

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

Defendants.

**FORFEITURE: 18 U.S.C. § 924(d),
18 U.S.C. § 1963, and
28 U.S.C. § 2461(c)**

SECOND 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,” and “Kg,”

KUNAL MEHTA (“MEHTA”), also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,” **ETHAN YARALLY (“YARALLY”)**, also known as “Rand,” and “15%,” **AAKAASH ANAND (“ANAND”)**, also known as “Light,” and “Dark,” **EVAN TANGEMAN (“TANGEMAN”)**, also known as “E,” “Tate,” and “Evan | Exchanger,” and **FNU LNU-1 (“CHEN”)**, also known as “Chen,” “~ ~” and “Squiggly,” 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 May 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, COCONSPIRATOR-C.F.** and others served as database hackers on behalf of the SE Enterprise or otherwise acquired databases for the SE Enterprise.

29. **LAM, COCONSPIRATOR-C.F.**, and others served as organizers for the SE Enterprise and identified targets for callers.

30. **COCONSPIRATOR-1, COCONSPIRATOR-2, YARALLY, COCONSPIRATOR C.D., ANAND, COCONSPIRATOR C.F.**, and others served as callers

for the SE Enterprise.

31. **COCONSPIRATOR H.D., MEHTA, COCONSPIRATOR J.C., MONEY EXCHANGER-1, COCONSPIRATOR M.F., TANGEMAN, ANAND,** and others served as money launderers for the SE Enterprise.

32. **COCONSPIRATOR M.F.** 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 May 2025, in the District of Columbia

and elsewhere, the defendants,

MALONE LAM,
also known as “King Greavys,” “\$\$\$,” “7,” “Kg,”

KUNAL MEHTA,
also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,”
ETHAN YARALLY,
also known as “Rand,” and “15%,”
AAKAASH ANAND,
also known as “Light,” and “Dark,”
EVAN TANGEMAN,
also known as “E,” “Tate,” “Evan | Exchanger” and,
FNU LNU-1,
Also known as “~_~” “Squiggly,” and “CHEN,”

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**, COCONSPIRATOR C.F., 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**, COCONSPIRATOR C.F., and COCONSPIRATOR-2 began committing social engineering attacks in various combinations.
- c. While in Texas from October 2023 through December 2023, **LAM**,

COCONSPIRATOR C.F., 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**, COCONSPIRATOR C.F., 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**, COCONSPIRATOR C.F., 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**, COCONSPIRATOR C.F., 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, COCONSPIRATOR C.F., 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**, **COCONSPIRATOR C.F**, **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**, **COCONSPIRATOR C.F**, **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**, **COCONSPIRATOR C.F**, **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

COCONSPIRATOR C.F. began targeting victim Gmail accounts for social engineering attacks.

- o. In or around early 2024, and CHEN shared breached cryptocurrency related databases with LAM and others for use in social engineering fraud schemes.
- p. In or around February 2024, COCONSPIRATOR H.D. joined the SE Enterprise and offered additional crypto-to-cash money laundering services for a fee. Soon thereafter, COCONSPIRATOR H.D. and MONEY EXCHANGER-1 began working together to service the SE Enterprise's need for currency exchanges.
- q. 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.
- r. From in or around early 2024 and continuing through at least May 2025, 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.
- s. From in or around early 2024 and continuing through at least September 2024, MEHTA assisted COCONSPIRATOR M.F. and other members of the SE Enterprise in obtaining firearms for their protection against rival cybercrime groups.
- t. In or around early 2024, COCONSPIRATOR J.C. began assisting various money launderers with retrieving and delivering bags of fiat cash to members of the SE Enterprise.
- u. In or around early 2024, and continuing until at least September 2024,

COCONSPIRATOR J.C. 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.

v. From in or around early 2024 and continuing through at least May of 2025,

COCONSPIRATOR C.F. and others reached an agreement to split profits from social engineering schemes with one another based on their role in the theft, whether they found the victim's information, and who obtained the breached databases that contained the information.

w. 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 to disguise and conceal the true ownership of the automobiles.

x. In or around March 2024, **TANGEMAN** assisted COCONSPIRATOR C.F., 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"). COCONSPIRATOR C.F., **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.

y. In or around March 2024, **TANGEMAN** arranged the lease documents for

COCONSPIRATOR C.F., 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.

- z. 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.
- aa. In or around May 2024, COCONSPIRATOR H.D. informed **LAM** that COCONSPIRATOR H.D. could obtain various private jet rentals for **LAM** and his associates and COCONSPIRATOR H.D. could arrange air travel for **LAM** and others where they would not need to provide any identification documents to travel on private jets.
- bb. 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.
- cc. In or around June 2024, COCONSPIRATOR J.C., **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.
- dd. In or around June 2024, COCONSPIRATOR H.D. and **MEHTA** assisted COCONSPIRATOR-1 in arranging for a rental mansion in the Hamptons and a fleet of exotic car rentals. **MEHTA** and COCONSPIRATOR H.D. used **MEHTA**'s crypto-to-wire transfer exchange service to assist COCONSPIRATOR-1 in paying for these items with stolen virtual currency.

- ee. Throughout the summer months in 2024, and at times both before and after, laundered stolen cryptocurrency through COCONSPIRATOR H.D. to obtain fiat cash and to obtain private jet rentals, Miami rental mansions, and nightclub services.
- ff. On or about June 21, 2024, **LAM** informed COCONSPIRATOR-1 that he was “trying to make \$5m[illion] for us atm [at the moment].”
- gg. 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.
- hh. In or around July 2024, COCONSPIRATOR-1, MONEY EXCHANGER-1, **YARALLY**, COCONSPIRATOR C.D., **ANAND**, COCONSPIRATOR H.D., and others traveled to Miami as a group. While in Miami, COCONSPIRATOR H.D. and MONEY EXCHANGER-1 assisted the group in exchanging hundreds of thousands of dollars in stolen virtual currency for fiat cash through COCONSPIRATOR H.D.’S network in Miami.
- ii. In or around July 2024, **LAM**, and COCONSPIRATOR-1 executed a social engineering fraud scheme against Victim-4.
- jj. In or around July 2024, **LAM** accessed Victim-4’s Apple iCloud account to monitor Victim-4’s location in real time.
- kk. In or around July 2024, COCONSPIRATOR M.F. flew to New Mexico to break into Victim 4’s home for the purpose of stealing Victim-4’s virtual currency hardware wallet.

- ll. In or around July 2024, while in New Mexico, COCONSPIRATOR M.F. set up 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 COCONSPIRATOR M.F. if the victim returned during the break-in.
- mm. On July 8, 2024, COCONSPIRATOR M.F., in coordination with **LAM** and others, broke into Victim-4's home in search of hardware virtual currency devices.
- nn. 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.
- oo. 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.
- pp. 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.
- qq. 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.
- rr. 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.

ss. In or around August and September of 2024, COCONSPIRATOR M.F. created a digital payment card on the site ReDotPay using fake documents from COCONSPIRATOR M.F.'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.

tt. On August 3, 2024, **LAM** asked COCONSPIRATOR J.C. to get him \$100,000 in fiat cash and COCONSPIRATOR J.C. responded "bet, bet...I'm getting the cash right now."

uu. On or about August 19, 2024, **LAM**, COCONSPIRATOR-1, COCONSPIRATOR-2, **CHEN**, and 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.

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

- ww. Following the Victim-7 theft, **LAM**, **COCONSPIRATOR-1**, **COCONSPIRATOR-2**, and **CHEN**, used sophisticated virtual currency laundering techniques to “clean” the stolen currency.
- xx. 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.
- yy. 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.
- zz. 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.
- aaa. 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.
- bbb. 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.
- ccc. 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.

ddd. 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.

eee. On or about August 26, 2024, COCONSPIRATOR J.C. 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.

fff. 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.

ggg. On or about August 29 and 30, 2024, **ANAND** discussed new social engineering callers who he was recruiting to work directly for them including COCONSPIRATOR C.D. **ANAND** told COCONSPIRATOR-1 that the callers know what they are doing because they also work with COCONSPIRATOR C.F. COCONSPIRATOR-1 replied, "if it's for Gmails, I'd have to get Malone [**LAM** because] he signs in[to accounts] and stuff."

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

iii. On or about September 4, 2024, COCONSPIRATOR C.F., and others executed a social engineering scheme against Victim-8 and stole

approximately \$5,000,000 in virtual currency.

jjj. In or around September 4, 2024, COCONSPIRATOR C.F., and others, split the profits from the \$5,000,000 theft, with receiving approximately 25% of the profits.

kkk. In or around September 2024, LAM requested that COCONSPIRATOR J.C. and COCONSPIRATOR H.D. assist him in exchanging \$400,000 in stolen virtual currency.

lll. 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.

mmm. On or about September 6, 2024, COCONSPIRATOR H.D. and COCONSPIRATOR-1 discussed the Victim-7 theft and COCONSPIRATOR H.D. 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." COCONSPIRATOR H.D. replied and told COCONSPIRATOR-1 "Bro delete your Tele[gram] chats and setup your new phone."

nnn. On or about September 7, 2024, COCONSPIRATOR M.F. and COCONSPIRATOR-1 discussed the Victim-7 theft and COCONSPIRATOR-2's involvement. COCONSPIRATOR M.F. 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.”

ooo. 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 [COCONSPIRATOR C.D.] 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 COCONSPIRATOR C.D. accessing a victim’s Gmail account during a social engineering scheme in real-time.

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

qqq. 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 [COCONSPIRATOR C.D.] too.”

rrr. On or about September 8, 2024, **LAM**, and COCONSPIRATOR C.F. discussed an arrangement in a group chat wherein **LAM** agreed to send all his databases to and COCONSPIRATOR C.F. if COCONSPIRATOR C.F. and agreed that they would send **LAM** and COCONSPIRATOR-1 20% of any successful social engineering targets where the theft was over \$10,000,000. COCONSPIRATOR C.F. agreed and stated “[w]e hackin, all day every day.”

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

ttt. 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.”

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

vvv. On or about September 9, 2024, **LAM** bragged to

COCONSPIRATOR C.F., and COCONSPIRATOR-1 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.” COCONSPIRATOR C.F. 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.” COCONSPIRATOR C.F. 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.”

www. 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 COCONSPIRATOR C.D.

xxx. On or about September 9, 2024, COCONSPIRATOR C.F. and **LAM** discussed past victims and COCONSPIRATOR C.F. 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 [COCONSPIRATOR C.F.], we, not me, we have the most Dbs [databases] in this world, in this community bro.” COCONSPIRATOR C.F. replied “oh ye, it’s not even close.”

yyy. 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.

zzz. 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.

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

bbbb. 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.

cccc. On or about September 12, 2024, COCONSPIRATOR H.D. 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?” COCONSPIRATOR H.D. 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].”

dddd. On or around September 13, 2024, LAM, COCONSPIRATOR-1, and others engaged in a group chat discussing social engineering thefts. LAM stated “man let’s just say the fbi better arrest me before October.” responded “LOL.” LAM replied “if not I swear to all of you we will make 50m ++ before December lol. I am going to grind so hard.”

eeee. On or around September 13, 2024, LAM, and others participated in a group chat titled “money,” that had victim information, including phone number, full name, and suspected crypto holdings, pinned to the top of the group chat.

ffff. On or about September 13, 2024, LAM shared a 4.5 gb data package with and others for use in social engineering fraud schemes. LAM stated “wait until you open the folder. LOL it’s go mode. Every single thing I’ve ever worked on. . . is in there.” responded “I needa get some fucking popcorn.”

gggg. On or about September 14, 2024, COCONSPIRATOR-2 and COCONSPIRATOR C.F. discussed the new cars LAM was purchasing with stolen

virtual currency. COCONSPIRATOR-2 then asked if the cars were under **MEHTA**'s name. COCONSPIRATOR C.F. responded "All my cars are chilling. I got all mine under him [**MEHTA**]. I got no clue how he [**LAM**] has his set up."

hhhh. 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."

iiii. 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."

jjjj. On or about September 16, 2024, COCONSPIRATOR C.F. told COCONSPIRATOR-2 "look what I smacked." COCONSPIRATOR-2 responded, "I heard a crazy seed [phrase]." COCONSPIRATOR C.F. replied "ended up being 5.8" million, referring to the Victim-8 theft. COCONSPIRATOR-2 replied

“Bonkers. . . that must’ve been [a] new car that day for u. New Newport house too. 1 yr lease.” COCONSPIRATOR C.F. then sent COCONSPIRATOR-2 a photo of a luxury watch he purchased with the stolen virtual currency.

kkkk. On or about September 16, 2024, COCONSPIRATOR C.F. 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.

llll. On or about September 16, 2024, COCONSPIRATOR-2 told COCONSPIRATOR C.F. 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 COCONSPIRATOR H.D. to perform the unlicensed virtual currency exchange to fiat currency with COCONSPIRATOR-2’s stolen virtual currency.

mmmm. On September 17, 2024, COCONSPIRATOR H.D. 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.

nnnn. On or about September 17, 2024, COCONSPIRATOR H.D. 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.

oooo. Throughout September 2024, **LAM**, COCONSPIRATOR H.D., 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.

pppp. 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**.

qqqq. On or about September 18, 2024, **LAM** walked to the rear of his Miami rental home and tossed 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**.

rrrr. On or about September 18, 2024, while in Los Angeles, **TANGEMAN** used his remote access to the security cameras located at **LAM**'s Miami rental homes to watch FBI Agents search the residence, inventory evidence, and share the video with other members of the SE Enterprise.

ssss. Following **LAM**'s arrest on or about September 18, 2024, **TANGEMAN** solicited other members of the S.E. Enterprise to retrieve digital devices owned by **LAM** and COCONSPIRATOR M.F. and destroy them.

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

uuuu. 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.

vvvv. On or about September 23, 2024, **LAM** spoke with **YARALLY** and **COCONSPIRATOR C.D.** and asked if they had been in contact with “Nic [REDACTED]” and told them to “tell Nic [REDACTED] to give [them] a number where [**LAM**] can call him,” because “Nic’s loyalty dies with me.” **LAM** further stated that “both their loyalty dies with me.” **LAM** then asked **YARALLY** and **COCONSPIRATOR C.D.** if the video that was released of the Victim-7 theft was “my screen.” They responded “no, it’s [Co-Conspirator 1’s screen].” **LAM** finally told **YARALLY** and **COCONSPIRATOR C.D.** that [REDACTED] and two other co-conspirators’ “loyalty dies with me” and “they’ll take care of all y’all for like for 5-10 years until I’m on the outside. . . Nic [REDACTED] especially Nic [REDACTED] will do anything for me.” **LAM**, **YARALLY**, and **COCONSPIRATOR C.D.** then discussed being excited that **LAM** was “TikTok famous,” for the cryptocurrency thefts.

www. On or about September 27, 2024, **LAM** asked **YARALLY** if he had spoken with [REDACTED] and **YARALLY** responded “yeah, we’re about to go see them on the jet right now.” **LAM** then informed **YARALLY** that [REDACTED] and other coconspirators “will pay anything for me, I’m confident they’ll pay anything for me.” **YARALLY** then facilitated a three-way phone call between **LAM** and another co-conspirator where **LAM** told this co-conspirator that he and [REDACTED] needed to provide anything that **YARALLY** needed until **LAM**

was out of jail.

xxxx. On or about September 27, 2024, helped YARALLY and COCONSPIRATOR C.D. flee Miami after LAM's arrest using a private jet paid for with stolen cryptocurrency and arranged through COCONSPIRATOR H.D.

yyyy. 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 [COCONSPIRATOR H.D.] 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."

zzzz. On or about September 28, 2024, YARALLY informed LAM that COCONSPIRATOR C.F. was selling a car to pay for lawyers. LAM responded "Why is he selling [their] M3s...Tell Conor [COCONSPIRATOR C.F.] 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."

aaaaa. 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 did not want to identify their location over the recorded line.

bbbb. From in or around November 2024 and continuing through at least March 2024, COCONSPIRATOR M.F. 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.

cccc. On or about October 21, 2024, and other co-conspirators executed a social engineering fraud scheme against Victim-9 and stole approximately \$2,000,000 in virtual currency from Victim-9.

dddd. On or about October 21, 2024, and others laundered the Victim-9 stolen virtual currency using the same process employed during the Victim-7 theft. They then split the funds among one another and sent some of the stolen funds to COCONSPIRATOR-1.

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

ffff. In or around November and December 2024, **YARALLY** sent COCONSPIRATOR M.F. approximately \$55,000 in fraud proceeds to support **LAM**.

gggg. From in or around November 2024 and continuing through March 2025,

COCONSPIRATOR M.F. regularly passed messages on **LAM**'s behalf inside of jail to members of the SE Enterprise, to include COCONSPIRATOR C.F., **YARALLY**, **TANGEMAN**, COCONSPIRATOR H.D., and others.

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

iiii. In or around January and February 2025, COCONSPIRATOR H.D., **YARALLY**, COCONSPIRATOR C.D., 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."

jjjj. In or around February or March of 2025, **YARALLY**, COCONSPIRATOR C.F. and others attempted to execute social engineering fraud schemes from Dubai in the United Arab Emirates.

kkkk. In or around April of 2025, used the money laundering services of **MEHTA** and COCONSPIRATOR H.D. to rent a luxury penthouse apartment in Miami, Florida.

llll. On or about May 13, 2025, COCONSPIRATOR C.F. possessed approximately \$8,000,000 in stolen cryptocurrency.

mmmm. On or about May 13, 2025, **MEHTA** possessed approximately \$300,000 in fiat cash that was being used in a crypto-to-cash money laundering transaction.

nnnn. On or about May 13, 2025, **TANGEMAN** possessed over \$10,000 in fiat cash in his apartment.

ooooo. On or about May 13, 2025, COCONSPIRATOR M.F. possessed two firearms in his residence, one which was given to him by **MEHTA**.

(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 May 2025, within the District of Columbia and elsewhere, the defendants,

MALONE LAM,
also known as “King Greavvs,” “\$\$\$,” “7,” “Kg,”

ETHAN YARALLY,
also known as “Rand,” and “15%,”
AAKAASH ANAND,
also known as “Light,” and “Dark,” and
FNU LNU-1,
Also known as “~_~” “Squiggly,” and “CHEN,”

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, Victim-8, Victim-9 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 May 2025, within the District of Columbia and elsewhere, the defendants,

MALONE LAM,
also known as “King Greavys,” “\$\$\$,” “7,” “Kg,”

KUNAL MEHTA,
also known as “Papa,” “The Accountant,” “Shrek,” and “Neil,”
AAKAASH ANAND,
also known as “Light,” and “Dark,” and
EVAN TANGEMAN,
also known as “E,” “Tate,” “Evan | Exchanger,”

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,** 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. **LAM,** **YARALLY,** COCONSPIRATOR-1, COCONSPIRATOR-2, COCONSPIRATOR C.F., COCONSPIRATOR C.D., and others, using various virtual currency exchanges (“VCEs”) that require little to no identifying information such as Thorswap or eXch to change stolen cryptocurrency into privacy coins such as Monero (XMR), in order to disguise and conceal the location, ownership, and origin of the cryptocurrency.

*

- c. Co-conspirators including **LAM, CHEN,** and others using peel chains and pass-through wallet addresses for the purpose of concealing ownership and disguising the location of the stolen funds.
- d. COCONSPIRATOR M.F. 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;
- e. **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.
- f. COCONSPIRATORS H.D., J.C., **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.
- g. COCONSPIRATOR J.C. shipping squishmallow® stuffed animals containing fiat cash across the country, knowing the funds represented criminally derived proceeds.
- h. COCONSPIRATOR T.D. 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.
- i. **ANAND** assisting with swapping and laundering stolen virtual currency on various VCE platforms.

- j. 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.
- k. **LAM, META, COCONSPIRATOR H.D., ANAND, COCONSPIRATOR J.C., COCONSPIRATOR T.D., COCONSPIRATOR M.F., CHEN,**
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)

FORFEITURE

43. 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, Section 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 in violation of 1962.

44. The allegations contained in COUNT TWO of this Indictment is 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 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.

45. 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

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

Cryptocurrency

- C1) 457,997.495978 USDT (\$458,256.26) currently located at virtual currency address 0xc63f41909DfeDEE97Cf88Ac3EfE7a5e2c3F7a462
- C2) 1,020,392 USDT (\$1,020,968.52) currently located at virtual currency address 0x588d86Fb0B8d8A318aDc5cFc7Dd460E1794D1e5c
- C3) 6.72069 ETH (\$26,769.31) currently located at virtual currency address 0x588d86Fb0B8d8A318aDc5cFc7Dd460E1794D1e5c
- C4) 0.2 ETH (\$827.52) transferred from virtual currency address 0xe8bde8169a2f6ed6855201afcac7be05a5639b25

- C5) 1,033.12224964 ETH (\$4,274,667.28) transferred from virtual currency address 0xe8bde8169a2f6ed6855201afcac7be05a5639b25
- C6) 499.99917711 ETH (\$2,068,806.60) transferred from virtual currency address 0xf40d997d761d39c57d57e9c7c39a8adf1b9bb3b3
- C7) 3.45229143 ETH (\$14,284.27) transferred from virtual currency address 0x7c3b327a07d0e27e4724510fbb05bc122ddd1fc6
- C8) 0.74997756 ETH (\$3,103.12) transferred from virtual currency address 0xbeca5140b0476b821dbb3ba410e02da39d141234
- C9) 0.5563215 ETH (\$2,301.85) transferred from virtual currency address 0xd2a61dade9fe4a1d4908fe68527b627cbe20d67e
- C10) 0.50262729 ETH (\$2,079.68) transferred from virtual currency address 0x74d579ab0aa2e610ab2b1a5c5fa32a32625679ca
- C11) 1031.68 USDT (\$1,032.26) transferred from virtual currency address 0x5a04e69A170FEE08Fa7Ce6530B3176a50D4754c5
- C12) 960.640622 USDT (\$961.18) transferred from virtual currency address 0x6A7633590095708ca4a3EE51ba2478A85ae2CfC1
- C13) 0.39913449 ETH (\$1,651.47) transferred from virtual currency address 0x4941a7be8441ffcc8f448aa5ff7bb31fleaf592f
- C14) 0.35656158 ETH (\$1,475.32) transferred from virtual currency address 0xd2e50f7d1dcb1cd39591dd2b9c7c1f482c9a70e7
- C15) 0.01004729 ETH (\$41.57) transferred from virtual currency address 0x21c90c1635afb5d5c09be0447eb92911e8fb02d3
- C16) 704.383325 USDT (\$704.78) transferred from virtual currency address 0x067ba3e7Ecbc4f6822f49271712a5e0120DF0c4d
- C17) 635.40673 USDT (\$635.77) transferred from virtual currency address 0xf4F49357fEF859a2DF8c40235C641D5eB08f6c1b

Vehicles

- V1) 2022 Ferrari SF90 Stradale, VIN: ZFF95NLA2N0274061
- V2) 2024 Mercedes-Benz G Class, VIN: W1NYC7HJ6RX512875
- V3) 2022 Mercedes-Benz s580, VIN: W1K6G7GB7NA126661
- V4) 2021 Bentley Flying Spur, VIN SCBBB6ZG0MC085063
- V5) 2024 Mercedes-Benz G, VIN: W1NYC7HJ8RX503658
- V6) 2019 Lamborghini Aventador LP770, VIN: ZHWUM6ZD24LA08868
- V7) 2023 Ferrari SF90 Spider, VIN ZFF96NMA0P0291651, with accessories
- V8) 2019 Rolls Royce Ghost, VIN SCATV0CO2MU27053
- V9) 2023 Mercedes-Benz G Wagon, VIN W1NYC7HJ9PX489640
- V10) 2024 Porsche 911 GT3 RS, VIN WP0AF2A96RS272078
- V11) 2022 Rolls Royce Ghost, VIN SCATV0C05NU211485

Cash

- C1) Cash in brown Louis Vuitton bag totaling \$169,700
- C2) Cash in black Samsonite bag totaling \$44,714
- C3) Cash in bag totaling \$275,212
- C4) One Hundred Ten (110) \$100 bills totaling \$11,000

Miscellaneous

- M1) Louis Vuitton bag
- M2) Black Samsonite bag
- M3) Black Louis Vuitton keychain
- M4) Diamond-encrusted bracelet
- M5) Seven bracelets
- M6) Key Fobs - Ferrari x1 BMW x3 Mercedes Benz x1
- M7) Louis Vuitton suitcase Brown and orange
- M8) Louis Vuitton Duffel Bag Black Check
- M9) Louis Vuitton Suitcase Bag
- M10) Louis Vuitton Small suitcase
- M11) Louis Vuitton Dop Kit
- M12) Louis Vuitton Wallet Black check full zip
- M13) Louis Vuitton Roll case Black
- M14) Louis Vuitton backpack Brown and orange
- M15) Louis Vuitton backpack black check
- M16) Louis Vuitton card case black
- M17) Louis Vuitton wallet Blackcheck, no zipper
- M18) Designer shirts, pants, belts, and jackets (Louis Vuitton etc.) A-E 2 boxes,
3 bags
- M19) Royal Oak Offshore Automatic Watch
- M20) Louis Vuitton et al receipts
- M21) Cartier Bracelet white gold with diamonds
- M22) Diamond Ring with solitaire cut
- M23) Cartier bracelet gold with diamonds
- M24) Cartier chain bracelet gold with diamonds
- M25) Diamond Stud earring (single)
- M26) White gold diamond ring band
- M27) Gold/diamond ring band
- M28) Cross pendant gold diamond earrings
- M29) Cartier chain white gold with diamonds
- M30) Gold diamond bracelet
- M31) Cartier bracelet, gold with diamonds
- M32) Louis Vuitton bracelet with clear stones SN 154502, Au750
- M33) Swarovski diamond bracelet
- M34) Rolex watch #116233
- M35) Richard Mille watch RM 35-01 SN RM3501 AOCA/203
- M36) Van Cleef bracelet, blue
- M37) Van Cleef bracelet, black

- M38) Van Cleef bracelet, white
- M39) Van Cleef bracelet, red
- M40) Rolex watch rose gold & silver with diamonds
- M41) Audemars Piguet Royal Oak Offshore - WF4785K
- M42) Richard Mille 11-03 watch SN RM11-03 RG/2748
- M43) Richard Mille 055 watch SN RM055 AATI/214
- M44) Richard Mille 11-03 watch, SN RM11-03 FQ1819
- M45) Richard Mille 30-01 watch, S/N RM30-01 Tirg/456
- M46) Richard Mille 65-01 watch, multiple bands
- M47) Van Cleef & Arpels bracelet 5 Motif green, yellow gold, malachite
diamonds
- M48) Van Cleef & Arpels bracelet Alhambra 5 motif, yellow gold, Guilloche
diamonds
- M49) Shotgun, Hawk Model 981R SN 0099154
- M50) 4x mags (1 empty) & 45mm ammo
- M51) Camo Handgun ammunition, 8 rounds
- M52) Camo Handgun Serial BXST341
- M53) Smith & Wesson ammo. 6 rounds and 2 magazines
- M54) Smith & Wesson Pistol JRP1176
- M55) 16 rounds of 9mm ammunition
- M56) Springfield Pistol
- M57) Black Geisler Pistol, SL-1071 Solarfish Light Attached, with one (1) empty
9mm 18 capacity magazine
- M58) Two 9mm Luger R-P Rounds
- M59) Black Chanel Boots
- M60) Wells Fargo Statements
- M61) Gray Louis Vuitton Backpack
- M62) Green Rene Caovilla Sandals
- M63) Black Chanel Purse with Gold Chain
- M64) Pink Hermes Slides
- M65) Black Louis Vuitton Case
- M66) Black Hermes Slides with Sheepskin
- M67) Brown Hermes Slides with Sheepskin
- M68) White Hermes Sandals with Velcro Straps
- M69) Black Hermes Sandals
- M70) White Hermes Sandals
- M71) Brown Hermes Sandals
- M72) Black Rubber Chanel Rain Boots
- M73) Black Louboutin Heeled Boots
- M74) Silver and Clear Femine Heels
- M75) Pink Patent Leather Louboutin Heels
- M76) White Louboutin Heels
- M77) Black Louboutin Sandals with Metal Studs
- M78) Black Louboutin Heels

M79) Patek Philippe Watch, REF 39701 W
M80) Necklace with clear gems

MONEY JUDGMENT

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

SUBSTITUTE ASSETS

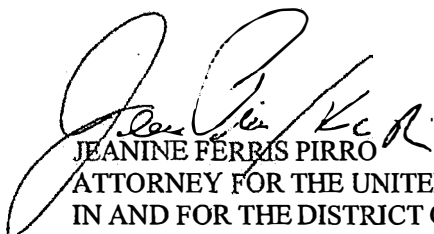
48. If any of the property described above, as a result of any act or omission of the defendant(s):

- 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


JEANINE FERRIS PIRRO
ATTORNEY FOR THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA