UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

JONATHAN SPALLETTA,
a/k/a "Cthulhon,"
a/k/a "Jspalletta,"

Defendant.

[redacted] **INDICTMENT**

26 Cr. ___ ( )

26CRIM118

COUNT ONE
(Computer Fraud – Intentionally Damaging Protected Computers)

The Grand Jury charges:

Overview

1. In or about April 2021, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, a United States citizen residing in Maryland, orchestrated and executed a scheme to hack Uranium Finance ("Uranium"), a decentralized cryptocurrency exchange, on two occasions, thereby fraudulently obtaining cryptocurrency worth tens of millions of dollars. On the first occasion, on or about April 8, 2021, SPALLETTA fraudulently obtained approximately $1.4 million worth of cryptocurrency from Uranium via his hack, of which he ultimately returned all but approximately $386,000 (the "First Attack"). On the second occasion, on or about April 28, 2021, SPALLETTA fraudulently obtained approximately $53 million worth of cryptocurrency from Uranium via his hack, and kept it all (the "Second Attack," and together with the First Attack, the "Attacks"). SPALLETTA subsequently laundered many of those funds, including through the use of the cryptocurrency mixer Tornado Cash. SPALLETTA ultimately spent many of the fraudulently obtained funds on collectible items for himself, such as trading cards for the games

Magic: the Gathering and Pokémon, antique Roman coins, and a piece of the Wright brothers' original airplane that Neil Armstrong had taken to the moon.

Uranium and the Attacks

2. At all relevant times, Uranium was a decentralized exchange that allowed users to deposit and exchange different kinds of cryptocurrencies. Uranium operated on a decentralized network of computers that were connected to the internet and used in and affected interstate commerce. Uranium had users in the United States, including in the Southern District of New York.

3. 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," in order to serve as an "automated market maker." 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. For the liquidity pool to function as an automated market maker, or currency exchange, it relies on individuals to deposit their cryptocurrency into a given liquidity pool.

4. At all relevant times, Uranium paid "rewards" to liquidity providers who deposited cryptocurrency into a liquidity pool.

5. On or about April 8, 2021, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, committed the First Attack against Uranium by engaging in a deceptive series of transactions with Uranium's smart contract that allowed SPALLETTA to withdraw far more "rewards" in cryptocurrency than he was authorized to withdraw. In particular, SPALLETTA deposited funds into liquidity pools and then used the "EmergencyWithdraw"

function to withdraw his funds without claiming the rewards to which he was entitled. Then, SPALLETTA took advantage of a vulnerability in Uranium's code that meant that one of the values used to track how much cryptocurrency a particular user held in a particular pool—called "AmountWithBonus"—remained positive even when a user had used "EmergencyWithdraw" to withdraw all his funds. To exploit the vulnerability, SPALLETTA used the regular "Withdraw" function to issue a command to Uranium to withdraw zero tokens of cryptocurrency for him (the "Zero Withdrawal"). Because the "AmountWithBonus" for SPALLETTA was incorrectly positive, SPALLETTA knowingly caused Uranium to erroneously send him a number of rewards tokens, despite the fact that SPALLETTA had nominally requested to withdraw zero tokens. Because the system was not designed to make a transaction like the Zero Withdrawal, Uranium's normal process by which it reduced a user's amount of rewards token in the pool by the amount he or she withdrew—a process that was designed to protect users—failed, leaving SPALLETTA, as he intended, with continued access to the same number of rewards tokens he had before the Zero Withdrawal. SPALLETTA could then repeat the fraudulent process over and over, draining the liquidity pool of nearly all rewards tokens.

6. In total, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, successfully extracted cryptocurrency worth approximately $1.4 million in the First Attack.[1] Approximately two weeks after he fraudulently obtained the funds, SPALLETTA told another individual in writing, "I did a crypto heist of $1.5MM a couple of weeks ago . . . There was a bug in a smart contract, and I exploited it . . . Crypto is all fake internet money anyway."

[1] Unless otherwise noted, the values of the cryptocurrency are as of the date that they were fraudulently obtained from Uranium.

7. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, then entered into extortionate negotiations with Uranium to return some portion of the fraudulently obtained funds if Uranium agreed to call the portion of the funds he fraudulently obtained a "bug bounty." A "bug bounty" is a payment offered to a person who identifies an error in a computer program or system. In many cases, bug bounties represent legitimate transactions. However, in some instances, malicious actors who have *already* stolen or fraudulently obtained funds or data or compromised a computer system extort a payment from the victim, and then attempt, after-the-fact, to characterize that extortion payment as a "bug bounty" in an effort to evade prosecution. SPALLETTA's extortion was one such example of a sham bug bounty designed to evade prosecution. SPALLETTA ultimately agreed to keep cryptocurrency worth approximately $386,000, as a sham "bug bounty," and to return the rest of the funds fraudulently obtained in the First Attack.

8. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, had the following exchange with Uranium in which he extorted Uranium into agreeing to call the portion of the fraudulently obtained funds he kept from the First Attack a "bug bounty":

Sender	**Message**
SPALLETTA	TX [transaction] confirmed
SPALLETTA	Sorry about the mess
Uranium Representative	Alright received
Uranium Representative	At least we could work [something] out
SPALLETTA	Get your code audited next time. Hire me if you want.
SPALLETTA	If it makes you feel any better, you won't even feel this loss in a few months after all the degens ape back in, and you're rolling money again.
SPALLETTA	DeFi [Decentralized Finance] shit always bounces back.
SPALLETTA	I'm going to consider the issue settled now, and I appreciate the bounty.

Uranium Representative	Yes, can call it settled

9. But approximately three weeks later, on or about April 28, 2021, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, committed the Second Attack, again fraudulently obtaining funds from Uranium. This time, SPALLETTA exploited an error in the Uranium smart contract that governed how much cryptocurrency he could withdraw in a liquidity pool on Uranium. In particular, SPALLETTA took advantage of a separate vulnerability in Uranium's code that checked to make sure transactions were permissible before allowing them to go through. In particular, Uranium's code incorrectly used the number 1,000 when it should have used the number 10,000, which allowed SPALLETTA to request far more in funds than he knew he was entitled to receive.

10. In one transaction, for example, a particular Uranium liquidity pool had approximately 69,000 tokens of a cryptocurrency called "U92" and approximately 2,232,000 tokens of a cryptocurrency called "BUSD" that was supposed to be a "stablecoin," whose value was approximately $1 per token. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, proposed a transaction to the liquidity pool in which he would deposit approximately 0.000000000000000001 tokens of U92 and approximately 0.000000000000000001 tokens of BUSD. In exchange for those extremely small—essentially zero—amounts, SPALLETTA requested to withdraw approximately 88% of the pool's U92 and approximately 90% of the pool's BUSD. At the time he proposed the transaction to the Uranium smart contract, SPALLETTA knew that he was not entitled to receive such large quantities of cryptocurrency in exchange for, effectively, nothing.

11. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, conducted similar transactions targeting 26 separate Uranium liquidity pools, ultimately

fraudulently obtaining approximately $53.3 million in cryptocurrency. That was the overwhelming majority of cryptocurrency that Uranium possessed, and, unable to function, Uranium shut down almost immediately after the Second Attack.

12. Several days before committing the Second Attack, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, created an encrypted file titled "uranium_bug.txt" in which he described the error in the smart contract that he used to commit the Second Attack.

Laundering of Fraudulently Obtained Funds

13. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, took a number of steps to conceal that he was the individual who committed the Attacks by laundering the funds he fraudulently obtained.

14. One way JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, laundered the funds was by moving them through multiple blockchains, including the Bitcoin blockchain. Nodes in the Bitcoin blockchain store and update the Bitcoin blockchain's current state and recorded updates to the blockchain, including wallet balances. As of in or about April 2021 until the present, there was a Bitcoin blockchain node located in the Southern District of New York.

15. Another way JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, laundered the funds was through his use of the cryptocurrency mixer Tornado Cash. Ordinarily, when cryptocurrencies are transferred, they are transferred on a publicly visible blockchain, and those transactions can therefore be tracked. When a cryptocurrency wallet sends cryptocurrency to a cryptocurrency mixer such as Tornado Cash, however, the cryptocurrency is "mixed" with other cryptocurrency sent from other wallets, and the sender can then withdraw

cryptocurrency from the mixer to a new receiving wallet. The effect of that mixing is that the link between the sender wallet and the receiver wallet is obscured, making it more difficult for law enforcement to determine from where the receiver wallet received the funds. Because cryptocurrency mixers like Tornado Cash effectively obscure the source, origin, and destination of cryptocurrency, they are frequently used by criminals to launder funds.

16. As to the First Attack, on or about April 10, 2021, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, transferred cryptocurrency worth approximately $386,000 fraudulently obtained in the First Attack to Tornado Cash for the purpose of laundering the fraudulently obtained funds.

17. As to the Second Attack, between in about April 2021 and November 2023, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, transferred cryptocurrency worth approximately $26 million fraudulently obtained in the Second Attack to Tornado Cash for the purpose of laundering the fraudulently obtained funds.

18. JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, also sought to launder funds by using a multitude of different cryptocurrency wallets and by using intermediaries to make purchases with the fraudulently obtained funds on his behalf.

Use of Funds Fraudulently Obtained in the Attacks

19. After laundering the funds, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, used the money fraudulently obtained in the Attacks to purchase millions of dollars in personal collectable items, including but not limited to (i) rare cards for the trading card game Magic: The Gathering ("Magic Cards"); (ii) rare cards for the trading card game Pokémon (the "Pokémon Cards"); and (iii) antique Roman coins (the "Antique Coins"), among other items.

20. In particular, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, used the fraudulently obtained funds to purchase: (i) a "Black Lotus" Magic Card for approximately $500,000; (ii) 18 packs of sealed "Alpha Booster" Magic Cards for approximately $1,512,500; (iii) one sealed box of first edition "Booster" Pokémon Cards for approximately $257,500; (iv) one first edition complete base set of Pokémon Cards for approximately $750,000; (v) a piece of fabric from the original Wright brothers' airplane that was subsequently transported to the surface of the moon by astronaut Neil Armstrong on the first moon landing, for approximately $137,500; (vi) one "Eid Mar Denarius," an Antique Coin commemorating the assassination of Julius Caesar, for approximately $601,545.

21. A photo of the $500,000 "Black Lotus" Magic Card that was seized pursuant ot a judicially-authorized search warrant from the residence of JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, is below:

22. A photo of the $137,500 piece of fabric from the original Wright brothers' airplane that was subsequently transported to the surface of the moon by astronaut Neil Armstrong on the first moon landing and that was seized pursuant to a judicially-authorized search warrant from the residence of JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, is below:

23. A photo of one of the boxes of Antique Coins seized pursuant to a judicially-authorized search warrant from the residence of JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, is below:

24. On or about February 24, 2025, law enforcement seized pursuant to a judicially-authorized seizure warrant cryptocurrency worth approximately $31 million at the time of seizure that JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, had fraudulently obtained in the Attacks.

STATUTORY ALLEGATION

25. In or about April 2021, in the Southern District of New York and elsewhere, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, which caused loss to one and more persons during a one-year period aggregating at least $5,000 in value, to wit, SPALLETTA transmitted commands to Uranium via the Binance Smart Chain blockchain that fraudulently caused Uranium to send him nearly $55 million to which he was not entitled.

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

COUNT TWO
(Money Laundering)

The Grand Jury further charges:

26. The allegations contained in paragraphs 1 through 24 of this Indictment are repeated and realleged as if fully set forth herein.

27. From at least in or about April 2021 through in or about July 2023, in the Southern District of New York and elsewhere, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, knowing that the property involved in a financial transaction represented the proceeds of some form of unlawful activity, conducted and attempted to conduct such a financial transaction, which transaction affected interstate and foreign commerce and involved the use of a financial institution which was engaged in, and the activities of which affected, interstate and foreign commerce, and which in fact involved the proceeds of specified unlawful activity, to wit, (i) the computer fraud offense charged in Count One, (ii) the Attacks, which also constituted wire fraud in violation of Title 18, United States Code, Section 1343, and (iii) the extortion committed after the First Attack, knowing that the transaction was designed in

whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity.

(Title 18, United States Code, Section 1956(a)(1)(B)(i) and 2.)

FORFEITURE ALLEGATIONS

28. As a result of committing the computer fraud offense alleged in Count One of this Indictment, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," 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 and the following specific property:

a. Cryptocurrency formerly contained in cryptocurrency wallet address 0x59d779bed4db1e734d3fda3172d45bc3063ecd69 that was seized on or about February 24, 2025 and consists of approximately 1,261.4 ETH, 521,447.26 USDC, 57,043 USDT, 2,125.46 WETH, 6.8 BNB, 22,174.67 WBNB, and 0.01 USDT;

b. Cryptocurrency formerly contained in cryptocurrency wallet address 0xc47bdd0a852a88a019385ea3ff57cf8de79f019d that was seized on or about February 24, 2025 and consists of approximately .628 BNB and .969 ETH;

c. Cryptocurrency formerly contained in cryptocurrency wallet address 0xc61429117038A1f13881DD7410B80771F28e06ec that was seized on or about February 24, 2025 and consists of approximately 19.26 ETH;

d. Cryptocurrency formerly contained in cryptocurrency wallet address

bc1q3a3kmk7kwy8xartpltz2496e0z6kspgwl4w8t3 that was seized on or about February 24, 2025 and consists of approximately 80 BTC;

e. One "Black Lotus" Magic Card;

f. One piece of fabric from the original Wright brothers' airplane that was subsequently transported to the surface of the moon by astronaut Neil Armstrong on the first moon landing;

g. 18 sealed packs of "Alpha Booster" Magic Cards;

h. One sealed box of first edition "Booster" Pokémon Cards;

i. One first edition complete base set of Pokémon Cards; and

j. One "Eid Mar Denarius," an antique coin commemorating the assassination of Julius Caesar.

29. As a result of committing the money laundering offense alleged in Count Two of this Indictment, JONATHAN SPALLETTA, a/k/a "Cthulhon," a/k/a "Jspalletta," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any and all property, real and personal, involved in said offense, or any property traceable to such property, including but not limited to a sum of money in United States currency representing the amount of property involved in said offense, as well as the specific property described in the above paragraph.

Substitute Assets Provision

30. 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, Section 981 and 982;
Title 21, United States Code, Sections 853; and
Title 28, United States Code, Section 2461.)

[redacted]

FOREPERSON

Jay Clayton

JAY CLAYTON
United States Attorney