UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	**SUPERSEDING INFORMATION**
v.	S1 23 Cr. 340 (VM)
SHAKEEB AHMED,	
Defendant.	

COUNT ONE
(Computer Fraud - Unauthorized Access to a Protected Computer to Further Intended Fraud)

The United States Attorney charges:

Overview

1.   In or about July 2022, SHAKEEB AHMED, the defendant, a United States citizen who was residing in Manhattan, New York, orchestrated and executed a scheme to fraudulently obtain approximately $9 million worth of cryptocurrency (the "Attack") from a decentralized cryptocurrency exchange (the "Crypto Exchange"), including cryptocurrency deposited by the Crypto Exchange's users. AHMED conducted the Attack by exploiting a vulnerability in the Crypto Exchange and inserting fake pricing data to fraudulently generate millions of dollars' worth of inflated fees that AHMED did not in fact earn, but which AHMED was able to withdraw from the Crypto Exchange in the form of cryptocurrency, thereby defrauding the Crypto Exchange and its users, whose cryptocurrency AHMED had fraudulently obtained. At the time of the Attack, AHMED was employed as a senior security engineer at a leading international technology company unrelated to the Crypto Exchange. His resume reflected skills in, among other things, reverse engineering smart contracts and blockchain audits, which are some of the specialized skills AHMED used to execute the Attack.

2.   After the Attack, SHAKEEB AHMED, the defendant, laundered the stolen cryptocurrency through a series of transactions designed to conceal the source and owner of the funds, including through: (a) conducting token-swap transactions; (b) "bridging" fraud proceeds from the Solana blockchain over to the Ethereum blockchain; (c) exchanging fraud proceeds into Monero, an anonymized and particularly difficult cryptocurrency to trace; and (d) using overseas cryptocurrency exchanges.

3.   After the Attack, SHAKEEB AHMED, the defendant, also searched online for information about, among other things, the Attack, his own criminal liability for the Attack, criminal defense attorneys with expertise in similar cases, law enforcement's ability to successfully investigate the Attack, and fleeing the United States to avoid criminal charges.

4.   After the Attack and once in possession of the stolen fees in cryptocurrency, SHAKEEB AHMED, the defendant, decided to return a substantial portion of the fraud proceeds to the Crypto Exchange, and to provide information to the Crypto Exchange about how AHMED accomplished the Attack, if the Crypto Exchange refrained from referring his fraudulent scheme to law enforcement. AHMED ultimately kept approximately $1.5 million worth of fraudulently obtained cryptocurrency.

Background on the Crypto Exchange

5.   The Crypto Exchange was incorporated overseas and operates on the Solana blockchain. At all relevant times, the Crypto Exchange was a decentralized exchange that allowed users to deposit and exchange different kinds of cryptocurrencies.

6.   A decentralized exchange does not rely on any sort of entity or company to act as an intermediary between buyers and sellers. Instead, it relies on "smart contracts" associated with "liquidity pools," analogous to pots of money, in order to serve as an "automated market maker."

2

A "smart contract" is a computer program that runs on a blockchain. An "automated market maker" controls a "liquidity pool" of different types of cryptocurrencies, and uses a smart contract to buy and sell the cryptocurrencies in that liquidity pool.

7. More specifically, the Crypto Exchange was a concentrated liquidity market maker, meaning that it allowed individuals or entities depositing cryptocurrency into its liquidity pools—referred to as "liquidity providers"—to set the price ranges—referred to as "ticks"—at which the individuals' cryptocurrency in the liquidity pool would be traded. For example, an individual who deposits 100 Ether into the concentrated liquidity market maker's liquidity pool can control the range at which the 100 Ether is offered for liquidity, so the individual might, for example, provide the 100 Ether subject to the limitation that it only be traded when the price is between .9 and 1.1 Bitcoin. In this example, the liquidity provider would profit by receiving a percentage of the transaction fees generated if the specified price range was triggered. In this example, .9 Bitcoin would be the lower tick, and 1.1 Bitcoin would be the upper tick.

8. At all relevant times, the Crypto Exchange paid fees to liquidity providers who deposited cryptocurrency into a liquidity pool. Those fees were calculated by a smart contract that took into account, among other things, the total amount of cryptocurrency the liquidity provider deposited and the actual amount of liquidity that was provided based on the price ranges selected by the liquidity provider. In essence, the greater the amount of cryptocurrency and liquidity provided, the higher the fee the liquidity provider could earn. More broadly, larger cryptocurrency deposits on the Crypto Exchange limit price volatility and increase liquidity.

9. One of the inputs into the smart contract that calculated those fees was referred to as a "tick account." The tick accounts were owned and controlled by the Crypto Exchange—in other words, the blockchain showed that the owner of the tick accounts was the Crypto Exchange,

3

and not any user or other third party. The tick accounts contained data about, among other things, how much liquidity all liquidity providers had provided for a particular price range, or tick. Users could not create or own tick accounts.

10.   Another input into the smart contract that calculated the fees was referred to as a "position account." Position accounts kept track of a user's share in a liquidity pool. In contrast to a tick account, which users could not create, the Crypto Exchange was set up to allow any user to create a "position account."

11.   Position accounts and tick accounts contained different types of data, but the general format of the two accounts was similar. As structured by the Crypto Exchange, both tick accounts and position accounts were listed as owned by the Crypto Exchange on the blockchain, even though position accounts could be created by a user. SHAKEEB AHMED, the defendant, exploited this vulnerability during the Attack, as described further below.

The Attack on the Crypto Exchange

12.   To carry out the Attack, SHAKEEB AHMED, the defendant, among other things: (a) the day before the Attack, conducted a series of test transactions of nominal value with the Crypto Exchange to obtain tick data and locate system vulnerabilities; (b) created at least two accounts that were *not* tick accounts; (c) supplied one of these non-tick accounts with fake price-tick data; and (d) carefully structured and designed these non-tick accounts to nonetheless falsely appear as authentic tick accounts. In other words, AHMED used at least two non-tick accounts that he intentionally created and designed to masquerade as tick accounts (the "Fake Tick Accounts") to fraudulently cause the Crypto Exchange's smart contract to accept them as legitimate tick accounts. As described below, AHMED used one such Fake Tick Account (the "First Fake Tick Account") to generate millions of dollars of inflated fees based on the fake price-

4

tick data he supplied, and the other Fake Tick Account (the "Second Fake Tick Account") to withdraw millions of dollars' worth of cryptocurrency.

13. On or about July 2, 2022, SHAKEEB AHMED, the defendant, created the First Fake Tick Account and fraudulently caused the Crypto Exchange's smart contract to accept it as authentic. AHMED entered fake price-tick data into the First Fake Tick Account in order to fraudulently cause the Crypto Exchange's smart contract to calculate that AHMED had provided more liquidity to the pool than he had actually contributed, which generated large fees for Ahmed that he had not legitimately earned. In other words, the Crypto Exchange's users legitimately earn fees based on how much cryptocurrency they provide to the liquidity pool in relation to pool-wide data. By entering fake price-tick data into the First Fake Tick Account, AHMED used fake data to make it falsely appear to the Crypto Exchange that AHMED had provided more liquidity to the pool than he actually had, and thus, AHMED was able to fraudulently generate fees for himself to which he was not entitled. In so doing, AHMED defrauded both the Crypto Exchange and its users.

14. To further the Attack, SHAKEEB AHMED, the defendant, took out a series of cryptocurrency "flash loans" worth tens of millions of dollars from a cryptocurrency lending platform (the "Crypto Lender"). A "flash loan" is an uncollateralized cryptocurrency loan without borrowing limits that is taken out and repaid in a single transaction, and can be used in situations where an individual sees an opportunity to immediately profit on the blockchain.

15. Over a period of several hours on or about July 2, 2022 and July 3, 2022, SHAKEEB AHMED, the defendant, deposited the funds from the flash loans into the Crypto Exchange's liquidity pools, withdrew the funds, claimed a falsely inflated percentage of the flash loans as fees from the Crypto Exchange through his deceptive use of the First Fake Tick Account,

and then repaid the flash loans to the Crypto Lender. In total, as part of the Attack, AHMED took out at least 21 flash loans from the Crypto Lender and used to them to generate falsely inflated fees from five separate liquidity pools controlled by the Crypto Exchange.

16. As part of the Attack, SHAKEEB AHMED, the defendant, also needed to withdraw the flash loan money that he had deposited into the liquidity pool—the principal—and return it to the Crypto Lender. In order to process a withdrawal of the principal, the Crypto Exchange's smart contract required a tick account that was listed as owned by the Crypto Exchange on the blockchain, and that contained data matching the tick data from the fee-claiming process. To satisfy this requirement, AHMED created the Second Fake Tick Account, a position account—listed as owned by the Crypto Exchange—and manipulated its data to closely resemble a tick account. Specifically, AHMED made a series of cryptocurrency deposits in specific amounts and in a specific order, in order to manipulate the data in the Second Fake Tick Account so that it contained data that matched certain of the data in the First Fake Tick Account. By doing this, AHMED was able to fraudulently cause the Crypto Exchange's smart contract to treat AHMED's position account—the Second Fake Tick Account—as a legitimate tick account. AHMED then used the Second Fake Tick Account to withdraw the principal he owed and returned it to the Crypto Lender.

17. An example of how SHAKEEB AHMED, the defendant, used the Fake Tick Accounts and one of the flash loans to defraud the Crypto Exchange is described below. Because each flash loan must be taken out and repaid as part of a single transaction on the blockchain, each of the following events together occurred as a single transaction conducted by AHMED:

6

a. On or about July 2, 2022, AHMED took out a flash loan from the Crypto Lender of approximately 840,000 PAI (Parrot) ("PAI"). PAI is a digital stablecoin worth approximately one dollar.

b. AHMED deposited the approximately 840,000 PAI into a liquidity pool ("Pool-1") controlled by the Crypto Exchange that covered exchanges between PAI and a second cryptocurrency: USDC (USD Coin) ("USDC"). Like PAI, USDC is a digital stablecoin worth approximately one dollar.

c. AHMED used the First Fake Tick Account, which contained fake price-tick data supplied by AHMED, to claim inflated fees of approximately 1,133.93 PAI and 120.14 USDC.

d. AHMED then used the Second Fake Tick Account to withdraw his principal of 840,000 PAI.

e. AHMED repeated the cycle four more times with the same flash loan. Each time, he redeposited the 840,000 PAI into Pool-1, claimed inflated fees of approximately 1,133.93 PAI and 120.14 USDC through his use of the First Fake Tick Account, and withdrew his principal of 840,000 PAI through his use of the Second Fake Tick Account.

f. After five cycles, AHMED returned the principal of 840,000 PAI to the Crypto Lender, plus a small fee to the Crypto Lender, and kept falsely inflated fees from the Crypto Exchange totaling approximately 5,669.65 PAI and 600.7 USDC.

18. SHAKEEB AHMED, the defendant, based on approximate U.S. dollar conversions of the cryptocurrency valuations at the time, ultimately claimed approximately $9 million in cryptocurrency as falsely inflated fees from 21 flash loans based on the falsified data in the First and Second Fake Tick Accounts. The chart below shows the fees AHMED claimed from the 21

flash loans, as well as the dates and times of the flash loans, the Crypto Exchange pools AHMED

exploited, and the amount of cryptocurrency AHMED borrowed:

Date/Time (UTC)	Crypto Exchange Pool	Amount Borrowed	Fees Extracted
07/02/2022 20:08:52	PAI/USDC	840,000 PAI	5,669.65 PAI 600.70 USDC
07/02/2022 21:57:55	USDT/USDC	5,500,000 USDT	2,228,250.55 USDT 424,501.75 USDC
07/02/2022 21:59:12	USDT/USDC	5,500,000 USDT	2,234,934.9 USDT 425,775.20 USDC
07/02/2022 22:06:26	USDH/USDC	400,000 USDH	303,414.00 USDH 34,041.90 USDC
07/02/2022 22:06:57	USDH/USDC	400,000 USDH	304,323.50 USDH 34,143.95 USDC
07/02/2022 22:07:23	USDH/USDC	400,000 USDH	304,323.50 USDH 34,143.95 USDC
07/02/2022 22:10:14	mSOL/SOL	10,500 mSOL	19,451 mSOL 14,525.55 SOL
07/02/2022 22:11:18	stSOL/SOL	57,000 stSOL	20,787.95 stSOL 19,631.50 SOL
07/02/2022 22:25:26	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:26:18	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:27:18	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:28:10	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:29:01	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:30:21	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:31:09	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:32:42	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:34:09	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:36:15	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC
07/02/2022 22:37:24	PAI/USDC	840,000 PAI	5,686.65 PAI 602.50 USDC

07/03/2022 0:26:08	stSOL/SOL	3,000 stSOL	1,094.10 stSOL 1,033.20 SOL
07/03/2022 0:32:40	stSOL/SOL	520 mSOL	963.25 mSOL 1,007.1 SOL

The example described in paragraph 17 is shown in the first row of this chart. Like PAI and USDC, USDT (Tether) and USDH (Hubble) are also digital stablecoins worth approximately one dollar. As used in the chart, Solana (SOL) is a cryptocurrency and Marinade staked SOL (mSOL) and Lido staked SOL (stSOL) are liquid staking tokens that users receive upon staking SOL on the Marinade and Lido protocols.

19.   After the Attack, the Crypto Exchange initiated a plan to compensate the users AHMED had victimized.

AHMED's Post-Attack Laundering of Stolen Fees

20.   After SHAKEEB AHMED, the defendant, fraudulently obtained inflated cryptocurrency fees in the Attack, he laundered the fraud proceeds through a series of transactions in order to conceal the nature, location, source, and his control of the stolen funds. AHMED engaged in the following laundering transactions, among others:

a.   In or about July 2022, after the Attack, AHMED conducted dozens of transactions exchanging one cryptocurrency token for another.

b.   In or about July 2022, after the Attack, AHMED "bridged" fraud proceeds across one blockchain over to another. A bridge contract is a mechanism to transfer cryptocurrency from one blockchain to another.

c.   In or about July 2022, after the Attack, AHMED laundered fraud proceeds through a swap aggregator to other wallets on the Solana blockchain. Swap aggregators aggregate

liquidity from across different decentralized exchanges to work out more favorable crypto prices for decentralized exchange traders.

      d.   On or about November 5, 2022, AHMED exchanged fraud proceeds into the cryptocurrency Monero, an anonymized and particularly difficult cryptocurrency to trace.

      e.   In or about May 2023, AHMED laundered fraud proceeds through overseas cryptocurrency exchanges.

Post-Attack Communications With the Crypto Exchange

21.   On or about July 3, 2022, almost immediately after the Attack, the Crypto Exchange initiated public communications on the blockchain with the unidentified "hacker" of the Crypto Exchange (in actuality, SHAKEEB AHMED, the defendant) in order to seek the return of the stolen funds. In these public statements on the blockchain, the Crypto Exchange indicated, among other things, that it would refer the Attack to law enforcement if the stolen funds were not returned and offered to pay the then-unidentified hacker $800,000 for the return of all the stolen funds.

22.   On or about July 6, 2022, a few days after the Attack, SHAKEEB AHMED, the defendant, using an encrypted email service based overseas, contacted the Crypto Exchange and stated that he would return a portion of the stolen funds if the Crypto Exchange agreed not to refer the Attack to law enforcement for investigation. At the time, AHMED was in possession of approximately $9 million in stolen funds. Specifically, AHMED told the Crypto Exchange that it was in a "tough spot" and stated that he would keep approximately $2.5 million of stolen cryptocurrency, noting that he would return of the remainder of the stolen funds to the Crypto Exchange on the condition that it not refer his conduct to law enforcement.

23.   In response, also on or about July 6, 2022, the Crypto Exchange restated its original figure of $800,000, noting that it was "starting to apply for legal support and in that case it wouldn't take long to find you" and "[o]therwise, you may face prosecution and likely lose everything."

24.   On or about July 7, 2022, SHAKEEB AHMED, the defendant, indicated that he intended to keep $1.8 million of the stolen cryptocurrency and stated, for the first time, that he would provide, in substance and in part, details on two purported vulnerabilities in the Crypto Exchange's platform and how to improve the Crypto Exchange's code. In doing so, AHMED told the Crypto Exchange that its post-Attack predicament was a "nightmare scenario." Later that same day, AHMED returned all but approximately $1.5 million of the fraudulently obtained cryptocurrency to the Crypto Exchange. The next day, on or about July 8, 2022, AHMED provided information about the Crypto Exchange's technical vulnerabilities.

AHMED's Post-Attack Internet History

25.   On or about July 5, 2022, just two days after the Attack and before he had communicated with the Crypto Exchange, SHAKEEB AHMED, the defendant, visited or searched for information about the Attack itself on the internet. For example:

a.   AHMED searched for the term "defi hack."

b.   AHMED visited a news article with the title, "[Crypto Exchange] Vulnerability Causes DeFi Clients to Lose Millions."

c.   AHMED visited a news article with the title, "Why Expensive Crypto Hacks Are The Cost of Doing Business in DeFi."

d.   AHMED also visited several pages on the Crypto Exchange's website.

26.   On or about July 5, 2022, still before he had communicated with the Crypto Exchange, SHAKEEB AHMED, the defendant, visited a news article describing a $10 million bounty that a cryptocurrency bridging platform had paid.

27.   On or about July 5, 2022, again before he had communicated with the Crypto Exchange, SHAKEEB AHMED, the defendant, visited or searched for information about white-collar criminal defense attorneys with expertise in cryptocurrency.

28.   SHAKEEB AHMED, the defendant, used a particular virtual private network ("VPN-1") to conceal his Internet Protocol address while he executed the Attack. On or about July 27, 2022, and continuing into August 2022, AHMED visited or searched for information in an attempt to confirm that VPN-1 could not be traced back to him.

29.   From approximately July 2022 through approximately December 2022, SHAKEEB AHMED, the defendant, visited or searched for information about whether he was likely to be prosecuted for the Attack. In particular:

a.   On or about July 5, 2022, still before he had communicated with the Crypto Exchange, AHMED searched for the term "embezzled."

b.   On or about August 6, 2022, AHMED searched for the term "defi hacks fbi."

c.   On or about August 8, 2022, AHMED searched for the term "defi hacks prosecution."

d.   On or about August 16, 2022, AHMED searched for "wire fraud," which is one of the charges in this Indictment.

e.   On or about August 16, 2022, AHMED searched for the term "how to prove malicious intent."

f.   On or about August 20, 2022, AHMED searched for the term "evidence laundering."

30.   From approximately August 2022 through approximately December 2022, SHAKEEB AHMED, the defendant, visited or searched for information about his ability to flee the United States, avoid extradition, and keep his stolen cryptocurrency. For example:

a.   On or about August 22, 2022, AHMED searched for the term, "can I cross border with crypto."

b.   On or about September 7, 2022, AHMED searched for the terms, "how to stop federal government from seizing assets" and "how to stop fed govt from seizing assets."

c.   On or about October 27, 2022, AHMED searched for the term, "buying citizenship" and visited related websites including: "16 Countries Where Your Investments Can Buy Citizenship . . . ."

STATUTORY ALLEGATION

31.   In or about July 2022, in the Southern District of New York and elsewhere, SHAKEEB AHMED, the defendant, knowingly and with the intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value totaling more than $5,000 during a one-year period, to wit, AHMED committed the Attack on the Crypto Exchange by, among other means, fraudulently accessing and exploiting without authorization a smart contract operated by the Crypto Exchange in order to steal approximately $9 million worth of cryptocurrency.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), and 2.)

FORFEITURE ALLEGATION

32.   As a result of committing the offense alleged in Count One of this Information, SHAKEEB AHMED, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offense, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

Substitute Assets Provision

33.   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 person;

        (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 subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and

Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 and 982;
Title 21, United States Code, Sections 853; and
Title 28, United States Code, Section 2461.)
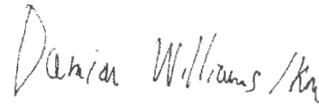
DAMIAN WILLIAMS
United States Attorney