Approved: _____
DANIELLE M. KUDLA
Assistant United States Attorney

Before: THE HONORABLE ROBERT W. LEHRBURGER
United States Magistrate Judge
Southern District of New York

22 mag 2478

UNITED STATES OF AMERICA - v. - ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," Defendants.	**SEALED COMPLAINT** Violations of 18 U.S.C. §§ 1349, and 1956(h) COUNTY OF OFFENSE: MANHATTAN

SOUTHERN DISTRICT OF NEW YORK, ss.:

MARCO DIAS, being duly sworn, deposes and says that he is a Special Agent with the Office of Internal Revenue Service, Criminal Investigation Division ("IRS-CI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Wire Fraud)

1. From at least in or about September 2021, up to and including at least in or about March 2022, in the Southern District of New York and elsewhere, ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and others known and unknown, willfully and knowingly combined,

conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

2. It was a part and object of the conspiracy that ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, and sounds for the purpose of executing such scheme and artifice to defraud, in violation of Title 18, United States Code, Section 1343, to wit, NGUYEN and LLACUNA used the Internet to advertise and sell approximately $1.1 million in non-fungible tokens ("NFT"), which included representations that the purchaser would receive certain benefits, including giveaways and access to a metaverse game, when in reality there were no such benefits.

(Title 18, United States Code, Section 1349.)

COUNT TWO
(Conspiracy to Commit Money Laundering)

3. From at least in or about September 2021, up to and including at least in or about March 2022, in the Southern District of New York and elsewhere, ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and others known and unknown, intentionally and knowingly combined, conspired, confederated, and agreed together and with each other to violate Title 18, United States Code, Section 1956(a)(1)(A)(i).

4. It was a part and an object of the conspiracy that ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions, to wit, cryptocurrency transactions, represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, wire fraud, with the intent to promote the carrying on of the specified

unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i).

(Title 18, United States Code, Section 1956(h).)

Overview

5. I am a Special Agent with IRS-CI, and I have been personally involved in the investigation of this matter. This Complaint is based upon my personal participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

6. Since in or about January 2022, IRS-CI and the Department of Homeland Security Investigations ("HSI") have been investigating a non-fungible token ("NFT") fraud scheme after purchasers of a particular NFT publicly reported that they had been defrauded in what is colloquially referred to as a "rug pull." As the term suggests, a "rug pull" refers to a scenario where the creator of a NFT and/or gaming project solicits investments and then abruptly abandons a project and fraudulently retains the project investors' funds. As detailed below, ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and others known and unknown, created an NFT project advertised under the name "Frosties," which sold NFTs in the form of various cartoon figures, often with an ice cream cone (a "Frostie"). According to the official Frosties website (the "Frosties Website"), Frosties purchasers would be eligible for holder rewards, such as, *inter alia*, giveaways, early access to a metaverse game, and exclusive mint passes to upcoming Frosties seasons. In reality, on January 9, 2022, NGUYEN and LLACUNA, whose legal identities were disguised to Frosties purchasers, abruptly abandoned the Frosties NFT project within hours after selling out of Frostie NFTs and transferring approximately $1.1 million in cryptocurrency to various cryptocurrency wallets under the control of NGYUGEN and LLACUNA, in multiple transactions designed to obfuscate the original source of funds. Currently, NGUYEN and LLACUNA are advertising a second

NFT project under the name "EmbersNFT," which, based upon similarities to the Frosties NFT project, is believed to be another fraud scheme expected to launch on or around March 26, 2022.

Cryptocurrency and NFTs

7. Based on my training and experience, and my conversations with other law enforcement officers, I have learned, among other things, the following regarding cryptocurrency as relevant to the instant offenses:

a. Cryptocurrency is a digital currency in which transactions are verified and records are maintained by a decentralized system using cryptography, rather than a centralized authority such as a bank or government. Like traditional fiat currency, there are multiple types of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, and Tether, among others. Due to its decentralized nature and limited regulation, cryptocurrency allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Although they are legal and have known legitimate uses, cryptocurrency is also known to be used by cybercriminals for money-laundering purposes.

b. Cryptocurrency owners typically store their cryptocurrency in digital "wallets," which are identified by unique electronic "addresses." By maintaining multiple cryptocurrency addresses, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track the flow of illegal proceeds by quickly transferring illicit proceeds in various amounts through multiple cryptocurrency addresses.

c. Each cryptocurrency transaction, however, regardless of the cryptocurrency denomination, is recorded on a public ledger commonly referred to as a "blockchain," which acts as an accounting ledger. The blockchain records, among other things, the date and time of each cryptocurrency transaction, the unique cryptocurrency addresses associated with the transaction and the sending and receiving parties, and the amount of cryptocurrency transferred, but does not identify the parties that control the cryptocurrency addresses involved in the transaction. Because each cryptocurrency address is unique, law enforcement can review the blockchain to identify relevant cryptocurrency transactions and trace the flow of cryptocurrency across various cryptocurrency addresses. This form of cryptocurrency tracing is labor intensive and can be complicated by the use of multiple cryptocurrency addresses, and through other commonly used

obfuscation techniques, including the use of "mixers," described later in greater detail.

8. Based on my training and experience, and my conversations with other law enforcement officers, I have learned, among other things, the following regarding NFTs as relevant to the instant offenses:

a. An NFT is a non-interchangeable unit of data stored on the blockchain that can be sold and traded. Most NFTs are part of the Ethereum blockchain, which is one of the largest open-source blockchains. Ether ("ETH") is the native cryptocurrency of the Ethereum blockchain.

b. There are different types of NFT data files that can be purchased. The most basic NFT data file is similar to a .jpeg image file that provides a purchaser with an electronic image and a certificate of ownership. By contrast, a "utility" NFT data file offers added benefits, such as reward programs, giveaways, and early access to events for NFT holders.

c. Each NFT is commonly referred to as a "token," which is uniquely identifiable on the blockchain.

d. The process of turning a digital file into an NFT (*i.e.* a crypto collectible or digital asset) on the Ethereum blockchain is typically referred to as "minting." The digital file is stored on the Ethereum blockchain, and typically cannot be edited, modified, or deleted.

e. The minting of a NFT requires the creation of a "smart contract," which is recorded on the blockchain and outlines the rules that will govern the sale of and any subsequent transfers of the NFTs after minting. NFT smart contracts are written in computer code and publicly viewable on the Ethereum blockchain.

f. OpenSea is the first and, currently, the largest NFT marketplace. OpenSea offers users the ability to mint NFTs directly on its platform or use a third-party platform for NFT minting. In the latter case, OpenSea is only used by OpenSea accountholders to trade and/or sell NFTs on the secondary market.

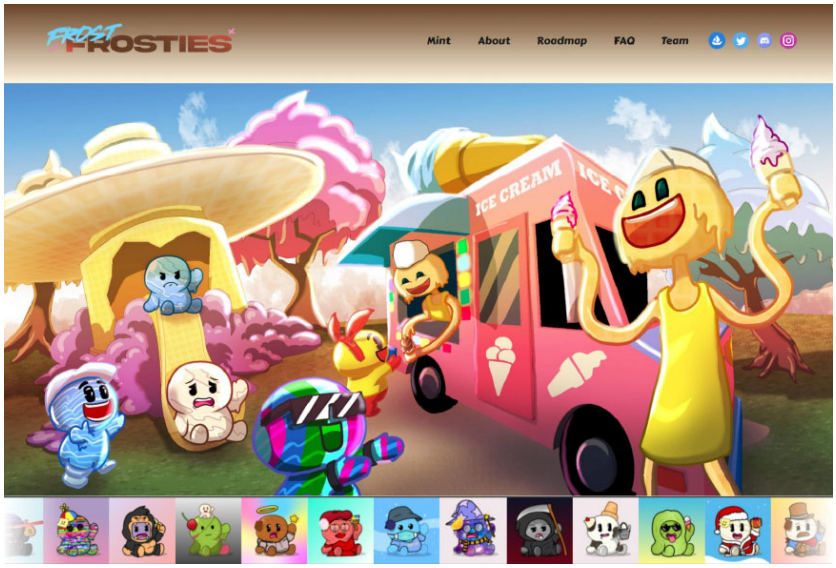
OpenSea generates revenue through fees associated with minting and trading NFTs on its platform.

The Frosties NFT Sale

9. Based on my participation in this investigation, my review of preserved internet screenshots retained and cataloged on a publicly available internet archival website, and my conversations with at least three Frosties NFT purchasers (the "Purchasers"),[1] I have learned, among other things, the following, in substance and in part:

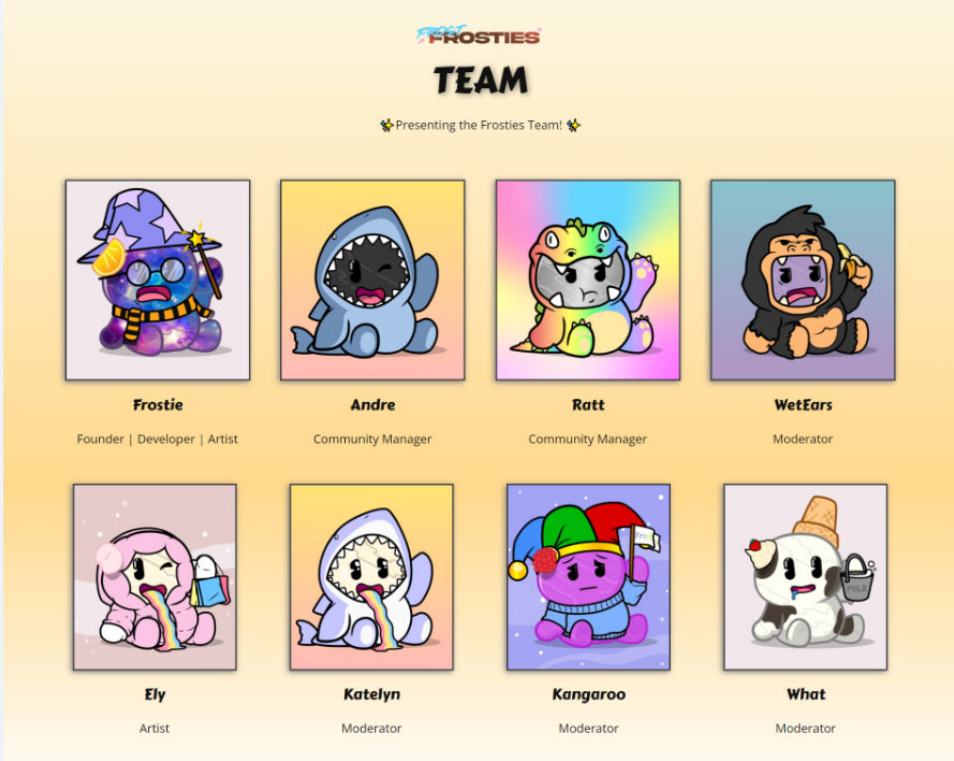
a. In or about December 2021, various social media communication platforms, including, among others, Twitter and Discord, began advertising the sale of a particular NFT termed a "Frostie." These platforms directed interested purchasers to a particular website (the "Frosties Website").

b. The Frosties Website advertised the sale of Frosties NFTs—electronic images of various cartoon figures often with an ice cream cone. The image below is a screenshot taken from the Frosties Website, which shows some of the various Frosties available for purchase:



[1] Based on a review of transactions on the blockchain, law enforcement believes that there were likely hundreds, if not thousands, of victims who purchased one or more Frosties NFTs. However, due to the covert nature of the investigation law enforcement has only been able to identify and interview a limited number of victims at this time.

c. The Frosties Website listed "Frostie" as the "founder, developer, and artist," "Andre" as the "Community Manager," and the entire "Frosties Team" as the following:



d. In addition to the sale of the digital NFT image, the Frosties Website advertised, in substance and in part, the following Frosties purchaser benefits (the "Frosties Benefits"):

i. "Staking," a "metaverse," and breeding functions. Based on my training and experience, I know that the terms "staking" refers to anticipated returns from a cryptocurrency investment; "metaverse" refers to a virtual-reality space in which users can interact with a computer-generated environment and other users; and "breeding functions" refers to the ability to create a new NFT token that resembles the image of two separate NFT tokens.

ii. Eligibility for holder rewards, such as giveaways, air drops, early access to a metaverse game, and exclusive mint passes to upcoming seasons.[2]

[2] Based on the Frosties Website, law enforcement believes that exclusive mint passes to upcoming seasons refers to presale access to future NFT projects.

iii. Development of the Frosties Benefits beginning "immediately" after the sale of all of the Frosties.

iv. The image below is a screenshot taken from the Frosties Website and shows the advertised the "launch" plan and "development" plan, which would be implemented immediately following the Frosties NFT sale. In particular, the "Launch Roadmap" advertised, among other things, that when 100% of the Frosties were sold the Frosties NFT project developers would "immediate[ly] start on [the] development [of the] roadmap, starting with staking, metaverse development, and marketing campaigns!"

e. At least two of the three Purchasers who visited the Frosties Website and purchased one or more Frosties did so based on, among other things, the advertised Frosties Benefits.[3]

f. Each Frostie was advertised to cost approximately 0.04 ETH, which at the time of the Frosties NFT sale, was equivalent to approximately $123 to $136. In total, the Frosties Website advertised 8,888 Frosties tokens for sale.

g. Between on or about January 7, 2022 and on or about January 9, 2022, the Frosties Website permitted individuals to purchase one or more Frosties tokens through either a private presale or a public sale. At or around the time of purchase/minting, the purchaser was provided with the unique smart contract address for the Frosties NFT project (the "Frosties Smart Contract"), which also served as the particular cryptocurrency wallet address to transfer the desired amount of Ether in exchange for the equivalent number of Frosties tokens ("Frosties Wallet Address-1").

h. Each minted Frosties token was publicly recorded on the Ethereum blockchain along with the Frosties Smart Contract.

10. Based on my participation in this investigation, my review of publicly-available information on the Ethereum blockchain, my review of social media posts, and my discussions with other law enforcement agents, I have learned, among other things, the following, in substance and in part:

a. The private presale took place between on or about January 7, 2022, through on or about January 8, 2022. On January 9, 2022, following the private presale, the Frosties public

[3] The third purchaser ("Purchaser-3") indicated that he/she did so as an investment opportunity based on the presale popularity of the NFT. In total, Purchaser-3 paid the Ether equivalent of approximately $750 for approximately three Frosties, which included associated service fees commonly referred to as "gas fees." After execution of the fraud, Purchaser-3 sold each Frostie for the Ether equivalent of approximately $6, after the market value of Frosties rapidly collapsed, as discussed later.

sale went live. Within approximately 48 minutes, by approximately 2:47 P.M. EST, all 8,888 Frosties tokens were sold out.

b. That same day, at approximately 5:45 P.M. EST, the proceeds of the Frosties NFT sale that had been transferred to Frosties Wallet Address-1 were then transferred to a separate cryptocurrency wallet address ("Fraud Wallet Address-1"). Because each cryptocurrency transaction is publicly recorded on the blockchain, certain Frosties purchasers observed the suspicious transfer of all the Frosties proceeds at or near real-time, which coincided with the deactivation of the Frosties Website and certain social media accounts that had been active promoting and discussing the Frosties NFT sale. Shortly after these events, there were several posts on social media sites, including Discord and Twitter, that there had been a "rug pull," meaning that the Frosties project creators had ended the NFT project prematurely and taken the purchasers' money.

c. Shortly after the announcement of the rug pull on social media platforms, several Frosties purchasers began selling their Frosties tokens at what appeared to be a steep discount, based on the apparent rug pull fraud.

11. Based on my participation in this investigation, my review of the Ethereum blockchain, including my review of the Frosties Smart Contract, and my discussions with other law enforcement officers, I have learned, among other things, the following, in substance and in part:

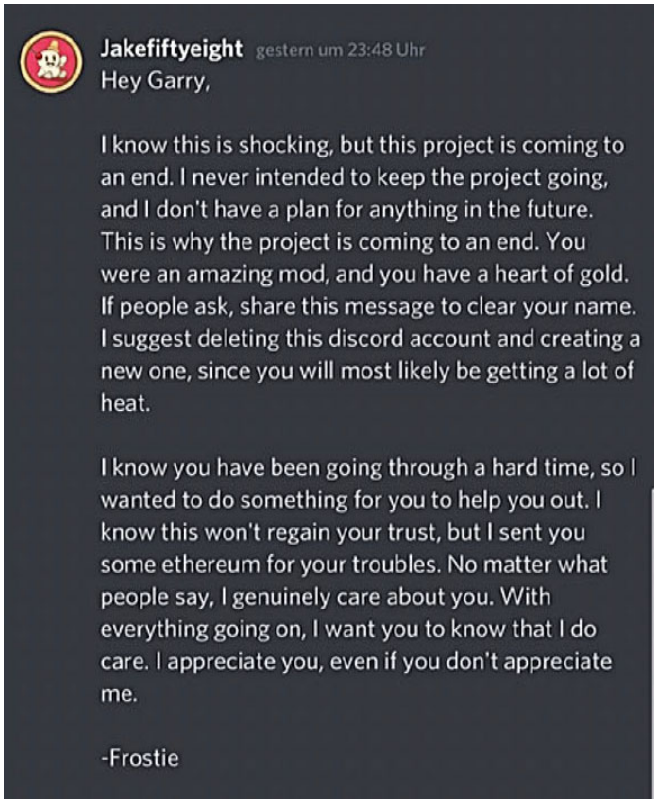
a. The Frosties Smart Contract computer code contained a conditional withdrawal function, which when executed by the smart contract owner, initiated the withdrawal and transfer of all funds in Frosties Wallet Address-1 to the wallet address of the owner of the Frosties Smart Contract, which was recorded on blockchain as Fraud Wallet Address-1.

b. In total, approximately 356.56 ETH, then valued at approximately $1.1 million, was transferred from Frosties Address-1 to Fraud Wallet Address-1.

12. Based on my participation in this investigation, my review of preserved internet screenshots retained and cataloged on a publicly-available internet archival website, and my conversations with the Purchasers, I have learned, among other things, the following, in substance and in part:

a. Shortly after the rug pull was announced on social media platforms, a screenshot of a Discord conversation

between username "Jakefiftyeight" and username "Garry_is_Back" was posted on Twitter. The screenshot, which is shown below, appears to show a private Discord message sent by "Jakefiftyeight" to "Garry_is_Back" on January 9, 2022, following the fraud, in which "Jakefiftyeight" stated, in substance and in part, the following:



b. After acknowledging that the Frosties NFT project was over within hours after the Frosties NFT sale and that the author of the message had no intentions of keeping the project going, "Jakefiftyeight" signed off as "Frostie" — the Frosties founder, developer, and artist.

The Identification of NGUYEN as "Frostie," LLACUNA as "heyandre," and the Laundering of the Frosties NFT Sale Proceeds

13. Based on my participation in this investigation, and my review of grand jury subpoena returns from Discord, Coinbase, Charter Communications, and my review law enforcement databases, I have learned, among other things, the following, in substance and in part:

a. Discord, one of the primary social media communication platforms that was used to promote and discuss the Frosties NFT sale and community discussions following the fraud,

captures account usernames and certain corresponding internet protocol ("IP") addresses.[4]

b. The individual who used the Discord username "Jakefiftyeight," as seen in the January 9, 2022 Discord message shown above, also used the following Discord usernames: "Jobo," "Frostie," "Meltfrost," and "Unc0vered Meltfrost." Specifically:

i. On or about October 17, 2021, Discord username "Jobo" conducted activity on Discord from a particular IP address (the "NGUYEN IP Address"). That same day, the NGUYEN IP Address was used to conduct transactions on a Coinbase account belonging to ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," the defendant. Based on my training and experience, I know that Coinbase is one of the largest cryptocurrency exchange platforms, which allows Coinbase accountholders to buy, store, and trade different cryptocurrencies and maintain cryptocurrency wallets.

ii. On or about December 17, 2021, Discord username "Frostie" conducted activity on Discord from the NGUYEN IP Address. That same day, within a few hours, the NGUYEN IP Address was used to conduct transactions on a Coinbase account belonging to NGUYEN.

c. The individual who used the Discord username "heyandre" while actively discussing the Frosties NFT sale listed a particular phone number ("LLACUNA Phone-1") and a particular email address ("LLACUNA Email-1") as part of "heyandre's" Discord account. LLACUNA Phone-1 and LLACUNA Email-1 are listed for a Coinbase account belonging to ANDRE LLACUNA.

i. LLACUNA's Coinbase account contained a required government-issued photograph identification, which was

[4] Based on my training and experience, I know that an IP address is a unique string of characters assigned by an internet service provider ("ISP") to Internet-connected devices for the purposes of communicating over a network. It is possible for two or more electronic devices to share an IP address if these devices access the internet from a local network ("LAN")—essentially, while users may be using different computers or devices in one location, if these devices are all using the same internet connection, they will share an IP address.

provided in the name of "Andre Marcus Quiddaoen Llacuna" residing at a particular address ("LLACUNA Home Address-1").

ii. Based on my review of law enforcement database records, I have learned that LLACUNA Home Address-1 is owned by a man and a woman who share the "Llacuna" surname (the "LLACUNA Home Address-1 Owners"). Based on the shared surname and my comparison of the dates of birth of the LLACUNA Home Address-1 Owners and LLACUNA, I believe that the LLACUNA Home Address-1 Owners are LLACUNA's parents or share some other familiar relationship with LLACUNA.

iii. Charter Communications is the ISP servicer for LLACUNA Home Address-1. The internet service for LLACUNA Home Address-1 is subscribed to in the name of the female LLACUNA Home Address-1 Owner. Since approximately October 2020, LLACUNA Home Address-1 has been assigned a particular static IP address (the "LLACUNA Home IP Address"). Based on my training and experience, I know that a static IP address refers to an IP address that does not change over time in contrast to a dynamic IP address, which changes frequently depending on factors such as location and service provider.

iv. Between on or about December 29, 2021 to on or about January 19, 2022, the LLACUNA Home IP Address was used more than 130 times to conduct activity on social media platforms, including Discord and Twitter, which were used to promote and discuss the Frosties NFT sale. On at least 13 occasions during this time period, the LLACUNA Home IP Address was used to log into the Twitter account named @FrostiesNFT. As described further below in paragraph 17(f)(i), the LLACUNA Home IP Address was also used to conduct transactions relating to a new NFT project linked to NGUYEN and LLACUNA.

d. Based on the matching IP address activity and the matching personal contact information outlined above, I believe that the individual who has utilized the following Discord usernames "Jakefiftyeight," "Jobo," "Frostie," "Meltfrost," and "Unc0vered Meltfrost," is NGUYEN, and the individual who has utilized the Discord username "heyandre," is LLACUNA.

14. Based on my participation in this investigation, my review of the Ethereum blockchain, including my review of the Frosties Smart Contract, my review of grand jury subpoena returns from Coinbase, and my discussions with other law enforcement

officers, I have learned, among other things, the following, in substance and in part:

a. On or about December 17, 2021, a Coinbase wallet owned by ETHAN NGUYEN sent approximately 0.024 ETH to Fraud Wallet Address-1. This was the first cryptocurrency transaction ever recorded on the blockchain involving Fraud Wallet Address-1. In the weeks that followed, the owner of Fraud Wallet Address-1 uploaded the Frosties Smart Contract to the blockchain and appears to have conducted various transactions without any financial value, but rather designed to test the operability of the Frosties Smart Contract computer code. Based on the fact that the very first cryptocurrency transaction to Fraud Wallet Address-1 was from a Coinbase wallet owned by NGUYEN, along with the many usernames linked to NGUYEN on various accounts that are also linked to the Frosties NFT project as outlined in this Complaint, I believe that NGUYEN owns and/or controls Fraud Wallet Address-1, which uploaded the Frosties Smart Contract that contained the withdrawal code to transfer all proceeds from Frosties Wallet Address-1 to Fraud Wallet Address-1.

15. Based on my participation in this investigation, my review of grand jury subpoena returns from GoDaddy, Citbank, T-Mobile, PayPal, and Coinbase, my physical surveillance of ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," the defendant, and my discussions with other law enforcement officers, I have learned, among other things, the following, in substance and in part:

a. On or about September 7, 2021, NGUYEN's Citibank credit card was used to make a purchase to Fiverr International ("Fiverr") in the amount of $1,424.25, which was processed through Manhattan, New York. Fiverr, which has offices located in Manhattan, New York, is an online marketplace for freelance services which, among other things, include assisting users to create websites and NFT artwork. This transaction included a purchase notation for designing a website and landing page.

b. Within approximately two days, on or about September 9, 2021, the Frosties Website domain name was registered with GoDaddy, a domain registrar and web hosting company. That same day, NGUYEN's Citibank credit card was used to make a purchase

to GoDaddy in the amount of $54.98.[5] I know that Citibank is located and headquartered in Manhattan, New York.

i. The Frosties Website domain name is subscribed to in the name of "Frosties NFT" with a particular phone number ("NGUYEN Phone-1") and a particular address ("NGUYEN Address-1").

ii. NGUYEN Phone-1's device details, which are associated with the phone and SIM number, are "Ethan N," which correspond to NGUYEN's initials.[6]

iii. NGUYEN Phone-1 is also listed on NGUYEN's Coinbase account, Citibank account, and PayPal account, which all include NGUYEN's full name.

iv. NGUYEN Phone-1 is also the recovery phone number for a particular email address, which includes the name "meltfrost" (the "Meltfrost Email"), which, apart from being thematically similar to the Frosties NFT project, is listed as an email account linked to NGUYEN's Coinbase account. The recovery email address for the Meltfrost Email is another email address, which includes a partial derivation of NGUYEN's full name ("NGUYEN Email-1").

v. NGUYEN's Citibank records include monthly check images beginning in or around August 2021 made payable to Simaco LLC and include a particular unit number notation. Based on my review of publicly-available records, Simaco LLC appears to be a property management company with a building under management located at NGUYEN Address-1.

vi. Between on or about March 1, 2022 and on or about March 3, 2022, law enforcement observed an individual who appeared to match NGUYEN's state-issued photograph identification enter and exit NGUYEN Address-1.

c. Based on the Frosties Website's domain registration subscriber information, which matches a transaction

[5] On or about December 17, 2021, NGUYEN's Citibank debit card was used to purchase approximately $400 in cryptocurrency from a Coinbase account belonging to NGUYEN. Within one hour, NGUYEN sent nearly an identical amount in cryptocurrency from the same Coinbase account to a particular recipient cryptocurrency address. The transaction notes labeled the payment as "Frosties."

[6] NGUYEN Phone-1 is subscribed to in the name of "John Mooc."

involving NGUYEN's Citibank credit card, and includes NGUYEN Phone-1 and NGUYEN Address-1, which match several records that include NGUYEN's full name, I believe that NGUYEN registered the Frosties Website, which was used to promote and sell the 8,888 Frosties tokens.

16. Based on my participation in this investigation, my review of grand jury subpoena returns from Citibank, Coinbase, Metamask, and OpenSea, my review of the Ethereum blockchain, and my discussions with other law enforcement officers, I have learned, among other things, the following regarding the transfer of the Frosties NFT sale proceeds:

a. On or about December 31, 2021, a Citibank credit card belonging to ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," the defendant, made a $9.99 purchase to Tunnel Bear. Based on my training and experience, I know that Tunnel Bear is a virtual private network ("VPN") service provider, which enables a user to send and receive data across a shared or public network as if the user's electronic device was directly connected to a private network. VPNs can be used individuals engaged in unlawful activity to obfuscate their true location (by concealing their true IP address) and avoid law enforcement detection. Based on my review of IP addresses recorded in connection with the Frosties NFT sale, I know that IP address ranges belonging to Tunnel Bear were used on various social media platforms and the Frosties Website to promote the Frosties NFT project.

b. In or about May 2021, an OpenSea account was created with the username "Joboethan," which is a combination of one of NGUYEN's Discord usernames, (*see* ¶ 13(b)), and NGUYEN's first name. The account profile photograph is a Frostie image and includes a particular Ethereum wallet address ("Ethereum Wallet-1"). Based on my review of blockchain records, Ethereum Wallet-1 and other Coinbase wallets owned by NGUYEN had transactions with another particular wallet address ("Intermediary Wallet Address-1") in or about August 2021 through in or about November 2021.

i. On or about January 15, 2022, and on or about January 16, 2022, approximately one week after the Frosties NFT rug pull fraud, Intermediary Wallet Address-1 sent cryptocurrency to Tornado Cash. Based on my training and experience, I know that Tornado Cash is an application designed to add a layer of privacy and anonymity on public blockchains such as Ethereum. Tornado Cash operates as a cryptocurrency transaction mixer, which scrambles the funds of multiple users together to anonymize the source. The Tornado Cash smart contract is specific

to Ether. Once Ether is deposited into the application, it is combined with other Ether deposits, and Ether tokens are thereafter scattered to different cryptocurrency addresses when withdrawn. This entire process is designed to ensure that any withdrawals from the Tornado Cash smart contract cannot be linked to the original depositing address.

c. On or about January 9, 2022, at approximately 5:45 p.m. EST, Fraud Wallet Address-1, which as outlined above is believed to be owned and/or controlled by NGUYEN, (*see* ¶ 14(a)), transferred approximately 358 ETH to another wallet address ("Fraud Wallet Address-2"). Based on law enforcement's review of the blockchain, this was also the first cryptocurrency transaction recorded involving Fraud Wallet Address-2.

i. On or about January 11, 2022, at approximately 12:16 a.m. EST, well after the Frosties NFT sale was publicly denounced as a fraud on social media platforms, Fraud Wallet Address-2 transferred approximately 210 ETH, then-valued at approximately $678,000 in three separate transactions in short succession to Tornado Cash. Two different IP addresses associated with a particular wallet were used to execute these three transactions ("IP Wallet Address-1" and "IP Wallet Address-2"). Both IP Wallet Address-1 and -2 were hosted by a VPN service, which as noted above, can be used by individuals engaging in unlawful activity to obfuscate their true location.

ii. That same day, between approximately 12:40 a.m. EST and 1:49 a.m. EST, IP Wallet Addresses-1 and -2 were used to (i) log into the Discord username account "heyandre," which as outlined above, (*see* ¶ 13(c)), is believed to belong to ANDRE LLACUNA, a/k/a "heyandre," the defendant, and (ii) IP Wallet Address-2 was used to purchase a Frostie with a wallet labeled "Cryptoandre.eth," which not only contains LLACUNA's first name, but is also linked to an OpenSea account for username "Cryptoandre" which is registered with an particular email address that contains LLACUNA's full name ("LLACUNA Email-2").

d. Between on or about January 15, 2022, and on or about February 15, 2022, the blockchain recorded a series of cryptocurrency transactions whereby ETH was sent from Tornado Cash to one or more unknown wallet addresses that ultimately deposited ETH into various Coinbase wallets owned by NGUYEN and LLACUNA. Specifically, law enforcement has observed the transfer of approximately 9.5 ETH into Coinbase wallets owned by NGUYEN, and approximately 12.16 ETH into Coinbase wallets owned by LLACUNA, which adhere to this pattern. Based on my training and experience, I have learned that this pattern of cryptocurrency transfers to

numerous intermediary wallets for various amounts is often designed as a means to obfuscate the source of illegal funds. For example, certain mainstream cryptocurrency exchanges, such as Coinbase, adhere to anti-money laundering, know your customer ("KYC") regulations. To avoid anti-money laundering scrutiny and law enforcement detection, individuals in possession of illicit proceeds often insert intermediary transactions between a KYC exchange like Coinbase and a high-risk source like Tornado Cash, a cryptocurrency mixer, to further obfuscate the source of funds.

e. Based on, among other things, (i) the purchase and use of VPN services, (ii) the timeline of the Frosties NFT sales proceeds transfer from Frosties Wallet-1 to Fraud Wallet Address-1 and -2, and then to Tornado Cash, (iii) the use of Tornado Cash, which is designed to further anonymize the source of cryptocurrency funds, and (iv) the receipt of multiple cryptocurrency transactions from Tornado Cash, I believe that NGUYEN and LLACUNA took deliberate steps to conceal their true identities and receipt of the Frosties NFT sales proceeds.[7]

Upcoming NGUYEN and LLACUNA NFT Project – "Embers NFT"

17. Based on my participation in this investigation, my review of grand jury subpoena returns from OpenSea, Coinbase, Bitpay, Fiverr, and PayPal, my review of publicly-available social media platforms, and my discussions with other law enforcement officers, I have learned, among other things, the following, in substance and in part:

a. On or about January 16, 2022, and January 17, 2022, ETHAN NGUYEN's a PayPal account belonging to ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," the defendant, made purchases to Fiverr, which, among other things, assists users to create NFT

[7] On or about January 9, 2022, Discord username "heyandre," who is believed to be LLACUNA, posted a message on social media platforms asserting in sum and substance that neither him nor another individual that was part of the Frosties team had any knowledge of the fraud scheme. That same day, Twitter account @FrostiesNFT also posted a message asserting, in sum and substance, that other members of the Frosties team did not have knowledge of the fraud scheme.

artwork. These transactions included purchase notations for "NFT crypto artwork."

b. A particular email address containing NGUYEN's first name ("NGUYEN Email-2") is linked to OpenSea accounts with the username "Joboethan," "Rarebunniftw," and "EmbersNFT." Based on my training and experience, I believe an email address is linked to an OpenSea account when it is either entered by the accountholder as part of the registration process and/or is used to access a particular account.

i. Prior to on or about March 10, 2022, the "EmbersNFT" OpenSea account included a hyperlink to a Twitter page that advertised the "EmbersNFT" project. Although the "EmbersNFT" OpenSea account no longer appears to contain the hyperlink, the Twitter page continues to advertise the "EmbersNFT" project and references a particular website as of on or about March 12, 2022 (the "Embers Website").

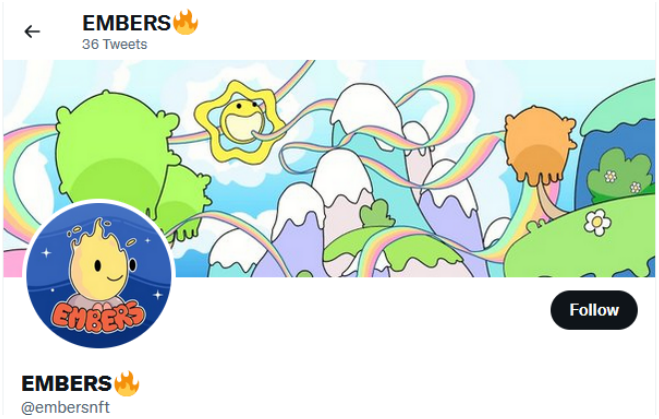
c. The Embers NFT project is currently advertised on various social media platforms, including Twitter and Discord, as the upcoming sale of approximately 5,555 "embers" NFTs for approximately 0.10 ETH each, which is approximately $267.

i. Based on ETH's present-day value, if all 5,555 Ember tokens are sold, the Embers sale will generate approximately $1.5 million – similar to the amount of the Frosties NFT sale.

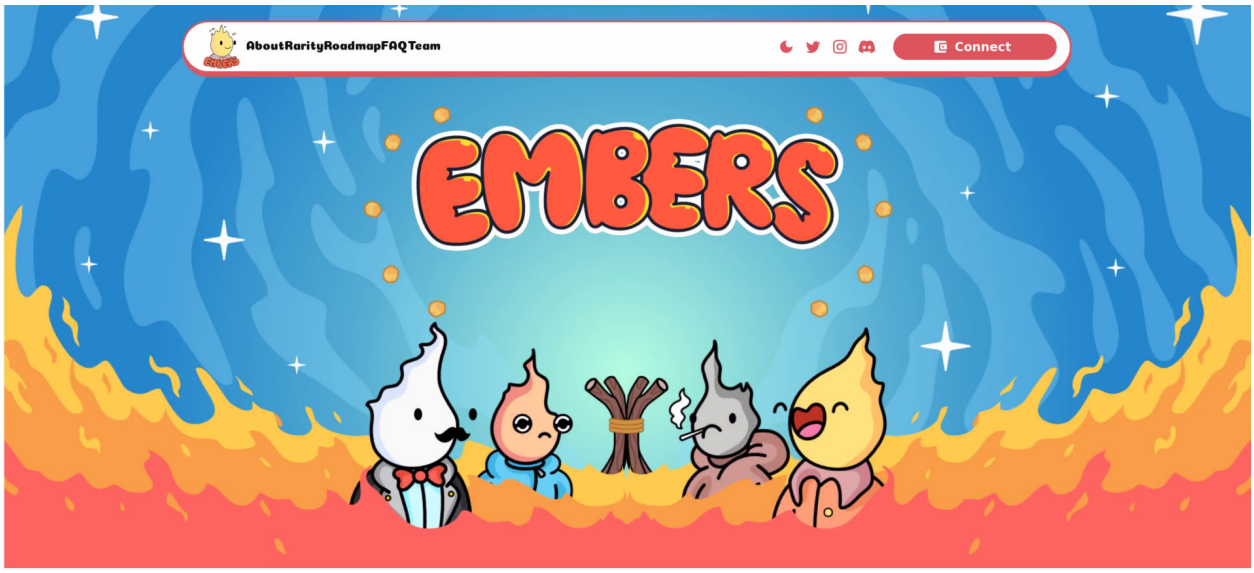
ii. A message on social media and the Ember Website lists the presale date as on or about March 26, 2022.

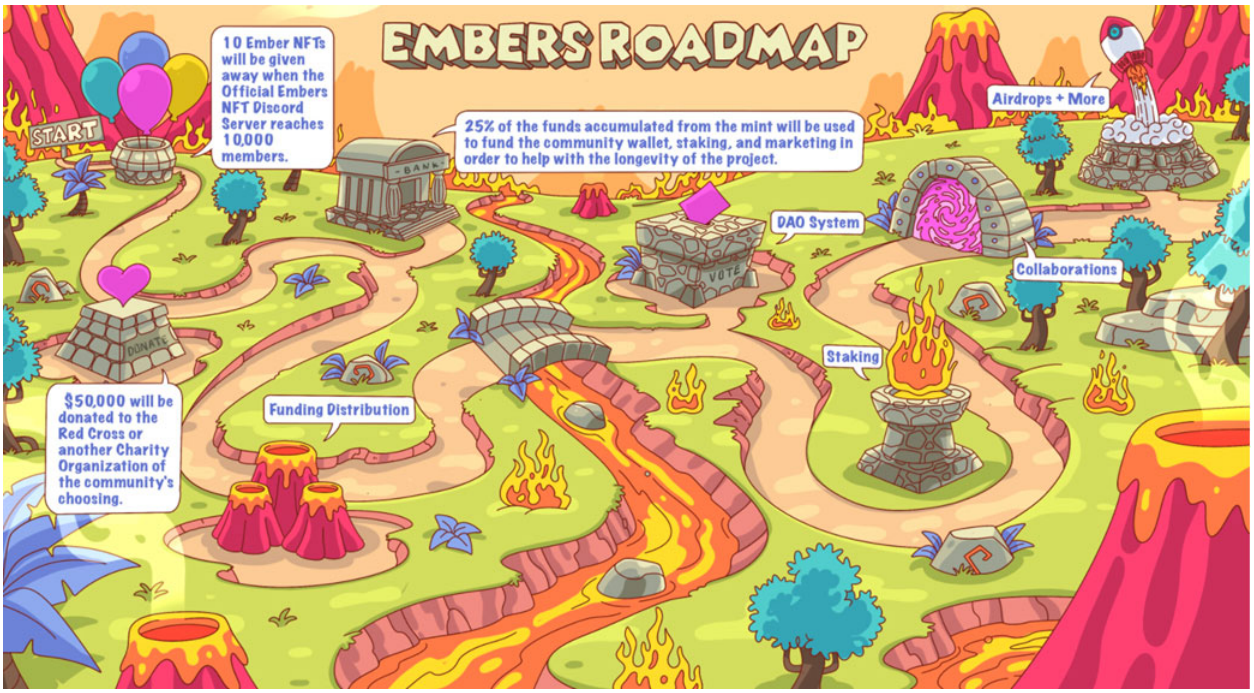
iii. Screenshots of the advertised Embers NFT and Embers Website are shown below:

Embers NFT



Embers Website





d. In particular, the Embers Website screenshot shown above advertises that the Embers NFT presale begins on March 26, 2022 at 7:00 p.m. UTC and the public sale begins on March 27, 2022 at 7:00 p.m. UTC. The Embers Website indicates that it will provide a "step-by-step" guide in the near future to describe how interested individuals can purchase an Embers NFT.

e. Similar to the previously advertised Frosties Benefits, the Embers Website promises Embers NFT purchasers the following NFT benefits, in substance and in part:

i. The Embers NFT project will donate $50,000 to the Red Cross Foundation;

ii. Free Embers NFT token giveaways;

iii. Airdrops;

iv. Staking opportunities;

v. Collaboration; and

vi. The promise that 25% of Embers NFT sales proceeds will be used to fund the community wallet, staking, and marketing to promote the longevity of the project.

f. On or about March 1, 2022, Discord username "Ogami," one of the Embers Website listed Embers NFT project developers, posted a screenshot of a letter from the Red Cross Foundation thanking "Embers NFT" for the donation of $50,000.

i. Based on law enforcement's review of grand jury subpoena returns from Bitpay, a cryptocurrency payment processor accepted by the Red Cross Foundation, I have learned, among other things, that between on or about February 21, 2022, and on or about February 28, 2022, the Red Cross Foundation received approximately $50,000 in cryptocurrency through six transactions processed through Bitpay. These transactions were all made from the LLACUNA Home IP Address, which as noted above in paragraph 13(c)(iv), was used to conduct activity on Discord and Twitter during the relevant time period.

g. Visitors to social media platforms advertising the Embers NFT project have asked if the creators, whose true legal identities are anonymous, will reveal their identities prior to the sale. To date the Embers NFT promotor(s) have indicated, in sum and substance, that they will continue to remain anonymous.

h. Based on the factors listed above, including (i) NGUYEN Email-2's link to the Embers NFT project, (ii) the similarities between the Embers NFT project advertisements and the Frosties NFT project advertisements, (iii) the Red Cross Foundation donation linked to LLACUNA and likely traced to the Frosties NFT fraud proceeds, and (iv) the intentional anonymity regarding the Embers NFT project creators, I believe that NGUYEN

and LLACUNA are preparing to execute a similar NFT rug pull fraud scheme in the near future.

WHEREFORE, deponent prays that a warrant be issued for the arrest of ETHAN NGUYEN, a/k/a "Frostie," a/k/a "Jakefiftyeight," a/k/a "Jobo," a/k/a "Joboethan," a/k/a "Meltfrost," and ANDRE LLACUNA, a/k/a "heyandre," the defendants, and that they be arrested and imprisoned, or bailed, as the case may be.

S/ by the Court with permission
MARCO DIAS
Special Agent
IRS-CI

Sworn to through the transmission of this Affidavit
by reliable electronic means, pursuant to Federal Rules
of Criminal Procedure 41(d)(3) and 4.1, this
15th day of March, 2022

THE HONORABLE ROBERT W. LEHRBURGER
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK