HDM/DMP/CQ/DGR/AFM/JP:NMA/ADR/TH
F. #2023R00907

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

ANDEAN MEDJEDOVIC,

Defendant.

----------X

24-CR-529

FILED UNDER SEAL

I N D I C T M E N T

Cr. No. _____
(T. 18, U.S.C., §§ 924(d)(1), 981(a)(1)(C), 982(a)(1), 982(a)(2), 982(b)(1), 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(i)(1), 1030(i)(2), 1343, 1951(a), 1956(a)(1)(B)(i), 1956(h), 3238, 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

Judge Nicholas G. Garaufis
Magistrate Judge Vera M. Scanlon

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

I. Overview

1. Between approximately 2021 and 2023, the defendant ANDEAN MEDJEDOVIC exploited vulnerabilities in the automated smart contracts used by the KyberSwap and Indexed Finance decentralized finance protocols to fraudulently obtain approximately $65 million in digital tokens from the protocols' investors, including investors in the United States. To further his fraudulent schemes, MEDJEDOVIC borrowed hundreds of millions of dollars in digital tokens, which he used to engage in deceptive trading that he knew would cause the protocols' smart contracts to falsely calculate key variables. Through his deceptive trades, MEDJEDOVIC was able to, and did, withdraw millions of dollars of investor funds from the protocols at artificial prices, rendering the victims' investments essentially worthless.

2. After fraudulently obtaining the tokens, the defendant ANDEAN MEDJEDOVIC laundered the proceeds of his fraudulent schemes through a series of transactions designed to conceal the source and ownership of the funds, including through swap transactions, "bridging transactions" and the use of a digital assets "mixer." MEDJEDOVIC, together with others, also schemed to open accounts with digital asset exchanges using false and borrowed identifying information to conceal the source and true ownership of the proceeds.

3. Following the KyberSwap exploit, in or about November 2023, the defendant ANDEAN MEDJEDOVIC also attempted to extort the victims of the KyberSwap exploit through a sham settlement proposal. Among other things, MEDJEDOVIC demanded complete control of the KyberSwap protocol and the decentralized autonomous organization (or "DAO") that oversaw the KyberSwap protocol in exchange for returning 50% of the digital assets that he fraudulently obtained through this scheme.

II. Background

A. The Defendant and a Co-Conspirator

4. The defendant ANDEAN MEDJEDOVIC was a citizen of Canada and resided outside the United States.

5. Co-Conspirator-1, an individual whose identity is known to the Grand Jury, was a relative of the defendant ANDEAN MEDJEDOVIC and resided in Canada and Cambridge, Massachusetts, among other places.

B. Relevant Definitions and Terms and Related Entities

i. Digital Assets

6. A "digital asset" or "digital token" was an asset issued and transferred using distributed ledger technology. The creation of a digital asset, and transactions using the digital asset, were verified and recorded on a decentralized system using cryptography, rather than through a centralized authority like a bank or government.

7. Certain digital tokens were "investment contracts." Investment contracts were instruments, schemes or transactions through which a person invested money in a common enterprise and reasonably expected profits or returns derived from the entrepreneurial or managerial efforts of others. Investment contracts were "securities" as defined by the Securities Exchange Act of 1934, 15 U.S.C. § 78c(a)(10).

8. A "blockchain" was a digital ledger run by a decentralized network of servers referred to as "nodes." Each node ran software that maintained an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets publicly recorded all of their transactions on a blockchain, including all of the known balances for each digital asset address on the blockchain. Blockchains consisted of blocks of cryptographically signed transactions, and blocks were added to the blockchain after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There were many different blockchains used by many different digital assets. For example, Bitcoin ("BTC") existed in its native state on the Bitcoin blockchain, while Ether ("ETH") existed in its native state on the Ethereum network.

9. A "digital asset address" was an alphanumeric string that designated the virtual location on a blockchain where digital assets could be sent and received. A digital asset address was associated with a digital asset wallet.

10. A "digital asset wallet" stored a user's public and private keys, allowing users to send and receive digital assets stored on the blockchain. Multiple digital asset addresses could be controlled by a single wallet.

11. "Smart contracts" were computer programs or transaction protocols that were intended to automatically execute according to preset terms and rules that were encoded in the contract that resided on the blockchain.

12. A "crypto-mixer" or "tumbler" pooled potentially identifiable tainted digital assets, such as funds flagged as proceeds of crimes, with other digital assets in order to obscure the source of the tainted digital assets.

ii. The Ethereum Network and Related Entities

13. The "Ethereum network" was a blockchain technology platform that supported a range of decentralized applications ("dApps"), including digital tokens. Users of the Ethereum network typically accessed the Ethereum network through uniform resource locators ("URLs") called RPC endpoints. The Ethereum network supported smart contracts.

14. "Bridges" were a type of decentralized application that facilitated the transfer of digital tokens and other digital assets from one blockchain to another.

15. The "Ethereum Virtual Machine" ("EVM") was the single state machine that was implemented by full nodes running the Ethereum protocol. The full nodes of the EVM stored and updated the Ethereum blockchain's current state and recorded updates to the blockchain including, among other things, information from applications running on the Ethereum

network, including account balances, smart contract code and changes made to the blockchain. Archive nodes performed the same functions as full nodes and also stored all historical data on the Ethereum blockchain. As of in or about November 2023, there was an archive Ethereum node located in the Eastern District of New York.

16. As with many blockchains, when executing digital asset trades on the Ethereum blockchain, profitable digital asset trades were susceptible to "front running" by other market participants. In particular, profitable trades could be identified by other participants—often algorithms or "bots"—while those trades were pending execution on the blockchain as they were visible in public memory pools or "mempools."

17. Developer-1, an entity the identity of which is known to the Grand Jury, created and marketed a decentralized application called "RPC Protect" that provided a private alternative to the public "mempool." The Ethereum nodes and servers used by Developer-1 were located in Ohio.

iii. The Arbitrum Network and Related Entities

18. The "Arbitrum network" was a "Layer 2" blockchain technology platform that operated in conjunction with the Ethereum network. The Arbitrum network's state, including account balances, smart contract code and changes made, were maintained on the EVM.

19. "Layer 2 Developer," an entity the identity of which is known to the Grand Jury, was the U.S.-based developer of the Arbitrum network.

20. Transactions on the Arbitrum network were typically submitted to and ordered by a centralized "sequencer" operated by Layer 2 Developer. The Arbitrum sequencer executed transactions on the Arbitrum network, provided receipts to the submitter of the transaction and submitted transactions from the Arbitrum network to the Ethereum network in

batches. The Ethereum nodes and servers used by Layer 2 Developer and the Arbitrum sequencer were located in Oregon.

iv. Decentralized Finance and Related Entities

21. "Decentralized Finance," or "DeFi," was an umbrella term for blockchain-based applications providing peer-to-peer financial services that did not require traditional centralized financial intermediaries. DeFi platforms offered a range of financial services involving digital assets, including the ability for users to lend, invest, earn interest and exchange digital assets. DeFi platforms provided these services through smart contracts, which were accessible to users through dApps.

22. A "decentralized exchange" ("DEX") was a peer-to-peer marketplace where users could trade digital assets with other traders without centralized intermediaries. DEX users generally retained control over their digital assets rather than entrusting a central authority to host funds in a centralized or "hosted" wallet. DEXs were operated by smart contracts, which automated the trading process.

23. A "liquidity pool" was a pool of paired digital tokens (e.g., "Token A" and "Token B") locked in a smart contract. Liquidity pools played the same role in DeFi as market makers in traditional finance by providing liquidity to DeFi traders who wanted to exchange or swap one of the digital tokens in the pool for the other, i.e., trading Token A for Token B or vice versa. Token prices in liquidity pools were expressed as exchange rates or ratios between Token A and Token B and typically tracked token prices in the market more generally.

24. Liquidity pools relied on investors to deposit digital tokens into the pools. These investors were generally referred to as "liquidity providers" ("LPs"). In exchange for providing liquidity, LPs were compensated with a share of the fees generated by transactions in

the liquidity pool. Deposits in liquidity pools were typically reflected by a form of non-fungible token called a "liquidity provider token" or "LP token." LP tokens functioned as receipts. Liquidity providers were able to redeem their LP tokens for their pro rata share of the digital assets and fees in the liquidity pool.

25. Liquidity pools relied on "automated market makers" ("AMMs") to facilitate digital asset trades and set prices. AMMs typically used pre-programmed functions and supply and demand to set prices in the liquidity pools so that they aligned with prices in the market more generally. For example, if the price of Token A in a liquidity pool was above the prevailing market price for Token A, arbitrage traders would use the pool to exchange Token A for Token B, increasing the supply of Token A in the liquidity pool and causing its price to fall into alignment with the market price.

26. A DAO was a governance mechanism used to manage DeFi protocols. DAOs provided a mechanism for stakeholders to vote on changes to the protocol including, for instance, changes to the functioning of the AMM.

27. A "flash loan" was an un-collateralized loan of digital assets in which a DeFi trader borrowed digital assets from a liquidity pool and repaid the pool plus a fee in a single cryptographic transaction. If a borrower did not pay back the flash loan in the same transaction, then the entire transaction was reverted, including the initial loan and any actions taken afterwards. DeFi traders could use flash loans to leverage trading strategies and increase their returns without posting collateral.

v. Indexed Finance

28. Indexed Finance was a decentralized exchange aggregator and operator of digital token liquidity pools on the Ethereum network. The Indexed Finance liquidity pools were available to and used by liquidity providers in the United States.

29. Certain of the digital tokens included in the Indexed Finance liquidity pools were investment contracts and "securities" as defined by the Securities Exchange Act of 1934, 15 U.S.C. § 78c(a)(10).

C. KyberSwap and KyberSwap Elastic

30. KyberSwap was a decentralized exchange aggregator and operator of digital token liquidity pools on several public blockchain technology platforms, including the Ethereum network and the Arbitrum network.

31. In 2022, KyberSwap launched a new liquidity pool product called KyberSwap Elastic. KyberSwap Elastic was a "concentrated" AMM. Concentrated AMMs improved market efficiency by permitting liquidity providers to pre-determine the price at which they were willing to provide liquidity to the pool. In a concentrated AMM, liquidity was "concentrated" within the price parameters specified by the liquidity providers. Liquidity contributed by liquidity providers within a specified price range could be used only for swaps in that price range.

32. In a concentrated AMM, prices were referred to as "ticks" and price ranges were referred to as "tick ranges." A "tick boundary" was the higher or lower bound of a tick range. Available liquidity in a concentrated AMM varied by tick range in accordance with the parameters specified by the liquidity providers.

33. Concentrated AMMs like KyberSwap Elastic generally executed swaps in steps, progressively adjusting price and using available liquidity in the current tick range until the swap was completed or the price reached the next tick. When a concentrated AMM reached a tick boundary, the concentrated AMM would adjust the price to a new tick and update liquidity by activating any dormant liquidity contributed at the new active tick.

34. The KyberSwap Elastic AMM used a function called "updateLiquidityAndCrossTick" to recalculate available liquidity, i.e. the liquidity available for trades at a particular price, each time the pool price crossed a tick boundary. If a swap did not cause the price to cross a tick boundary, the KyberSwap Elastic AMM used different functions, including "estimateIncrementalLiquidity," "calcFinalPrice" and "updatePoolData" to update the pool state, including the pool price.

35. The KyberSwap Elastic liquidity pools were available to and used by liquidity providers in the United States.

36. The Kyber Decentralized Autonomous Organization ("KyberDAO") was responsible for governance of the KyberSwap protocol. Proposed changes to the KyberSwap protocol were voted on by the KyberDAO. A "multiple signature" ("multisig") crypto wallet with nine signatories was used to submit proposals to the KyberDAO. Multisig wallets typically required two or more private key signatures to authorize transactions. At least one of the signatories to the KyberDAO multisig wallet was in the United States.

III. The KyberSwap Exploit

37. In or about November 2023, the defendant ANDEAN MEDJEDOVIC used hundreds of millions of dollars in borrowed digital tokens to manipulate prices in the KyberSwap Elastic liquidity pools and corrupt the functioning of the KyberSwap Elastic AMM. In

furtherance of the scheme, MEDJEDOVIC executed dozens of swaps that were intended to deceive the KyberSwap Elastic AMM by misrepresenting supply and demand in the KyberSwap Elastic liquidity pools and to fraudulently induce the KyberSwap Elastic AMM to miscalculate available liquidity at the artificial prices created by MEDJEDOVIC. By corrupting the functioning of the KyberSwap Elastic AMM, MEDJEDOVIC was able to drain approximately $48.4 million in digital tokens from 77 different KyberSwap Elastic liquidity pools, rendering the liquidity providers' LP tokens essentially worthless. After withdrawing the digital tokens from the KyberSwap Elastic liquidity pools, MEDJEDOVIC transferred the stolen digital tokens to digital asset wallets that he controlled.

38. The defendant ANDEAN MEDJEDOVIC understood that his conduct circumvented the intended functioning of the KyberSwap Elastic liquidity pools. Among other things, and as described further below, MEDJEDOVIC discussed a plan to "steal crypto," referred to the exploit as involving "glitch" and "fake" liquidity, and described the code for the exploit as a "rape." MEDJEDOVIC also described himself as a "pirate" and stated that he "may or may not be a criminal."

A. Planning the KyberSwap Exploit

39. The defendant ANDEAN MEDJEDOVIC carefully planned the KyberSwap exploit over a period of months. MEDJEDOVIC maintained a directory containing files related to the exploit called "arbitrage/KYBER_KILL/ARB_kyberArb." Among other things, MEDJEDOVIC drafted code labeled "templateexploit," which included a function called "templateexploit.rape()." MEDJEDOVIC also drafted and maintained a "POOL HIT LIST" that contained a list of the liquidity pools to be drained in the KyberSwap exploit. He planned the optimal time to execute the exploit, writing to himself "Find time to Strike! CEO is in Ho-Chi

Min 5:00AM HCM is 11:00pm for me *attacking around 7:00AM-8:00AM my time means most americans are asleep and euros too." MEDJEDOVIC also prepared a "POST-EXPLOITATION" plan for himself, which included, among other things, "*KEEP the configs *Burn the evidence, including the histfile" and "*Book flight to: *Pack Bags," as well as another file labeled "Decisions and Mistakes," in which he wrote, "Going On the run / Yes / Chance of getting caught<Payoff for not getting caught / (NA) / Risk is typically underpriced in modern world."

40. In or about October 2023, approximately two months before the KyberSwap exploit, in a private chat on an electronic communication service, the defendant ANDEAN MEDJEDOVIC wrote to another user, "I've been working but no breakthroughs yet . . . trying to make a breakthrough on the finite field version, so I can steal crypto lol."

B. The Exploit

41. On or about November 22, 2023, the defendant ANDEAN MEDJEDOVIC put his plan into action to exploit the KyberSwap Elastic liquidity pools. MEDJEDOVIC's plan was executed through a series of steps, which generally consisted of the following: (1) borrowing funds; (2) creating artificial prices in the KyberSwap Elastic liquidity pools; (3) submitting manipulative swaps to cause the KyberSwap Elastic AMM to miscalculate available liquidity at these artificial prices; (4) extracting liquidity from the KyberSwap Elastic liquidity pools; (5) repaying the flash loan; and (6) withdrawing tokens. Although the exploit involved numerous swaps, the swaps used to exploit each liquidity pool were submitted as a single cryptographic transaction, meaning that they were executed in nearly instantaneous succession, and the steps were substantially similar in each of the drained liquidity pools. Publicly available event logs created during the exploit and programmed by MEDJEDOVIC catalog the steps of the exploit in each of the liquidity pools.

42. For example, below is a description of the steps of the exploit in the KyberSwap Elastic liquidity pool for the digital tokens Wrapped Staked Ether ("wstETH") and Wrapped Ether ("wETH") on the Ethereum network.

a. Borrowing Funds. At the beginning of the exploit, MEDJEDOVIC borrowed 10,000 units of wstETH (valued at approximately $23.6 million at the time) through a flash loan from a leading DeFi protocol. Immediately after obtaining the flash loan, MEDJEDOVIC wrote "Raping Now" in the public event log for the transaction.

b. Creating Artificial Prices. MEDJEDOVIC then swapped approximately 2,842 units of borrowed wstETH (valued at approximately $6.2 million at the time) for approximately 2,998 units of wETH, flooding the liquidity pool with wstETH and removing substantially all of the wETH in the liquidity pool. This swap caused the pool price of wstETH to fall from 1.147 wETH to 0.0000152 wETH, a more than 99.99% discount to the most recent market price for wstETH. At the time, no liquidity provider had contributed liquidity at this artificial price.

c. Adding Liquidity at Artificial Prices. After creating artificial prices in the wstETH-wETH liquidity pool, MEDJEDOVIC contributed liquidity in a tick range corresponding to the artificial price he created (the "Artificial Tick Range"), which, in turn, gave the appearance of user-contributed liquidity at the artificial prices. In fact, MEDJEDOVIC never intended for this liquidity to be used for swaps with other market participants, and he referred to this liquidity as "Glitch Liquidity" and "fake liquidity." MEDJEDOVIC precisely calculated the amount of liquidity he contributed to set the stage for the next steps in the exploit and wrote in the event log that "the liquidity should be exact."

d. Triggering the Corrupt State. Next, the defendant ANDEAN MEDJEDOVIC executed a wash trade for approximately 99.999999999999999997% of the "Glitch Liquidity" that he had deposited in the wstETH-wETH liquidity pool. Because MEDJEDOVIC was the only liquidity provider in the Artificial Tick Range, MEDJEDOVIC was trading with himself.

i. This manipulative swap was precisely calculated to deceive the KyberSwap Elastic AMM so that it would miscalculate available liquidity. In particular, MEDJEDOVIC designed this swap to take advantage of a rounding error affecting two key functions of the KyberSwap Elastic AMM to circumvent the updateLiquidityAndCrossTick function so that the KyberSwap Elastic AMM would calculate an available liquidity value that did not reflect actual user contributions.

ii. In the wstETH-wETH pool, for example, MEDJEDOVIC submitted a swap quantity of 1,056,056,735,638,220,799,999. The KyberSwap Elastic AMM calculated that the swap quantity necessary to cross a tick boundary was 1,056,056,735,638,220,800,000. Because the submitted amount of the swap was slightly less than available liquidity in the Artificial Tick Range—liquidity MEDJEDOVIC contributed earlier in the exploit and specified must be "exact"—the KyberSwap Elastic AMM determined that there was sufficient available liquidity to execute the swap without crossing a tick boundary and did not run the updateLiquidityAndCrossTick function. However, a rounding error affecting the estimateIncrementalLiquidity and calcFinalPrice functions led the KyberSwap Elastic AMM to calculate a new price that exceeded the tick boundary. The result of this manipulative swap was a mismatch in the state of the KyberSwap Elastic AMM: specifically, the KyberSwap Elastic AMM calculated a new price in a new tick range but did not update available liquidity to reflect

user contributions in the new tick range, which were approximately zero. Instead, the KyberSwap Elastic AMM calculated available liquidity at this new price to be the same as the liquidity contributed by MEDJEDOVIC in the Artificial Tick Range, i.e. the "Glitch Liquidity."

iii. In the ordinary course, the rounding error affecting the estimateIncrementalLiquidity and calcFinalPrice functions would have only a minimal impact on price calculations. Only by controlling for price and liquidity through the earlier swaps in the exploit and then submitting a swap that was designed to use almost all available liquidity was the defendant ANDEAN MEDJEDOVIC able to take advantage of the rounding error to cause the KyberSwap Elastic AMM to calculate a new price in a new tick range without updating available liquidity.

e. Generating and Extracting Artificial Liquidity. The next step was intended to drain the KyberSwap Elastic pools by doubling the "Glitch Liquidity." MEDJEDOVIC submitted another swap in the opposite direction, causing the price to cross back over the tick boundary and triggering the updateLiquidityAndCrossTick function. This caused the KyberSwap Elastic AMM to add back the "Glitch Liquidity" and calculate available liquidity to be twice the amount MEDJEDOVIC originally contributed in the Artificial Tick Range. MEDJEDOVIC referred to this in the public event log as the "doubling move." This allowed MEDJEDOVIC to execute swaps for twice as much liquidity as he had deposited in the Artificial Tick Range. The digital tokens MEDJEDOVIC obtained through these swaps were contributed by other liquidity providers who did not agree to contribute liquidity at the artificial prices MEDJEDOVIC created. MEDJEDOVIC was able to execute these swaps only by corrupting the intended functioning of the KyberSwap Elastic AMM so that available liquidity no longer

reflected user contributions. As a result of the exploit, the liquidity contributed to the pool was used outside the price parameters agreed to by the users and without their permission.

f. Repaying the Flash Loan. After executing the "doubling move," MEDJEDOVIC repaid the flash loan plus interest and fees.

g. Withdrawing Tokens. Finally, MEDJEDOVIC withdrew 4.83 wstETH (valued at approximately $11,429) and 2,988.92 wETH (valued at approximately $6,192,204) from the wstETH-wETH pool, essentially draining the liquidity pool and rendering the LP tokens worthless. After transferring these digital tokens to his own digital asset wallet, MEDJEDOVIC wrote "DONEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE!" in the public event log for the transaction.

43. The defendant ANDEAN MEDJEDOVIC obtained approximately $6.2 million in digital tokens by draining the wstETH-wETH liquidity pool.

44. The defendant ANDEAN MEDJEDOVIC used substantially similar steps to drain 76 other KyberSwap Elastic liquidity pools on six public blockchains causing a total of $48.4 million in losses to the KyberSwap liquidity providers, including liquidity providers in the United States, thus rendering their LP tokens essentially worthless and the KyberSwap Elastic liquidity pools practically unavailable for use. Set out below is a list of the KyberSwap Elastic liquidity pools exploited on the Ethereum and Arbitrum networks, the exploit transactions used and the estimated market value of the stolen digital assets as of the time of the exploit:

Network	Pool	Exploit Transaction	Total Value Drained
Ethereum	frxETH-wETH	0x485e08dc2b6a4b3aeadcb89c3d18a37666dc7d9424961a2091d6b3696792f0f3	$15,595.63
Ethereum	MEME-wETH	0x485e08dc2b6a4b3aeadcb89c3d18a37666dc7d9424961a2091d6b3696792f0f3	$11,439.19
Ethereum	FRAX-USDC	0x485e08dc2b6a4b3aeadcb89c3d18a37666dc7d9424961a2091d6b3696792f0f3	$11,062.56
Ethereum	frxETH-wETH	0x485e08dc2b6a4b3aeadcb89c3d18a37666dc7d9424961a2091d6b3696792f0f3	$15,433.78

Network	Pool	Exploit Transaction	Total Value Drained
Ethereum	MONA-wETH	0x485e08dc2b6a4b3aeadcb89c3d18a37666dc7d9424961a2091d6b3696792f0f3	$10,753.35
Ethereum	wstETH-wETH	0x09a3a12d58b0bb80e33e3fb8e282728551dc430c65d1e520fe0009ec519d75e8	$6,203,633.46
Ethereum	wETH-KNC	0x09a3a12d58b0bb80e33e3fb8e282728551dc430c65d1e520fe0009ec519d75e8	$558,974.77
Ethereum	wETH-KNC	0x09a3a12d58b0bb80e33e3fb8e282728551dc430c65d1e520fe0009ec519d75e8	$502,368.00
Ethereum	wETH-HAY	0x396a83df7361519416a6dc960d394e689dd0f158095cbc6a6c387640716f5475	$8,607.46
Ethereum	USDC-ETHx	0x396a83df7361519416a6dc960d394e689dd0f158095cbc6a6c387640716f5475	$37,679.73
Ethereum	wETH-ELK	0x396a83df7361519416a6dc960d394e689dd0f158095cbc6a6c387640716f5475	$29,652.92
Ethereum	wstETH-USDC	0x396a83df7361519416a6dc960d394e689dd0f158095cbc6a6c387640716f5475	$36,493.40
Ethereum	frxETH-FRAX	0x396a83df7361519416a6dc960d394e689dd0f158095cbc6a6c387640716f5475	$23,422.58
Arbitrum	wETH-ARB	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$2,530,500.68
Arbitrum	wETH-ARB	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$564,936.74
Arbitrum	wETH-ARB	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$256,147.11
Arbitrum	wETH-ARB	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$169,625.67
Arbitrum	wstETH-axl-wstETH	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$1,875,758.68
Arbitrum	USDC-USDC.e	0xcea8599b8b82d5c17739fda9fe69a3e19a1613405929b3e191118681b702fc6a	$1,745,786.10
Arbitrum	wBTC-wETH	0x986e1683edea5d1c21a64ee6836d487c61127467494797 9023a433afaafaf7d0	$1,796,518.85
Arbitrum	wstETH-wETH	0x986e1683edea5d1c21a64ee6836d487c61127467494797 9023a433afaafaf7d0	$1,408,782.00
Arbitrum	DAI-USDC.e	0x986e1683edea5d1c21a64ee6836d487c61127467494797 9023a433afaafaf7d0	$1,627,380.13
Arbitrum	USDT-USDC.e	0x986e1683edea5d1c21a64ee6836d487c61127467494797 9023a433afaafaf7d0	$1,459,763.69
Arbitrum	USDC-USDT	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$1,078,782.71
Arbitrum	wETH-USDC.e	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$1,397,813.58
Arbitrum	wETH-USDC.e	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$228,023.28
Arbitrum	axlUSDC-USDC.e	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$843,396.92
Arbitrum	ARB-USDT	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$711,753.16
Arbitrum	ARB-USDT	0x339a65bb935f69e584ea979aa39282414371767576d4f1186a047768ef0a57c5	$215,867.04
Arbitrum	ARB-USDC.e	0x567f0ba7741d097b6b1aaba68e8b75b9930f3cf946681cf9ad068aa34eb11c5b	$887,641.44

Network	Pool	Exploit Transaction	Total Value Drained
Arbitrum	wETH-swETH	0x567f0ba7741d097b6b1aaba68e8b75b9930f3cf946681cf9ad068aa34eb11c5b	$418,959.39
Arbitrum	ARB-KNC	0x567f0ba7741d097b6b1aaba68e8b75b9930f3cf946681cf9ad068aa34eb11c5b	$286,131.63
Arbitrum	wETH-GMX	0x567f0ba7741d097b6b1aaba68e8b75b9930f3cf946681cf9ad068aa34eb11c5b	$292,493.76
Arbitrum	wETH-USDT	0x567f0ba7741d097b6b1aaba68e8b75b9930f3cf946681cf9ad068aa34eb11c5b	$342,304.48
Arbitrum	wstETH-KNC	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$170,568.06
Arbitrum	wstETH-USDC	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$237,707.55
Arbitrum	wETH-SWTH	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$80,510.79
Arbitrum	KNC-LINK	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$67,277.17
Arbitrum	fUSDC-USDC.e	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$32,291.38
Arbitrum	ARB-LINK	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$27,739.25
Arbitrum	wETH-ELK	0x0106c7549ac4e0de16aefce2b8fe339127ee8003b236f623d05edc41429de779	$11,986.95
Arbitrum	STG-ARB	0x8464ee4eab7e10c9c07aee4637644708cd0ce43a7265f481eac2dfb0dbab942c	$346.57

45. The defendant ANDEAN MEDJEDOVIC submitted at least two of the exploit transactions on the Ethereum network through RPC Protect and the Ethereum nodes and servers used by RPC Protect. The exploit transactions on the Arbitrum network were submitted through the Arbitrum sequencer and the Ethereum nodes and servers used by the Arbitrum sequencer.

46. Following the exploit, KyberSwap suspended new contributions to the KyberSwap Elastic liquidity pools and discontinued KyberSwap Elastic.

IV. The Attempted Extortion

47. In the hours following the KyberSwap exploit, the defendant ANDEAN MEDJEDOVIC began an attempt to extort the members of the KyberDAO, KyberSwap liquidity providers and the KyberSwap developers.

48. On or about November 22, 2023, approximately one hour after the KyberSwap exploit, the defendant ANDEAN MEDJEDOVIC sent a direct on-chain message through RPC Provider, an entity the identity of which is known to the Grand Jury, to a digital asset address used to deploy the KyberSwap liquidity pools. MEDJEDOVIC wrote:

> Dear Kyberswap Developers, Employees, DAO members and LPs,
> Negotiations will start in a few hours when I am fully rested.
> Thank you.

49. In response to this message, the KyberSwap developers offered the defendant ANDEAN MEDJEDOVIC a 10% "bounty" for the return of the digital tokens he obtained through the KyberSwap exploit.

50. Five days later, on or about November 28, 2023, the defendant ANDEAN MEDJEDOVIC sent another on-chain message through RPC Provider to the KyberDAO multisig wallet:

> Dear Kyberswap Executives, Employees, Token Holders and LPs, I said I was willing to negotiate. In return, I have received (mostly) threats, deadlines, and general unfriendliness from the executive team. That's ok, I don't mind. I have prepared a statement concerning our (potential) treaty. I plan to release it on Nov. 30 at Noon UTC, sharp. Under the assumption that I am treated with further hostility, we can reschedule for a later date, when we all feel more civil. You need only say the word. If not, we proceed as planned on Nov. 30. Thank you.

51. On or about November 30, 2023, the defendant ANDEAN MEDJEDOVIC sent a second on-chain message through RPC Provider to the KyberDAO multisig wallet. This message was addressed to "ALL relevant and/or interested parties" of KyberSwap, including "Token Holders and Investors" and "LPs." In the message, MEDJEDOVIC demanded control of KyberSwap "the company," and "temporary full authority and ownership over the governance mechanism (KyberDAO)."

52. The defendant ANDEAN MEDJEDOVIC wrote that "once [his] demands have been met" he would provide "LPs" "a rebate on your recent market-making activity. The rebate will be for 50% of the losses you incurred. I know this is probably less than what you wanted. However, it is also more than you deserve."

53. The defendant ANDEAN MEDJEDOVIC also addressed "Token Holders and Investors." He wrote that "under this treaty, your tokens will no longer be worthless. Is this not sweet enough? I'll go further still. Under my management, Kyber will undergo a complete makeover. It will no longer be the 7th most popular DEX, but rather, an entirely new cryptographic project."

54. As part of the proposed "treaty," the defendant ANDEAN MEDJEDOVIC warned the recipients of his messages not to involve any governments or law enforcement. MEDJEDOVIC wrote, "should I be contacted by agents from any of the 206 sovereignties, concerning the trades I placed on Kyber, the treaty falls through. In this case, rebates will total to exactly 0."

V. The Indexed Finance Exploit

55. On or about October 14, 2021, the defendant ANDEAN MEDJEDOVIC used similar means to exploit the Indexed Finance DeFi protocol to steal approximately $16.5 million in digital tokens from two Indexed Finance liquidity pools.

56. The Indexed Finance liquidity pools were referred to as "index pools," and functioned similarly to a mutual fund or exchange-traded fund ("ETF") in traditional finance. Instead of holding an index or basket of traditional equities, index pools held an index of digital tokens. Like ETF shares, the price of the LP tokens in the Indexed Finance liquidity pools was intended to track the net asset value of the digital tokens in the liquidity pool. The Indexed

Finance liquidity pools used an AMM (the "Indexed Finance AMM") and a related smart contract called the "Index Controller" to manage the Indexed Finance liquidity pools.

57. The "DeFi Top 5 Tokens Index" was an index pool composed of the top five Ethereum-based digital tokens by market capitalization (the "DEFI5 Pool"). The LP token associated with the DeFi Top 5 Tokens Index liquidity pool was called DEFI5. In or about October 2021, the DEFI5 index was composed of the digital tokens UNI, AAVE, CRV, COMP, MKR and SNX, the latter of which was being phased out of the index. Liquidity providers could use the DEFI5 Pool to invest in the index of tokens held by the DEFI5 Pool by depositing digital tokens in the DEFI5 Pool in exchange for DEFI5 tokens.

58. The "Cryptocurrency Top 10 Tokens Index" was an index pool composed of the top 10 Ethereum-based digital tokens (the "CC10 Pool"). The LP token associated with the Cryptocurrency Top 10 Tokens Index was called "CC10." In or about October 2021, the CC10 index was composed of the digital tokens UNI, AAVE, CRV, COMP, MKR, SNX, BAT, LINK, YFI and UMA. Liquidity providers could use the CC10 Pool to invest in the index of tokens held by the CC10 Pool by depositing digital tokens in the CC10 Pool in exchange for CC10 tokens.

59. On or about October 14, 2021, the defendant ANDEAN MEDJEDOVIC exploited vulnerabilities in the Index Controller and Indexed Finance AMM to obtain approximately $16.5 million in digital tokens from the DEFI5 and CC10 liquidity pools.

60. The Indexed Finance exploit took advantage of a process called "re-indexing" which was used to add new tokens to the DEFI5 and CC10 liquidity pools in response to changes in the market capitalization of digital tokens. For instance, if a new token overtook by market capitalization any of the five digital tokens included in the DEFI5 index, a re-indexing would be necessary to add the new digital token to the DEFI5 index and remove the previously

included token with the lowest market capitalization. The re-indexing process was managed by the Index Controller.

61. To exploit the DEFI5 liquidity pool, the defendant ANDEAN MEDJEDOVIC triggered a re-indexing to add the SUSHI digital token to the DEFI5 Pool. MEDJEDOVIC then took out a flash loan of approximately $157 million in digital tokens, which he used to manipulate supply and demand in the DEFI5 Pool in order to create artificial prices and drain the pool of UNI. MEDJEDOVIC used over $100 million in borrowed tokens to swap for almost all of the UNI in the DEFI5 Pool, driving up the price of UNI in the DEFI5 Pool to approximately 860 times its then-market price.

62. After creating artificial prices, the defendant ANDEAN MEDJEDOVIC triggered a function in the Index Controller called UpdateMinimumBalance, which was used to reset the weight of the assets in the DEFI5 index during the re-indexing process. Calling the UpdateMinimumBalance function at distorted pool prices caused the Index Controller to dramatically undervalue the digital tokens held by the DEFI5 Pool and dramatically overvalue SUSHI. Because of the price distortion caused by MEDJEDOVIC, the Index Controller estimated the value of the digital tokens held by the DEFI5 Pool to be approximately $314,100 when the market value of these tokens was in fact approximately $117.2 million. This in turn caused the Index Controller to overvalue SUSHI. As a result of MEDJEDOVIC's manipulation, a user could swap 299 SUSHI tokens with a market value of $3,200 for digital tokens in the DEFI5 Pool with a market value of $1.17 million.

63. Next, the defendant ANDEAN MEDJEDOVIC gifted approximately $2.4 million worth of SUSHI tokens to the DEFI5 Pool. This gift was illusory and intended to circumvent trade volume restrictions built into the re-indexing process by the Indexed Finance

developers to prevent manipulation and the intended functioning of the re-indexing process. MEDJEDOVIC used a function called gulp, intended by the Indexed Finance developers to be used in response to erroneous trades, to force the Indexed Finance AMM to integrate the gifted tokens. The "gift" distorted the re-indexing process and caused the Indexed Finance AMM to dramatically undervalue the digital tokens in the pool. Following the "gift," the Indexed Finance AMM set pool prices implying that the digital tokens in the pool were worth approximately $2.75 million when in fact the tokens held by the pool were worth approximately $172.8 million at then-prevailing market prices. The "gift" also caused the Indexed Finance AMM to overvalue SUSHI relative to the other tokens in the pool.

64. After creating artificial prices and distorting the re-indexing process, the defendant ANDEAN MEDJEDOVIC drained the DEFI5 Pool through a series of swaps using overvalued SUSHI tokens at artificial prices, ultimately obtaining approximately $12.5 million in digital tokens from the DEFI5 Pool, representing approximately 93% of the assets in the pool and rendering the liquidity providers' DEFI5 tokens effectively worthless.

65. The defendant ANDEAN MEDJEDOVIC used substantially similar steps to exploit the CC10 liquidity pool, obtaining approximately $4 million in digital tokens from the CC10 pool, representing approximately 98% of the assets in the pool and rendering the liquidity providers' CC10 tokens effectively worthless.

VI. Additional Relevant Conduct and Communications

66. Following the Indexed Finance exploit and before the KyberSwap exploit, the defendant ANDEAN MEDJEDOVIC discussed the criminal nature of his conduct in private messages on various electronic communication services.

67. For instance, in or about October 2021, shortly after the Indexed Finance exploit, the defendant ANDEAN MEDJEDOVIC messaged another user, "I did something very cool but accidentally doxxed myself in the process. I may be on the run forever now . . . Need some advice about becoming a pirate."

68. In another example from October 2022, approximately one year after the Indexed Finance exploit, the defendant ANDEAN MEDJEDOVIC discussed his conduct with a journalist. MEDJEDOVIC told the journalist that "between this and my political projects. I was gonna 'commit a crime' someday lol, just a question of how severe and when." He went on to say, "if your after real power in the world, eventually you will have to clash with nationstates [sic] at some level." After the journalist pushed back on MEDJEDOVIC's claims, he replied, "I mean, luckily my first time is small, no one cares about some kid dude give me some time lol a few more years is all I need." The journalist responded, "Some time to grow something real or steal more money?" MEDJEDOVIC replied, "both."

69. Following the KyberSwap exploit, MEDJEDOVIC co-mingled the proceeds of the two exploits. On or about November 23, 2023, MEDJEDOVIC transferred approximately 1,000 wETH with an estimated market value of approximately $2.06 million to a digital assets wallet that also received approximately $7.26 million in digital tokens obtained in the Indexed Finance exploit.

VII. Money Laundering

70. Beginning in or about 2022, the defendant ANDEAN MEDJEDOVIC undertook a scheme to launder the proceeds of his illegal conduct through digital asset exchange accounts using false account opening information and through a crypto-mixer (the "Mixer"), an entity the identity of which is known to the Grand Jury, to disguise the audit trail and conceal the

source of the proceeds of his illicit scheme. MEDJEDOVIC documented his plans and methods to launder the criminal proceeds in a file titled, "moneyMovementSystem." Among other things, the "moneyMovementSystem" file contained a step-by-step "operating procedure when moving large amounts through [the Mixer]" and instructions that would allow co-conspirators to access the stolen funds. MEDJEDOVIC also maintained files containing keys that could be used to redeem deposits from the Mixer, as well as files with instructions on using false identities to launder the criminal proceeds by circumventing "know your customer" ("KYC") procedures used by banks and cryptocurrency exchanges. In one such file, MEDJEDOVIC wrote, "Make a new bank account under fake ID (Signum is good)," "Order a thinkpad for storing crypto + hacks," and, "In general, a fake id, fake person with consistent name and bank account (crypto CC idealy), looks like me, order documents online (russian + brazil + american citizen) . . . fake kyc'd accounts for hacks and cashing out."

A. The Defendant and Co-Conspirator 1 Agree to Launder Proceeds of the Exploits

71. The defendant ANDEAN MEDJEDOVIC conspired with Co-Conspirator-1 to launder the proceeds of the KyberSwap and Indexed Finance exploits.

72. For example, in or about December 2022 and September 2023, following the Indexed Finance exploit, Co-Conspirator-1 helped the defendant ANDEAN MEDJEDOVIC open accounts at centralized digital assets exchanges. MEDJEDOVIC also sent Co-Conspirator-1 digital assets funded with tokens from the Mixer to conceal the criminal source of the funds. Between August 2023 and December 2024, MEDJEDOVIC sent Co-Conspirator-1 approximately $155,000 in digital assets in six transactions, each funded from the Mixer.

73. The defendant ANDEAN MEDJEDOVIC and Co-Conspirator-1 discussed the criminal source of MEDJEDOVIC's digital assets and used encrypted messaging applications

to evade detection by law enforcement. For example, on or about November 3, 2022, MEDJEDOVIC wrote to Co-Conspirator-1, "download [an encryption-enabled messaging application] when you can" and provided his user handle. Co-Conspirator-1 asked, "you usually use [the application]?" MEDJEDOVIC responded, "just for more secret stuff lolol." Several days later, on or about November 11, 2022, MEDJEDOVIC wrote to Co-Conspirator-1 "You here, I have a mission[.] Will give you the briefing on [the encrypted application.] Check [the encrypted application], mission details are there[.]" On or about November 15, 2022, Co-Conspirator-1 wrote to MEDJEDOVIC on a different electronic communication service, "Yeahyeahyeah, but the thing is ur money is all ready kind of dirty, which is epic for you because like you can't be hunted for twice y'know, but I'd like to still remain, you know emancipated to an extent[.] I'd like to be legit[.]"

B. Laundering the Proceeds of the KyberSwap Exploit and the Undercover Operation

74. Following the KyberSwap exploit, the defendant ANDEAN MEDJEDOVIC consolidated the proceeds from the exploit by transferring the stolen digital tokens from five Layer 2 blockchains onto the Ethereum network so that he could launder the funds through the Mixer. MEDJEDOVIC attempted to use several Layer 2 bridges to move approximately $42 million in fraudulently obtained crypto assets to the Ethereum blockchain. However, because the funds could be traced to the KyberSwap exploit, several of the bridges attempted to block MEDJEDOVIC's transactions. MEDJEDOVIC messaged support channels for those bridges seeking help in moving the transactions forward. For example, on or about January 21, 2024, MEDJEDOVIC messaged the support channel for a bridge protocol, "I'm willing to offer $50k in order to get my $100k unfrozen . . . If not, I have no other options but to alert [] authorities." The protocol support service replied, "You want to alert the authorities .. that

you hacked kyber and stole users funds..??" MEDJEDOVIC replied, "Yes, I am willing to alert the authorities. Committing a crime against someone who may or may not be a criminal is still a crime."

75. On or about December 1, 2023 and December 2, 2023, the defendant ANDEAN MEDJEDOVIC transferred approximately 2,000 ETH and wETH, with an estimated market value of approximately $8.3 million, through a bridge developed by the Bridge Protocol Developer, an entity the identity of which is known to the Grand Jury, from various Layer 2 protocols to the Ethereum blockchain. These transactions initially were delayed and prompted MEDJEDOVIC to reach out to the Bridge Protocol Developer for help. MEDJEDOVIC inquired whether the transactions had been blacklisted because "I have links to a controversial wallet." MEDJEDOVIC identified his transactions as "funded by the kyberswap incident." Eventually, these transactions were completed.

76. On or about December 6, 2023 and December 24, 2023, the defendant ANDEAN MEDJEDOVIC initiated two more transfers on the Bridge Protocol Developer bridge to move an additional 200 ETH from the Layer 2 protocols Arbitrum and Optimism to the Ethereum blockchain. These transactions were not completed because, at the time, the Bridge Protocol Developer had manually blacklisted the KyberSwap exploit digital asset addresses before these two transactions were executed. MEDJEDOVIC again contacted the Bridge Protocol Developer support for assistance and offered a bounty of $40,000 to anyone who could help him complete the transactions.

77. Thereafter, the defendant ANDEAN MEDJEDOVIC was introduced to an individual who, unbeknownst to him, was an undercover law enforcement employee ("UC-1"), to assist him in laundering proceeds of the KyberSwap exploit by moving the proceeds to the

Ethereum blockchain. UC-1 agreed to assist MEDJEDOVIC in moving the proceeds in exchange for a $100,000 "bounty." In connection with the relay completion, UC-1 advised MEDJEDOVIC of his presence in Brooklyn, New York, and UC-1 in fact communicated with MEDJEDOVIC through messages sent from the Eastern District of New York.

78. Between on or about February 21, 2024 and on or about February 23, 2024, as requested by the defendant ANDEAN MEDJEDOVIC, UC-1 circumvented the blacklist and successfully completed the relay transactions which included multiple transactions through the Eastern District of New York. MEDJEDOVIC paid UC-1 approximately 1.7 BTC worth approximately $86,559 at then-prevailing market prices in exchange for UC-1's assistance laundering the stolen funds.

COUNT ONE
(Wire Fraud)

79. The allegations contained in paragraphs one through 78 are realleged and incorporated as if fully set forth in this paragraph.

80. On or about November 22, 2023, within the Southern District of Ohio, the District of Oregon and elsewhere and out of the jurisdiction of any particular State or district, the defendant ANDEAN MEDJEDOVIC, together with others, did knowingly and intentionally devise a scheme and artifice to defraud KyberSwap and its liquidity providers, and to obtain money and property from them by means of one or more materially false and fraudulent pretenses, representations and promises, and, for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted writings, signs, signals, pictures and sounds by means of wire communication in interstate and foreign commerce, to wit: the smart contracts,

commands and swaps related to the KyberSwap exploit on the Ethereum network and the Arbitrum network.

(Title 18, United States Code, Sections 1343, 2, 3238 and 3551 et seq.)

COUNT TWO
(Unauthorized Damage to a Protected Computer)

81. The allegations contained in paragraphs one through 78 are realleged and incorporated as if fully set forth in this paragraph.

82. On or about November 22, 2023, within the Eastern District of New York and elsewhere and out of the jurisdiction of any particular State or district, the defendant ANDEAN MEDJEDOVIC, together with others, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage without authorization to one or more protected computers, including the Ethereum Virtual Machine (EVM), which was implemented through, among other nodes, a full Ethereum node running in the Eastern District of New York, and cause loss to one or more persons during a one-year period affecting protected computers aggregating at least $5,000 in value, to wit: the loss of approximately $28.2 million worth of digital assets MEDJEDOVIC obtained from the KyberSwap Elastic liquidity pools on the Ethereum network and the Arbitrum network.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), 2, 3238 and 3551 et seq.)

COUNT THREE
(Attempted Hobbs Act Extortion)

83. The allegations contained in paragraphs one through 78 are realleged and incorporated as if fully set forth in this paragraph.

84. In or about November 2023, within the Eastern District of Virginia and elsewhere and out of the jurisdiction of any particular State or district, the defendant ANDEAN MEDJEDOVIC, together with others, did knowingly and intentionally attempt to obstruct, delay and affect commerce, and the movement of articles and commodities in commerce, by extortion, in that MEDJEDOVIC attempted to obtain property, to wit: control of KyberSwap, ownership of the KyberDAO, and digital tokens, with the consent of the KyberSwap developers, the KyberDAO multisig wallet members, the members of the KyberDAO and the KyberSwap Elastic liquidity providers, which consent was to be induced by wrongful use of actual and threatened force, violence and fear, including fear of economic loss.

(Title 18, United States Code, Section 1951(a), 2, 3238 and 3551 et seq.)

COUNT FOUR
(Money Laundering Conspiracy)

85. The allegations contained in paragraphs one through 78 are realleged and incorporated as if fully set forth in this paragraph.

86. In or about and between October 2021 and the present, both dates being approximate and inclusive, within the District of Massachusetts and elsewhere and out of the jurisdiction of any particular State or district, the defendant ANDEAN MEDJEDOVIC, together with others, did knowingly and intentionally conspire to conduct one or more financial transactions in and affecting interstate and foreign commerce, which transactions in fact involved the proceeds of one or more specified unlawful activities, to wit: (i) wire fraud, in violation of Title 18, United States Code, Section 1343, (ii) unauthorized damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (iii) securities fraud, in violation of Title 15, United States Code, Section 78j(b), knowing that the property involved in such financial transactions represented the proceeds of some form of unlawful activity, and

knowing that such transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Sections 1956(h), 3238 and 3551 et seq.)

COUNT FIVE
(Money Laundering)

87. The allegations contained in paragraphs one through 78 are realleged and incorporated as if fully set forth in this paragraph.

88. In or about and between December 2023 and February 2024, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere and out of the jurisdiction of any particular State or district, the defendant ANDEAN MEDJEDOVIC, together with others, did knowingly and intentionally conduct and attempt to conduct one or more financial transactions in and affecting interstate and foreign commerce, which transactions in fact involved the proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and unauthorized damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), knowing that the property involved in such financial transactions represented the proceeds of some form of unlawful activity, and knowing that such transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity.

(Title 18, United States Code, Sections 1956(a)(1)(B)(i), 2, 3238 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT ONE

89. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count One, the government will seek forfeiture in

accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offense to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense.

90. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT TWO

91. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Two, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2) and 1030(i)(1), which require any person convicted of such offense to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, and such person's interest in

any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

92. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2), 982(b)(1), 1030(i)(1) and 1030(i)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT THREE

93. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Three, the government will seek forfeiture in accordance with: (a) Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which requires any person convicted of such offense to forfeit any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offense; and (b) Title 18, United States Code, Section 924(d)(1) and Title 28,

United States Code, 2461(c), which require the forfeiture of any firearm or ammunition involved in or used in any violation of any other criminal law of the United States.

94. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 924(d)(1) and 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS FOUR AND FIVE

95. The United States hereby gives notice to the defendant that, upon his conviction of any of the offenses charged in Counts Four and Five, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offenses to forfeit any property, real or personal, involved in such offenses, or any property traceable to such property.

96. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(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;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

Breon Peace

BREON PEACE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

John T. Lynch, Jr.

JOHN LYNCH
Chief, Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice

F. #2023R00907

FORM DBD-34
JUN. 85

No.

UNITED STATES DISTRICT COURT

EASTERN *District of* NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

ANDEAN MEDJEDOVIC,

Defendant.

INDICTMENT

(T. 18, §§ 924 (d)(1), 981(a)(1)(C), 982(a)(1), 982(a)(2), 982(b)(1), 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(i)(1), 1030(i)(2), 1343, 1951(a), 1956(a)(1)(B)(i), 1956(h), 3238, 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C. § 2461(c))

A true bill.

_____ *Foreperson*

Filed in open court this _____ *day,*

of _____ *A.D. 20* _____

_____ *Clerk*

Bail, $ _____

_____

Nick M. Axelrod and Andrew D. Reich, Assistant U.S. Attorneys
Tian Huang, Trial Attorney