCONSPIRATOR-1** so that **COCONSPIRATOR-1** could watch them performing social engineering attacks.

tttt. In or around January and February 2025, **DOOST**, **YARALLY**, **DEMIRTAS**, and others communicated with **COCONSPIRATOR-1** in jail and spoke in code regarding social engineering schemes. The group used coded language such as "playing tournaments," "winning games," or "being really good players."

(In violation of Title 18, United States Code, Section 1962(d))

COUNT TWO
(18 U.S.C. § 1349)
(Conspiracy to Commit Wire Fraud)

38. Paragraphs 1 through 33 and 37 are re-alleged herein.

39. Beginning on a date unknown, but no later than in or around October 2023 and continuing until at least in or around March 2025, within the District of Columbia and elsewhere, the defendants,

MALONE LAM,
also known as "King Greavys," "\$\$\$," "7," "Kg," and "Anne Hathaway,"
MARLON FERRO,

also known as “Marlo,” and “GothFerrari,”
CONOR FLANSBURG,
Also known as “O O,” “Green Room,” and “@d0uu0b,”
ETHAN YARALLY,
also known as “Rand,” and “15%,”
CODY DEMIRTAS,
also known as “K O,” and “Kody,”
AAKAASH ANAND,
also known as “Light” and “Dark,”
FNU LNU-1,
Also known as “~ ~” “Squiggly,” and “CHEN,” and
FNU LNU-1,
Also known as “Danny,” and “Meech,”

did knowingly and willfully conspire, confederate, and agree, with each other and with other persons, to commit wire fraud by devising, intending to devise, and engaging in a scheme to defraud and to obtain money, property, and cryptocurrency from Victim-1, Victim-2, Victim-3, Victim-4, Victim-5, Victim-6, Victim-7, and others by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing and attempting to execute the scheme to defraud, did knowingly cause to be transmitted by means of wire communications in interstate commerce, writings, signs, signals, pictures, and sounds.

(In violation of Title 18, United States Code, Section 1349)

COUNT THREE
(18 U.S.C. § 1956(h))
(Conspiracy to Launder Monetary Instruments)

40. Paragraphs 1 through 33 and 37 are re-alleged herein.

41. From in or around at least October 2023 and continuing until at least in or around March 2025, within the District of Columbia and elsewhere, the defendants,

MALONE LAM,
also known as “King Greavys,” “\$\$\$,” “7,” “Kg,” and “Anne Hathaway,”
MARLON FERRO,

also known as “Marlo,” and “GothFerrari,”
HAMZA DOOST,
also known as “Scyllia,” and “¢,”
KUNAL MEHTA,
also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,”
AAKAASH ANAND,
also known as “Light,” and “Dark,”
EVAN TANGEMAN,
also known as “E,” “Tate,” “Evan |Exchanger,”
JOEL CORTES,
also known as “J,”
TUCKER DESMOND,
FNU LNU-1,
Also known as “~_~” “Squiggly,” and “CHEN,” and
FNU LNU-2,
Also known as “Danny,” and “Meech,”

did knowingly combine, conspire, and agree with each other and with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1957, to wit: (1) the movement of \$245,093,239.00 in stolen cryptocurrency, along with other stolen cryptocurrency, which involved the proceeds of a specified unlawful activity and the numerous financial transactions designed in whole or in part to conceal or disguise the nature, location, source, ownership, and control of the proceeds of the conspiracy to commit wire fraud charged in Count Two of the Indictment, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) and (2) knowingly engage and attempt to engage in monetary transactions in criminally derived property of a value greater than \$10,000 that was derived from specific unlawful activity, that is the conspiracy to commit wire fraud charged in Count Two of the Indictment, in violation of Title 18, United States Code, Section 1957.

MANNER AND MEANS

42. The manner and means used to accomplish the objectives of the conspiracy included, among others,

- a. **LAM, CHEN, DANNY**, and others transferring portions of the \$245,093,239.00 stolen from Victim-7 between multiple cryptocurrency addresses and through cryptocurrency mixers and exchanges for the purpose of concealing ownership and disguising the origin and current location of the stolen funds.
- b. Co-conspirators including **LAM, CHEN, DANNY**, and others using peel chains and pass-through wallet addresses for the purpose of concealing ownership and disguising the location of the stolen funds.
- c. **FERRO** creating a digital payment card to assist members of the conspiracy in engaging in financial transactions in excess of \$10,000 in criminally derived property;
- d. **TANGEMAN** exchanging stolen virtual currency for fiat currency to help **LAM** and others obtain rental homes paid with cash deposits and placing fictitious names on the lease documents to conceal the ownership and control of the funds and homes.
- e. **DOOST, CORTES, MEHTA**, and others changing criminally derived virtual currency into fiat cash, in excess of \$10,000 at a time, knowing that the transactions were also designed to conceal the source, ownership, and control of the currency.

- f. **CORTES** shipping squishmallow® stuffed animals containing fiat cash across the country, knowing the funds represented criminally derived proceeds.
- g. **DESMOND** delivering fiat cash for members of the conspiracy and assisting **LAM** in procuring luxury handbags valued at over \$10,000 and flying the handbags to **LAM**'s girlfriend in Miami while **LAM** was incarcerated.
- h. **ANAND** assisting with swapping and laundering stolen virtual currency on various VCE platforms.
- i. Co-conspirators including **LAM** and others attempting to obfuscate their identities by using virtual private network ("VPN") services to attempt to mask their true IP addresses.
- j. **LAM, META, DOOST, ANAND, CORTES, DESMOND, FERRO, CHEN, DANNY, and TANGEMAN**, engaging in financial transactions in excess of \$10,000, knowing that the transactions represented criminal proceeds generated through specified unlawful activity.

(In violation of Title 18, United States Code, Sections 1956(h), 1956(a)(1)(B)(i) and 1957)

COUNT FOUR
(18 U.S.C. §§ 1512(c)(1) and (2))
(Obstruction of Justice)

43. Paragraphs 1 through 33 and 37 are re-alleged herein.

44. On or about a date unknown, but shortly after September 18, 2024, the defendant,

TUCKER DESMOND,

did corruptly alter, destroy, mutilate, and conceal a record, document, or other object, that is,

recovering and destroying computers and cell phones belonging to **LAM** and **FERRO** following **LAM's** arrest, with the intent to impair their integrity and availability for use in an official proceeding in the District of Columbia, that is *United States v. Malone Lam, et. Al.*, 24-cr-417, in violation of Title 18, United States Code, Section 1512(c)(1).

(In violation of Title 18, United States Code, Sections 1512(c)(1) and (2))

FORFEITURE

45. The allegations contained in COUNT ONE of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant Title 18, United States Code, Sections 1963. Pursuant to Title 18, United States Code, Section 1963, upon conviction of an offense in violation of Title 18, United States Code, Section 1962, the defendant(s) shall forfeit to the United States of America:

- a. any interest acquired or maintained in violation of section 1962;
- b. any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over, any enterprise which the defendant[s] established, operated, controlled, conducted, or participated in the conduct of, in violation of section 1962; and
- c. any property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity or unlawful debt collection in violation of 1962.

46. The allegations contained in COUNTS TWO and FOUR of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section

2461(c). Upon conviction of the offense in violation of Title 18, United States Code, Section 1349 set forth in COUNT TWO or Title 18, United States Code, Section 1512 set forth in COUNT FOUR of this Indictment, the defendant(s), shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

47. The allegations contained in COUNT THREE of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(1). Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of an offense in violation of Title 18, United States Code, Section 1956, the defendant(s), shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property.

SPECIFIC PROPERTY SUBJECT TO FORFEITURE

48. The property to be forfeited includes, but is not limited to, the following:

Vehicles

- V1) 2017 Rolls-Royce Dawn, VIN SCA666D58HU107052
- V2) 2024 Porsche 911 Turbo, VIN WP0CD2A95RS257974
- V3) 2024 Lamborghini Revuelto, VIN ZHWUC1ZM9RLA00502
- V4) 2024 Lamborghini Urus, VIN ZPBUC3ZL8RLA28270
- V5) 2020 Lamborghini Aventador, VIN ZHWUN6ZD4LLA09485
- V6) 2023 Rolls Royce Ghost, VIN SCATD6C01PU218443
- V7) 2022 Ferrari, VIN ZFF99SLA5N0286515
- V8) 2024 Ferrari Purosangue, VIN ZSG06VTA9R0308458
- V9) G Mercedes Benz, VIN WDB4632761X308913
- V10) 2021 Lamborghini Urus, VIN ZPBUA1ZL9MLA15711
- V11) 2020 Lamborghini Aventador, VIN ZHWUM6ZD4LLA09411
- V12) 2023 Mercedes-Benz Metris, VIN W1XV0CEY9P4259188
- V13) 2024 Rolls-Royce Phantom, VIN SCATT6C09RU222911
- V14) 2023 Lamborghini Urus, VIN ZPBUC3ZL2PLA21277
- V15) 2022 Mercedes-Benz G-Class, VIN W1NYC8AJ4NX448250
- V16) 2021 Lamborghini Urus, VIN ZPBUA1ZL8MLA14985

V17) 2024 Porsche 911, VIN WPOAD2A97RS252394
 V18) 2023 Mercedes-Benz G-Class, VIN W1NYC7HJ7PX468026
 V19) 2024 BMW M3, VIN WBS43AYO6RFS40948
 V20) 2023 BMW M4, VIN WBS63AZ08PCM06345
 V21) 2023 Ferrari 296 GTB, VIN ZFF99SLA5P0296996
 V22) 2023 McLaren GT, VIN SBM22GCA8PW002500
 V23) 2022 Mercedes-Benz Metris, VIN W1YVOCEY5N3976394
 V24) 2024 Porsche 911, VIN WP0AD2A9ORS253399
 V25) 2014 Pagani Huayra, VIN ZA9H11UAXESF76028
 V26) 2023 Mercedes-Benz S-Class, VIN W1K6X7GBXPA191975
 V27) 2024 Porsche 911, VIN WPOAF2A99RS272656
 V28) 2024 BMW X6, VIN 5UX33EXOXR9U94401

Cash

C1) Cash in brown Louis Vuitton bag: \$169, 700
 C2) Cash in black Samsonite bag: \$44, 714

Miscellaneous

M1) Black Louis Vuitton sneakers with box
 M2) One Audemars Piguet white watch with shiny rocks
 M3) One yellow star shaped ring with white rocks
 M4) One yellow bracelet with white rocks
 M5) One yellow/silver chain necklace with white rocks
 M6) Yellow color teeth guard (grill)
 M7) Black jacket
 M8) Chrome hearts silver paper chain
 M9) Car keys BMW
 M10) Gold in color chain
 M11) Yellow champagne bottle with receipt
 M12) Two shirts
 M13) One pair of jeans
 M14) McLaren 600 key fob
 M15) iPad
 M16) MacBook, Serial No. M6N93WC75K, Model A2681
 M17) Louis Vuitton bag with receipt
 M18) Rolex watch
 M19) Christian Dior Jeans
 M20) Louis Vuitton leather pants
 M21) Amiri Silver Shoes
 M22) Dark/light blue jeans
 M23) Indigo Blouson

- M24) Louis Vuitton green shoes
- M25) Louis Vuitton ring
- M26) Clear stone silver colored ring
- M27) Clear stone ring
- M28) Blue Audemars Piguet watch
- M29) Silver with clear stone ring
- M30) Silver in color, Audemars Piguet watch
- M31) Silver ring with clear stones
- M32) Silver colored ring
- M33) Silver colored ring with clear stones
- M34) Silver and gold in color with clear stones watch
- M35) Patek Philippe watch, silver in color with clear stones
- M36) Red and black Louis Vuitton case
- M37) Silver colored Rolex watch
- M38) Black and silver colored Richard Mille watch
- M39) Grey colored Dior box
- M40) Louis Vuitton navy and white shirt
- M41) Two silver colored with clear stone pillows
- M42) Bracelet with hearts and clear stones, silver in color
- M43) Blue denim Louis Vuitton shoes
- M44) Black and red colored Christian Louboutin shoes
- M45) Light blue Louis Vuitton shoes
- M46) Purple colored Louis Vuitton shoes
- M47) Amiri shoes, white and red in color with stones
- M48) Dior shoes, red and pink in color
- M49) Grey colored Dior shoes
- M50) White Louis Vuitton backpack
- M51) White colored Audemars Piguet watch
- M52) Silver and black colored Richard Mille watch
- M53) Red and silver colored Richard Mille watch
- M54) White Richard Mille watch
- M55) Dior shoes, black and white in color
- M56) Grey and white colored Dior shoes
- M57) Dior shoes, blue denim in color
- M58) Black colored Dior shoes
- M59) Two pairs of Amiri shoes, blue and white in color with stones
- M60) Black Louis Vuitton shoes
- M61) Orange colored Louis Vuitton shoes
- M62) Louis Vuitton shoes, black and yellow in color
- M63) Denim white, blue, red Christian Louboutin shoes

M64) Louis Vuitton shoes, pink in color
M65) Black Louis Vuitton shoes with black stones
M66) Louis Vuitton pants camouflage
M67) White Chanel bag
M68) Brown Louis Vuitton bag
M69) Black and red Christian Louboutin bag
M70) Rolex watch, silver and gold in color with clear stones and red numerals
M71) Black and yellow colored Amiri Jacket
M72) Black and white Amiri Jacket
M73) Amiri black T-shirt
M74) Christian Dior black T-shirt
M75) Amiri black shirt
M76) Black and white Christian Dior hoodie
M77) White Louis Vuitton hoodie
M78) Black striped shirt, Louis Vuitton
M79) Black Louis Vuitton Jacket
M80) Black, white and red Louis Vuitton hoodie
M81) Black and red Louis Vuitton Jacket
M82) Blue and white Louis Vuitton button up shirt
M83) Black Louis Vuitton Jacket
M84) Black Dior Pants
M85) Black Dior Pants
M86) Navy Dior Pants
M87) Louis Vuitton grey pants
M88) Black Louis Vuitton Pants
M89) Blue Louis Vuitton button shirt
M90) Blue Amira sneakers
M91) Louis Vuitton receipts
M92) Black Alienware laptop & charger. ST: 8X0DL44, EX: 19410276388
M93) 3 of 6 Louis Vuitton Pillows
M94) Black Louis Vuitton Belt
M95) Silver colored Rolex watch
M96) Red Hermes bag
M97) Porsche key
M98) Lamborghini car key
M99) Silver colored bracelet

MONEY JUDGMENT

49. In the event of conviction, the United States may seek a money judgment.

SUBSTITUTE ASSETS

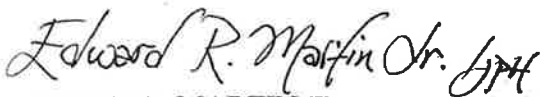
50. If any of the property described above, as a result of any act or omission of the defendant(s):

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 18, United States Code, Section 1963(m) and Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL

FOREPERSON



EDWARD MARTIN JR.
ATTORNEY FOR THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA