UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* rafa0george@gmail.com (Google Account ID 1033521631013), cryptoxiaomi@gmail.com (Google Account ID 1087185743577), edilsonbersai@gmail.com (Google Account ID 468512438816), and nhocboxmr@gmail.com (Google Account ID 788780590890) ("TARGET ACCOUNTS"), that is stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), at 1600 Amphitheater Parkway, Mountain View, CA 94043	)	Case No. 2:22-MJ-03119

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343, 1956	Wire Fraud; Money Laundering

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

ICE, HSI Special Agent Brandon Dreyer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Alexander F. MacKinnon, U.S. Magistrate Judge

Printed name and title

AUSA: Tian Huang

ATTACHMENT A

Property to Be Searched

This warrant applies to information which is associated with the Google, LLC account(s) identified by:

- rafa0george@gmail.com (Google Account ID 1033521631013)
- edilsonbersai@gmail.com (Google Account ID 468512438816)
- cryptoxiaomi@gmail.com (Google Account ID 1087185743577)
- nhocboxmr@gmail.com (Google Account ID 788780590890)

and which is stored at premises owned, maintained, controlled, or operated Google, LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Google, LLC ("PROVIDER") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier ("Account") listed in Attachment A:

a. For the time period of 09/08/2021 through present (for **cryptoxiaomi@gmail.com**), the time period of 07/02/2021 through present (for **edilsonbersai@gmail.com**), the time period of 01/01/2020 through present (for **rafa0george@gmail.com**), and the time period of 01/01/2020 through present (for **nhocboxmr@gmail.com**): The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, including Google Drive), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

b. For the time period of 09/08/2021 through present (for **cryptoxiaomi@gmail.com**), the time period of 07/02/2021 through present (for **edilsonbersai@gmail.com**), the time period of 01/01/2020 through present (for **rafa0george@gmail.com**) and the time period of 01/01/2020 through present (for **nhocboxmr@gmail.com**): The contents of all other data and related transactional records for all PROVIDER services used by an Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, including Google Drive), including any information generated, modified, or stored by user(s) or PROVIDER in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period of 09/08/2021 through present (for **cryptoxiaomi@gmail.com**), the time period of 07/02/2021 through present (for **edilsonbersai@gmail.com**), the time period of 01/01/2020 through present (for **rafa0george@gmail.com**) and the time period of 01/01/2020 (for **nhocboxmr@gmail.com**): All PROVIDER records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

d. For the time period of 09/08/2021 through present (for **cryptoxiaomi@gmail.com**), the time period of 07/02/2021 through present (for **edilsonbersai@gmail.com**), the time period of 01/01/2020 through present (for **rafa0george@gmail.com**) and the time period of 01/01/2020 (for **nhocboxmr@gmail.com**): All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents

and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

f. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities ("IMEI"), Mobile Equipment Identifiers ("MEID"), Global Unique Identifiers ("GUID"), Electronic Serial Numbers ("ESN"), Android Device IDs, phone numbers, Media Access Control ("MAC") addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s), including unique application numbers and push notification tokens associated with the Account (including Apple Push Notifications ("APN"), Google Cloud Messaging ("GCM"), Microsoft Push Notification Service ("MPNS"), Windows Push Notification Service ("WNS"), Amazon Device Messaging ("ADM"), Firebase Cloud Messaging ("FCM"), and Baidu Cloud Push);

g. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any PROVIDER account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

h. All information held by PROVIDER related to the location and location history of the user(s) of the Account, including geographic locations associated with the Account (including those collected for non-PROVIDER based applications), IP addresses, Global Positioning System ("GPS") information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers;

i. For the time period of 09/08/2021 through present (for **cryptoxiaomi@gmail.com**), the time period of 07/02/2021 through present (for **edilsonbersai@gmail.com**), the time period of 01/01/2020 through present (for **rafa0george@gmail.com**), and the time period of 01/01/2020 (for **nhocboxmr@gmail.com**): All records of communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken;

j. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel); and

Within 14 days of the issuance of this warrant, PROVIDER shall deliver the information set forth above via United States mail, courier, e-mail, or other electronic means to the following:

Brandon Dreyer
Special Agent
Homeland Security Investigations
40 S. Gay St.
Baltimore, MD 21202
Brandon.dreyer@ice.dhs.gov

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1956 (Money Laundering) as described in the affidavit submitted in support of this Warrant, including, for each Account, information pertaining to the following matters:

(a) Information that constitutes evidence of the identification or location of the user(s) of the Account;

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

(c) Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information that constitutes evidence concerning cryptocurrency transactions, transfers, investments, storage, or other financial arrangement involving cryptocurrency.

(f) Communications with any individual regarding cryptocurrency transactions, transfers, investments, storage, or other financial arrangement involving cryptocurrency.

(g) Information that constitutes evidence of transactions or laundering of funds representing the proceeds of any NFT rug pull scam, or funds intended to promote any NFT rug pull scam; and

(h) Information that constitutes evidence concerning any solicitation of funds from any individual.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATIONS

I, Brandon Dreyer, a Special Agent ("SA") with the United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is associated with four accounts—namely, rafa0george@gmail.com (Google Account ID 1033521631013), cryptoxiaomi@gmail.com (Google Account ID 1087185743577), edilsonbersai@gmail.com (Google Account ID 468512438816), and nhocboxmr@gmail.com (Google Account ID 788780590890) (hereafter "**TARGET ACCOUNTS"**), that is stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. The requested warrant would permit the search and seizure of information associated with the **TARGET ACCOUNTS**, which were utilized by various individuals in connection with a non-fungible token ("NFT") rug pull scheme involving individuals who solicited investments for NFTs but then abruptly abandoned the project and fraudulently retained the project

investors' funds.

3. I am a Special Agent with HSI and as such, am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations and make arrests for offense enumerated in Title 18, United States Code Section 2516.

4. I have been employed with HSI since November of 2010. I am currently assigned to HSI Baltimore's Transnational Cyber Crimes Team ("TCCT"), which conducts investigations into transnational criminal organizations that utilize the internet, darknet, and other technological means to violate the laws of the United States of America. Before arriving to HSI Baltimore, I was assigned to HSI Nogales, Arizona where I worked from April 2011 to March 2017 investigating transnational criminal organizations operating along our southwest border. Prior to being hired by HSI, I was employed by US Customs and Border Protection ("CBP") in Miami, Florida from July 2005 to November 2010. I graduated from the Criminal Investigator Training Program and the HSI Special Agent Training Program, both of which were conducted at the Federal Law Enforcement Training Center in Glynco, Georgia. I received specialized training involving gangs, narcotics, fraud, cybercrime, cryptocurrency, import and export violations, child pornography, immigration, and firearms offenses. I also received training regarding firearms, officer response tactics, surveillance techniques, and undercover operations.

5. I have been involved in the execution of approximately fifty-five (55) residential search warrants related to gangs, narcotics, child pornography, money laundering, cybercrime, and illegal exportation of weapons from the United States. I have also been the affiant on search warrants for cell phones, email accounts, vehicles, residences, and storage units. I also have Title III wiretap investigative experience involving narcotics distribution in Baltimore, MD and Title

III wiretap investigative experience involving organized retail crime groups located in Mexico and the United States. I also have multiple overseas deployments in furtherance of Homeland Security Investigations' mission to disrupt and dismantle transnational criminal organizations. Lastly, I have a Bachelor of Science Degree in Animal Sciences from Kansas State University, Manhattan, Kansas, in May 2004.

6. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant for the **TARGET ACCOUNTS**, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. However, I have not excluded any information known to me that would defeat a determination of probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

7. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1956 (Money Laundering) ("**TARGET OFFENSES**") have been committed by the users of the **TARGET ACCOUNTS** and other unidentified co-conspirators. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). In addition, the criminal offenses under investigation began or were committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. See 18 U.S.C. § 3238.

PROBABLE CAUSE

9. HSI Baltimore has an ongoing criminal investigation into potential violations of the wire fraud and money laundering statutes in connection with a scheme to defraud investors, as described in greater detail herein.

I. Background of Baller Ape Club

10. The Baller Ape Club ("BAC") was an NFT investment project that sold NFTs in the form of various cartoon figures, often with the figure of an ape (a "Baller Ape"). BAC conducted its business principally by means of a website accessible at https://www.ballerapeclub.com. The BAC website marketed the sale of Baller Ape NFTs, as well as advertised various benefits to investors of Baller Ape NFTs, such as:

a. Access to "an exclusive VIP Lounge where all fellow Primates gather to flex their Rolex, NFT's and sip on a banana cocktail," and where "benefits, offerings and rewards will increase over time."

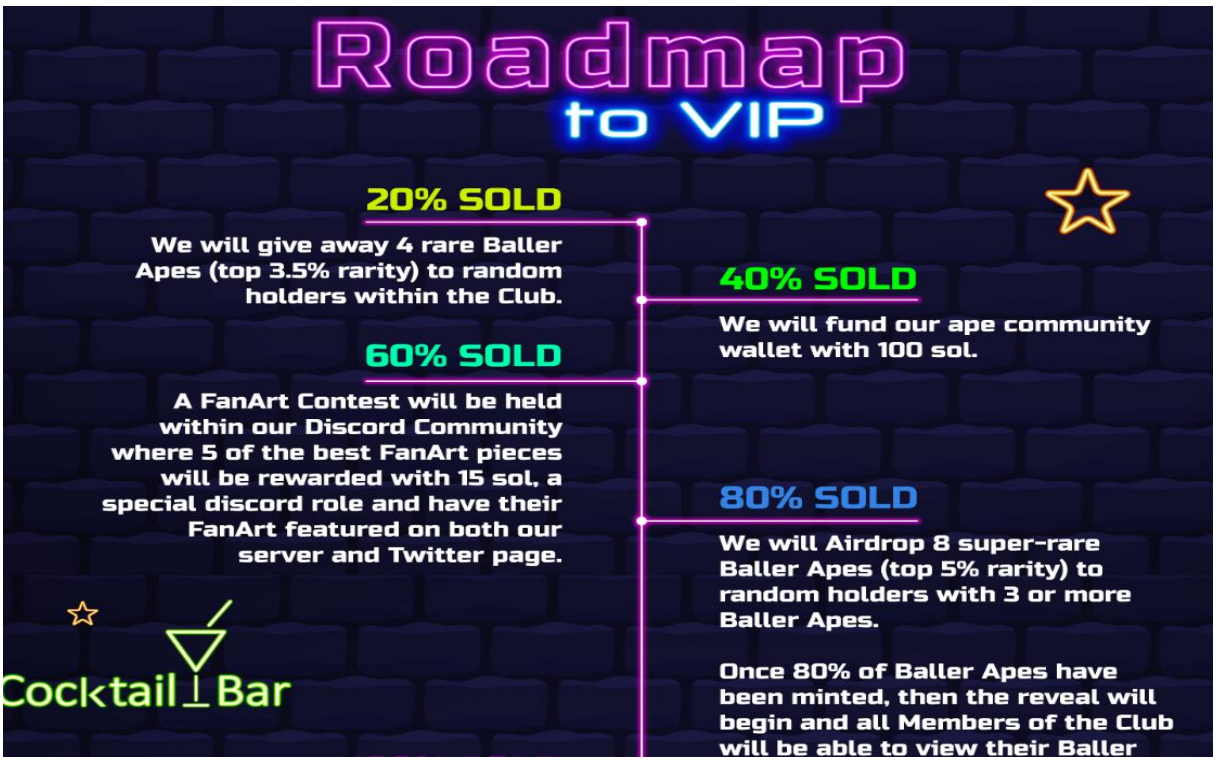
b. Donations to "a number of charity organizations, starting with 50 SOL[1] to a charity of the Club's choosing, [that] we will achieve . . . through community voting power on our Discord."

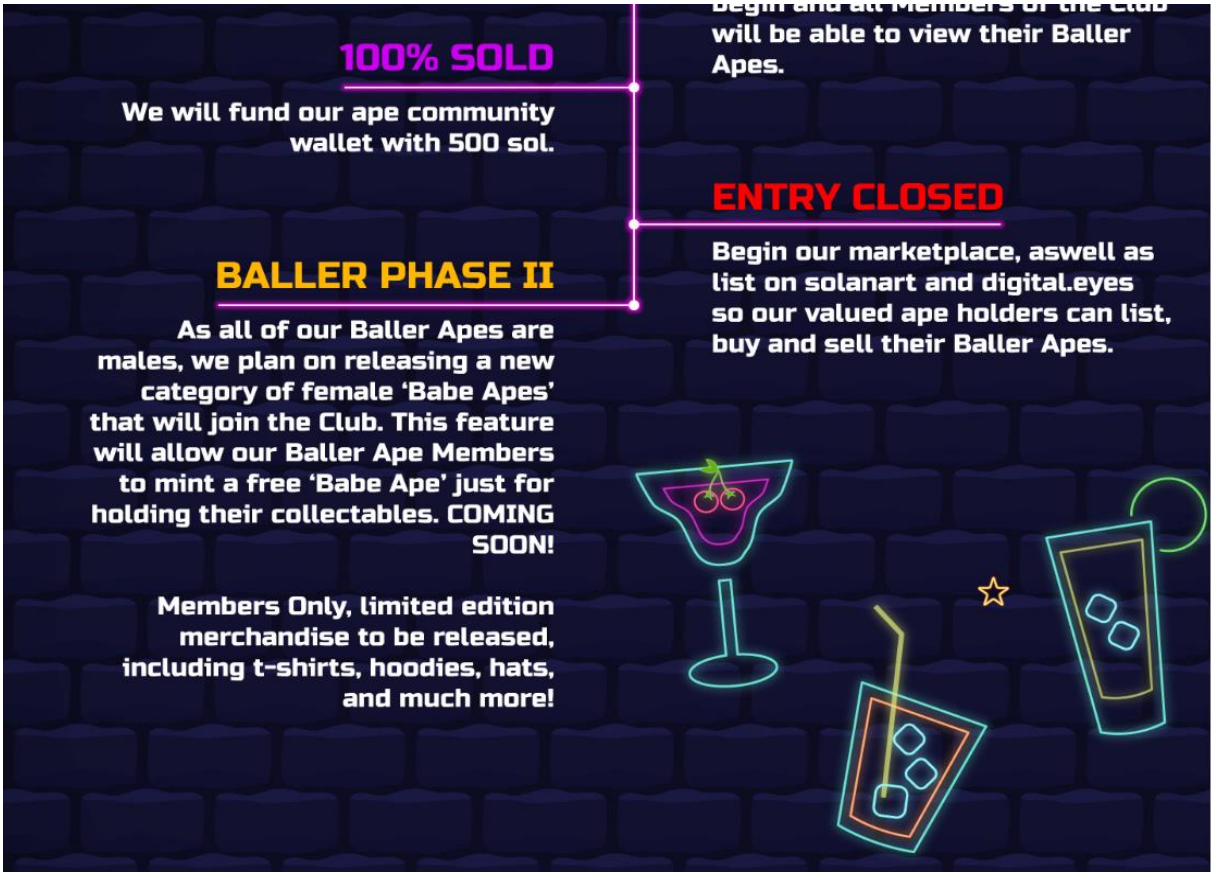
[1] SOL, also referred to as Solana, is a type of cryptocurrency that operates on the Solana Blockchain.

c. "All Baller Ape holders receive 5% in Sol [SOL] rewards."

11. The Baller Ape Club Website also claimed that a "rarity app . . . will be available via our website after minting is complete, thus will allow all holders to get their exact [NFT] rarity statistics!"

12. The images below are screenshots taken from the Baller Ape Club Website and show the advertised "roadmap" and plan for October 2021 to December 2021, which purportedly was to be implemented immediately following the Baller Ape NFT sale. In particular, the "Roadmap to VIP" advertised, among other things, that when 100% of the Baller Apes were sold, the Baller Ape NFT project developers would "fund our ape community wallet with 500 sol [SOL]."




will be able to view their Baller Apes.
100% SOLD
We will fund our ape community wallet with 500 sol.
ENTRY CLOSED
Begin our marketplace, aswell as list on solanart and digital.eyes so our valued ape holders can list, buy and sell their Baller Apes.
BALLER PHASE II
As all of our Baller Apes are males, we plan on releasing a new category of female 'Babe Apes' that will join the Club. This feature will allow our Baller Ape Members to mint a free 'Babe Ape' just for holding their collectables. COMING SOON!
Members Only, limited edition merchandise to be released, including t-shirts, hoodies, hats, and much more!

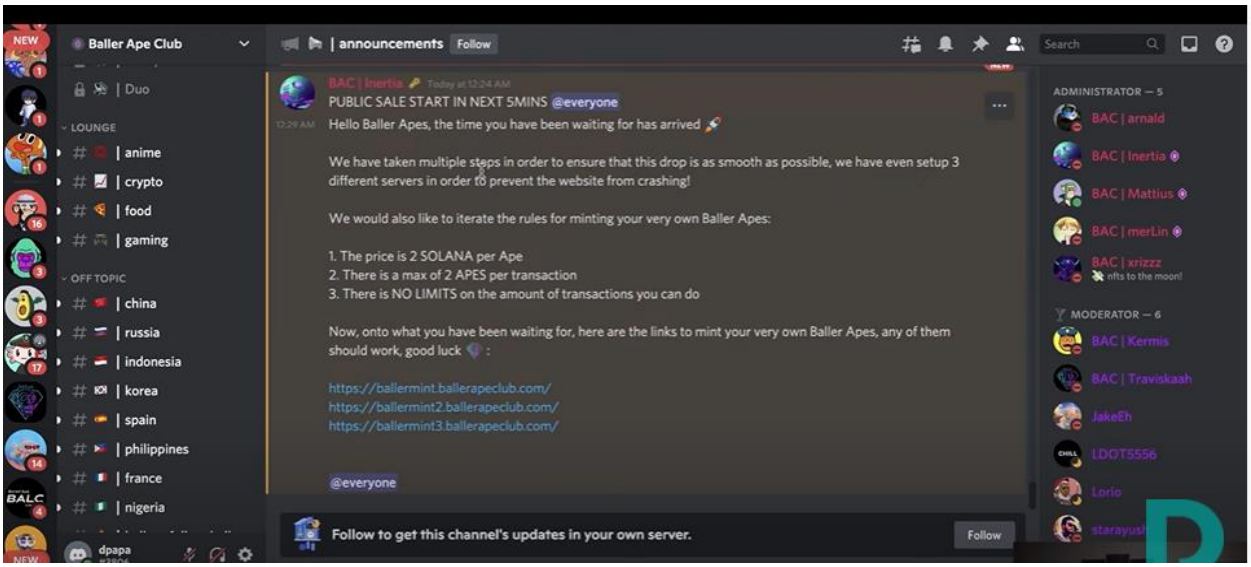
13. Notably, BAC also used other social media accounts, such as Twitter and Discord, to market the Baller Ape NFTs.

II. Baller Ape Club Rug Pull

14. In October of 2021, HSI Baltimore received information from the HSI Financial Crimes Unit regarding an NFT[2] rug pull scam involving BAC. On October 1, 2021, the BAC

[2] According to Ethereum.org, NFTs are tokens that people can use to represent ownership of unique items. They let users tokenize things like art, collectibles, even real estate. They can only have one official owner at a time, and they are secured by the blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence. NFT stands for non-fungible token. Non-fungible is an economic term that a person could use to describe things like furniture, a song file, or computer. These things are not interchangeable for other items because they have unique properties.

began to offer 5,000 Baller Apes NFTs for minting[3] using Solana cryptocurrency on the Solana blockchain[4] by providing three website links, connected to the BAC website, on the BAC Discord channel for investors to click on so that investors could purchase a newly minted NFT. A screenshot of the BAC Discord channel providing the three minting website links is below:



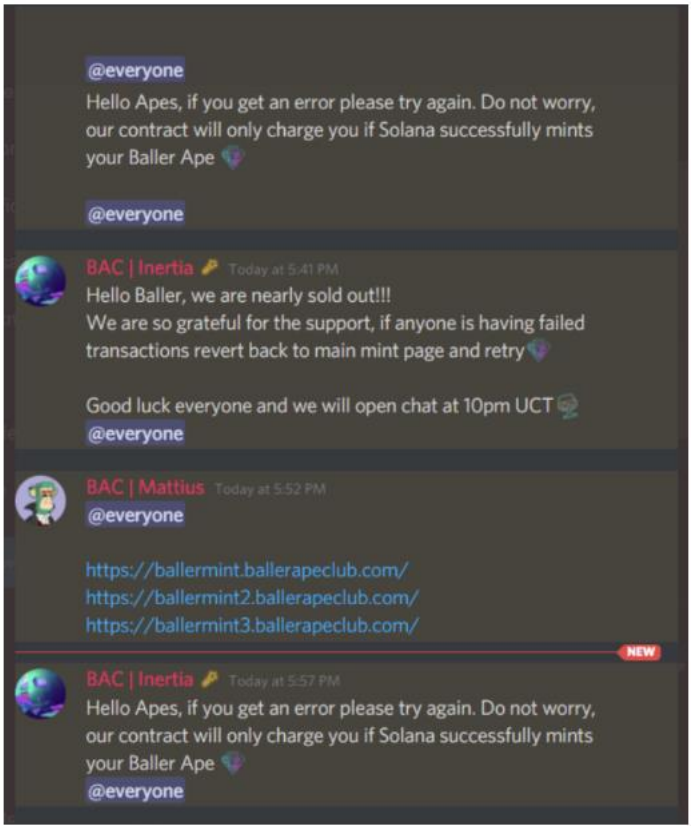
15. After an investor clicked on one of the website links, the site asked the investor to connect his or her Solana wallet[5] to the BAC website in order to purchase a BAC NFT. After connecting his or her wallet, the investor was asked how many NFTs he or she wanted to mint, and then the investor would click on a "Mint" button.

[3] Minting refers to the process of creating a brand new NFT.

[4] A blockchain is essentially a distributed public ledger that keeps track of all transactions, incoming and outgoing, and updates approximately multiple times per hour. The Solana blockchain was designed specifically for the Solana cryptocurrency. The Solana blockchain was designed to support NFTs.

[5] A cryptocurrency wallet is a software program or physical device that allows an individual to store his or her cryptocurrency, such as Solana, and allow for the sending and receiving of cryptocurrency transactions.

16. However, each time an investor clicked the "Mint" button, he or she would receive an error message that the transaction failed, and would be told to try again. Investors were unaware that even though they received the failed transaction message and did not receive any Baller Ape NFTs, they were sending Solana from their Solana wallets to one of the BAC scam wallets each time they had clicked the "Mint" button because they had connected their wallet to the BAC scam wallet. A screenshot of the BAC Discord channel shows one of the BAC administrators stating that if investors were receiving an error message, the investors should continue to try minting the NFTs, and assuring investors that they would only be charged if the Solana successfully minted their NFT.



17. Shortly after all the NFTs were "minted," the administrators behind the BAC NFT investment project deleted the BAC's Twitter and Discord accounts, which were being used by the BAC administrators to communicate with investors, and shut down the BAC website.

Investors who thought that they were purchasing a Baller Ape NFT realized that this was a type of scam called a rug pull. A "rug pull" is a colloquial term that referred to a scenario where the creator of an NFT project solicited investments and then abruptly abandoned a project and fraudulently retained the project investors' funds.

18. Blockchain analysis of the four Solana addresses used for the BAC NFT rug pull revealed approximately $2,600,000 United States Dollars (USD) worth of Solana at the time of the rug pull was stolen from investors. Investors also never received any BAC NFTs or any of the benefits listed on the BAC Website.

III. Binance Accounts

19. Blockchain analysis of the four Solana addresses used for the BAC NFT rug pull allowed investigators to identify two Binance[6] accounts that received approximately $679,000 (USD) in Solana and approximately $459,000 (USD) in Solana of BAC investors' funds. Information received from Binance regarding the accounts showed that, according to Know Your Customer (KYC) requirements, the accounts were opened by Jorge Eduardo BOLANOS Urena and Carlos Rodrigo MEDINA Najera, respectively. Further analysis revealed a third Binance account that received Solana from an address that also sent Solana to BOLANOS' Binance account prior to the NFT rug pull. This third Binance account also received cryptocurrency from BOLANOS' and MEDINA's Binance accounts that was traced back to the BAC scam addresses. KYC information from Binance revealed this third account was opened by Jorge Rafael Bolanos SANCHEZ Aldana. Binance KYC documents revealed BOLANOS, MEDINA, and SANCHEZ

[6] Binance is a cryptocurrency exchange, or a digital currency exchange, which is a business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies.

reside in the state of Quintana Roo, near Cancun, Mexico. Internet Protocol (IP)[7] address location data from Binance also resolve to the area referenced above.

20. A fourth Binance account also was identified during the investigation. This Binance account received approximately $570,000 USD in cryptocurrency that was traced back to the BAC scam addresses. Information received from Binance revealed the account, according to KYC requirements belongs to Le Anh TUAN. Binance KYC documents revealed TUAN resides in Vietnam. IP address location data from Binance resolves to Vietnam.

21. Analysis of the BOLANOS Binance account revealed the account was opened on September 8, 2021 at 01:30:19 UTC with an IP address of 187.252.205.162 and an email address of cryptoxiaomi@gmail.com. A Redmi Note 8 Android[8] device with an IP address of 200.68.172.60 is linked to the account. The KYC documents provided were a picture of a Costa Rican passport belonging to BOLANOS as well as a photograph of BOLANOS' face. The photographs of BOLANOS contain the logo "Redmi Note 8 AI Quad Camera" indicating the pictures were taken with the Redmi Note 8 (IP 200.68.172.60) Android device.

22. Analysis of the MEDINA Binance account revealed the account was opened on September 8, 2021 at 23:06:32 UTC with an IP address of 187.252.205.162 and an email address of edilsonbersai@gmail.com. A moto g(7) Android device with an IP address of 200.68.172.60 is linked to the account. The KYC documents provided were a picture of a Mexican identification card belonging to MEDINA as well as a photograph of MEDINA's face.

---

[7] An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other both over the internet as well as on other networks.

[8] Android is a mobile operating system that was developed by Google and runs on smartphones and tablets.

23. Analysis of the SANCHEZ Binance account revealed the account was opened on February 4, 2021 at 00:20:47 UTC with an IP address of 187.252.201.43 and an email address of rafa0george@gmail.com. There are multiple associated devices linked to SANCHEZ's account; however, the two devices linked to his account during the timeframe of the BAC NFT rug pull are a Chrome V85.0.4183.121 (Windows) Android device with an IP of 187.252.205.162, and a T770B Android device with an IP of 200.68.172.60. The KYC documents provided were a picture of a Mexican identification card belonging to SANCHEZ as well as a photograph of SANCHEZ's face.

24. Analysis of the TUAN Binance account revealed the account was opened on 01/12/2018 at 00:56:51 UTC with an IP address of 115.78.5.159 and an email address of nhocboxmr@gmail.com. An Android[9] device with an IP address of 27.79.124.253 is the most recently linked device to the account. The KYC documents provided were a picture of a Vietnamese identification card belonging to TUAN as well as a photograph of TUAN's face.

GMAIL ACCOUNT ANALYSIS

25. On February 18, 2022, your Affiant served a Federal Grand Jury subpoena to Google for subscriber information related to the **TARGET ACCOUNTS.** On February 20, 2022, Google provided the requested information for the **TARGET ACCOUNTS**. Below documents the analysis of the four **TARGET ACCOUNTS**.

26. The first **TARGET ACCOUNT**, cryptoxiaomi@gmail.com (Google Account ID: 1087185743577) was registered on September 8, 2021 at 01:28:21 UTC with an IP address of 187.252.205.162. The account name is "Crypto Washer." Google Services include Gmail, Web

[9] Android is a mobile operating system that was developed by Google and runs on smartphones and tablets.

& App Activity, Android, Google Calendar, Location History, Google Hangouts, YouTube, and Google Keep. No recovery email or phone numbers are associated with the account. The first login was on September 8, 2021 at 01:28:22 UTC with an IP address of 187.252.205.162. From September 8, 2021 to October 23, 2021, there were 13 logins with the IP address 187.252.205.162. From November 2, 2021 to December 22, 2021, there were 11 logins with the IP address of 187.252.200.174. On February 17, 2022, there was one login with the IP address of 187.252.195.34. This **TARGET ACCOUNT** was used to register BOLANOS' Binance account.

27. The second **TARGET ACCOUNT,** edilsonbersai@gmail.com (Google Account ID: 468512438816) was registered on July 2, 2021 at 07:52:12 UTC with an IP address of 200.68.172.129. The account name is "Edilson Gomez." Google Services include Gmail, Web & App Activity, Location History, Google Calendar, YouTube, Google Hangouts, Android, Google Keep, and Blogger. No recovery email or phone numbers are associated with the account. The first login was on July 2, 2021 at 07:52:14 UTC with an IP address of 200.68.172.129. On September 8, 2021, there were 3 logins at 07:08:43, 10:16:36, and 20:00:54 with the IP address of 187.252.205.162. On September 9, 2021, there was one login at 02:50:34 with the IP address of 187.252.205.162. On October 1, 2021, the date of the BAC NFT rug pull, there were 2 logins using the IP addresses of 200.68.172.60 and 200.68.172.168. On October 2, 2021, there was one login using the IP 200.68.172.60. This **TARGET ACCOUNT** was used to register MEDINA's Binance account.

28. The third **TARGET ACCOUNT**, rafa0george@gmail.com (Google Account ID: 1033521631013) was registered on April 24, 2007 at 15:43:11 with an IP address of 189.149.118.74. The account name is "George." Google Services include Web & App Activity, Gmail, Google Hangouts, Google Calendar, Google Base, Google Reader, Google Shopping,

Google News, orkut, Google Drive, Google Docs, YouTube, Google Page Creator, Google Sites, Google Services, Google URL Shortener, Android, Google Payments, Google Developers Console, Android Market, Google Code, iGoogle, Google Chrome Sync, Google Voice, Google Photos, Google Cloud Print, Location History, Tasks In Tingle, Android Device Console, Google Play, FeedBurner, Contacts, Google Play Music, Google Maps Engine, Google My Maps, Google Takeout, Google Keep, and Blogger. The email address lolquadcore@gmail.com was listed as a recovery email and the phone number +529987054292 was used as a recovery phone number. This phone number was also used to register SANCHEZ's Binance account. On September 8, 2021, there were 2 logins with an IP address of 187.252.205.162 at 01:29:38 and 02:38:00. From September 8, 2021 to October 25, 2021, there were multiple logins with the IP address of 187.252.205.162 and 200.68.172.60. This **TARGET ACCOUNT** was used to register SANCHEZ's Binance account.

29. The fourth **TARGET ACCOUNT**, nhocboxmr@gmail.com (Google Account ID: 788780590890) was registered on October 8, 2017 at 11:22:06 with an IP address of 171.255.166.149. The account name is "Nhoc Bo." Google Services include Web & App Activity, Gmail, Google Hangouts, Google Calendar, Android, Location History, YouTube, Google Payments, Google My Maps, Google Keep, Google URL Shortener, Google Docs, Google Analytics, Project Fi, Google Developers Console, and Google Groups. The email address bonttlat@gmail.com was listed as a recovery email, and the phone number +84964314444 was used as a recovery phone number. This phone number was also used to register TUAN's Binance account. This **TARGET ACCOUNT** was used to register TUAN's' Binance account.

IP ADDRESS AND ACCOUNT ACTIVITY ANALYSIS

TARGET ACCOUNT CRYPTOXIAOMI@GMAIL.COM

30. Analysis of the IP addresses and account activity collected from the **TARGET ACCOUNT cryptoxiaomi@gmail.com's** Google account and Binance account revealed the following: There is one associated device linked to BOLANOS' Binance account. That device is a Redmi Note 8 Android device with an IP address of 200.68.172.60. On September 8, 2021, a "Bind Google Verification" operation was performed within BOLANOS' Binance account with an IP address of 187.252.205.162. A "Bind Google Verification" enables a user to use a Google account as Two-factor Authentication (2FA)[10] when accessing their Binance account or conducting transactions within the Binance account. On September 8, 2021 at 05:18:51 UTC, BOLANOS' Binance account received nine Solana from 9FTHCfPDTpfWd2fHza873zRxafxsmuCXXWSnKZx1wd6D. This is the same address that sent one Solana to SANCHEZ's Binance account on September 7, 2021. On September 8, 2021 at 01:28:22, 01:28:23, 01:28:26, 01:29:41, and 02:38:00, there were five logins to **TARGET ACCOUNT cryptoxiaomi@gmail.com** using IP address 187.252.205.162. From October 1, 2021 to October 2, 2021, BOLANOS' Binance account received ten deposits of Solana directly from some of the BAC NFT rug pull scam addresses. On October 3, 29021 at 07:58:32 UTC there was one login to **TARGET ACCOUNT cryptoxiaomi@gmail.com** using IP address 187.252.205.162. The Solana was then converted to Dai[11] and sent from BOLANOS' Binance address to various other addresses. It appears the Solana was converted to Dai from within BOLANOS' Binance account. Converting the Solana to Dai causes the cryptocurrency to move

[10] Two-factor authentication (2FA) is a specific type of multi-factor authentication (MFA) that strengthens access security by requiring two methods (also referred to as authentication factors) to verify your identity.

[11] Dai is a stable coin cryptocurrency which aims to keep its value as close to one United States dollar as possible through an automated system of smart contracts on the Ethereum blockchain.

from the Solana blockchain to the Ethereum blockchain which is known as chain-hopping.[12] Based on your affiant's training and experience, he knows criminals will use chain-hopping in an attempt to make it harder for law enforcement to trace or follow the movement of illegally obtained cryptocurrency. Based on your affiant's training and experience, the name of the **TARGET ACCOUNT cryptoxiaomi@gmail.com**, "Crypto Washer," leads your affiant to believe this account was specifically set up to "wash" or launder the Solana cryptocurrency stolen from victims of the BAC NFT rug pull. Based on your affiant's training and knowledge, he knows cryptocurrency exchanges such as Binance will send emails to a user's account email to confirm trades, account logins, or other account activity. Your affiant believes this **TARGET ACCOUNT** was being used solely to facilitate the movement of the stolen cryptocurrency and will contain evidence of the **TARGET OFFENSES** such as emails, location data, photographs and other documentation used during the Binance account registration process and the subsequent laundering of the stolen cryptocurrency.

TARGET ACCOUNT EDILSONBERSAI@GMAIL.COM

31. Analysis of the IP addresses and account activity collected from the **TARGET ACCOUNT edilsonbersai@gmail.com's** Google account and Binance account revealed the following. There is one associated device linked to MEDINA's Binance account. That device is a Moto g(7) Android device with an IP address of 200.68.172.60. On October 1, 2021, a "Bind Google Verification" operation was performed within MEDINA's Binance account using the IP

[12] Chain hopping is the changing of one cryptocurrency into a different type of cryptocurrency therefore moving onto a different block chain as an attempt to make it harder for law enforcement to trace the movement of illicit cryptocurrency. In this case, the cryptocurrency was moved from the Solana blockchain to the Ethereum blockchain.

address 200.68.172.60. From October 1, 2021 to October 2, 2021, MEDINA's Binance account received six deposits of Solana directly from some of the BAC NFT rug pull scam addresses. The account was accessed using IP addresses 200.68.172.168 and 200.68.172.60. On October 1, 2021 at 00:43:22 UTC and 14:11:18 UTC, there were two logins to the **TARGET ACCOUNT edilsonbersai@gmail.com** using IP address 200.68.172.168 and 200.68.172.60 respectively. On October 2, 2021 at 14:14:26 UTC, there was one login to the **TARGET ACCOUNT edilsonbersai@gmail.com** using the IP address 200.68.172.60. The Solana is then converted to Dai and sent from MEDINA's Binance address to various other addresses. It appears the Solana was converted to Dai from within MEDINA's Binance account. Based on your affiant's training and experience, the user of MEDINA's Binance account used chain-hopping in an attempt to hide the true origin of the cryptocurrency. Based on your affiant's training and knowledge, he knows cryptocurrency exchanges such as Binance will send emails to a user's account email to confirm trades, account logins, or other account activity. Your affiant believes this **TARGET ACCOUNT** was being used solely to facilitate the movement of the stolen cryptocurrency and will contain evidence of the **TARGET OFFENSES** such as emails, location data, photographs and other documentation used during the Binance account registration process and subsequent laundering of the stolen cryptocurrency.

TARGET ACCOUNT RAFA0GEORGE@GMAIL.COM

32. Analysis of the IP addresses and account activity collected from the **TARGET ACCOUNT rafa0george@gmail.com's** Google account and Binance account revealed the following. There are multiple associated devices linked to SANCHEZ's Binance account however the two devices linked to his account during the timeframe of the BAC NFT rug pull are a Chrome V85.0.4183.121 (Windows) Android device with an IP of 187.252.205.162. The second was a

T770B Android device with an IP of 200.68.172.60. On February 28, 2021, a "Bind Google Verification" operation was performed within SANCHEZ's Binance account using the IP address 187.252.201.43. On September 7, 2021 at 20:00:04, SANCHEZ received 1 Solana from address 9FTHCfPDTpfWd2fHza873zRxafxsmuCXXWSnKZx1wd6D. Access logs for SANCHEZ's Binance account revealed login and account activity on September 7, 2021 at 19:33:47 UTC, 19:57:45 UTC, 20:51:19 UTC, and 23:08:26 with an IP address login of 187.252.205.162. On September 8, 2021 at 01:29:38 UTC, there was a login to **TARGET ACCOUNT rafa0george@gmail.com** using IP address 187.252.205.162. Shortly after receiving the 1 Solana, the 1 Solana was sent to 2ojv9BAiHUrvsm9gxDe7fJSzbNZSJcxZvf8dqmWGHG8S. On September 8, 2021 at 02:38:00 UTC, there was one login to **TARGET ACCOUNT rafa0george@gmail.com** using IP address 187.252.205.162. On October 19, 2021 at 15:22:19 UTC, SANCHEZ's Binance account received a deposit of Dai that originated from BOLANOS's Binance account. The IP address 187.252.205.162 was used to access SANCHEZ's Binance account during this transaction. On October 20, 2021, there were two logins to **TARGET ACCOUNT rafa0george@gmail.com** at 08:46:32 UTC and 10:58:02 UTC using the IP address of 187.252.205.162. On November 5, 2021 at 18:10:05 UTC, SANCHEZ's Binance account received a deposit of Dai. These funds were traced back to a Binance swap[13] wallet. Due to the use of the Binance swap service, investigators have not been able to confirm the exact origin of the Dai at this time but based on prior deposits of Dai that originated from BAC NFT scam addresses or addresses linked to the BAC NFT rug pull and the totality of the investigation, there

[13] A swap service is a service provided by exchanges such as Binance that allows a user to convert one cryptocurrency to another cryptocurrency such as SOL to Dai, USDT, and ETH in this case.

is probable cause to believe these funds originated from the BAC NFT scam addresses. The IP address 187.252.200.174 was used to access SANCHEZ's Binance account during this transaction. On November 5, 2021 there were two logins to the **TARGET ACCOUNT rafa0george@gmail.com** at 01:36:32 UTC and 21:18:05 UTC using the IP address of 187.252.200.174 and 200.68.161.29. On November 10, 2021 at 13:05:34 UTC, SANCHEZ's Binance account received a deposit of Tether (USDT).[14] These funds traced back to a Binance swap wallet. Due to the use of the Binance swap service, investigators have not been able to confirm the exact origin of the USDT at this time but based on prior deposits of funds into SANCHEZ's Binance account that originated from BAC NFT scam addresses or addresses linked to the BAC NFT rug pull and the totality of the investigation, there is probable cause to believe these funds originated from the BAC NFT scam addresses. The IP address 187.252.205.162 was used to access SANCHEZ's Binance account during this transaction. On November 10, 2021, there were three logins to **TARGET ACCOUNT rafa0george@gmail.com** at 09:08:11 UTC, 12:56:04 UTC, and 12:57:12 UTC using the IP address of 187.252.200.174. On November 12, 2021, SANCHEZ's Binance account received a deposit of Dai at 13:44:37 UTC. These funds were traced back to BOLANOS' Binance account. On November 12, 2021 at 15:30:26 UTC, there was one login to **TARGET ACCOUNT rafa0george@gmail.com** using the IP address 200.68.172.21. On November 26, 2021 at 20:36:34 UTC, SANCHEZ's Binance account received a deposit of Dai. These funds were traced back to BOLANOS' Binance account. On November 26, 2021, there were three logins to **TARGET ACCOUNT rafa0george@gmail.com** at 00:25:16 UTC, 00:32:55 UTC, and 06:31:16 UTC using the IP address 187.252.200.174. On December 6,

[14] Tether (USDT) is another type of stable coin cryptocurrency that operates on the Ethereum blockchain.

2021 at 06:52:58 UTC and 20:34:51 UTC, SANCHEZ's Binance account received two deposits of Dai. These funds were traced back to BOLANOS' Binance account. On December 6, 2021 at 23:37:24 UTC, there was one login to **TARGET ACCOUNT rafa0george@gmail.com** using IP address 200.68.137.202. On January 6, 2022 at 01:39:40, SANCHEZ' Binance account received one deposit of Dai. These funds were traced back BOLANOS' Binance account. On January 6, 2022 at 01:34:02 UTC and 13:02:20 UTC, there were two logins to **TARGET ACCOUNT rafa0george@gmail.com** using IP addresses 187.252.200.174 and 200.68.137.227. On January 16, 2022 at 10:40:18 UTC and 18:00:20 UTC, SANCHEZ's Binance account received one deposit of USDT and one deposit of ETH. These funds were traced back to a wallet that contains comingled funds that were traced back to MEDINA's and BOLANOS' Binance accounts. On January 16, 2022 at 18:43:13 UTC and 20:56:46 UTC, there were two logins to **TARGET ACCOUNT rafa0george@gmail.com** using IP addresses 187.252.200.174 and 200.68.161.103. On January 17, 2022 at 16:19:16 UTC and 20:12:16 UTC there were two deposits of Dai to SANCHEZ's Binance account. These funds were traced back to a wallet that contains comingled funds that were traced back to MEDINA's and BOLANOS' Binance accounts. On January 17, 2022 at 06:02:17 UTC, 16:46:53 UTC, 20:55:36 UTC, and 20:55:37 UTC, there were four logins to **TARGET ACCOUNT rafa0george@gmail.com** using IP addresses 200.68.172.161, 200.68.172.133, and 200.68.172.56. On January 25, 2022 at 17:33:40 UTC, SANCHEZ's Binance account received one deposit of Dai. These funds were traced back to a wallet that contains comingled funds that were traced back to MEDINA's and BOLANOS' Binance accounts. On January 25, 2022 at 06:10:38 UTC, 16:56:43 UTC, 16:57:21 UTC, 16:57:22 UTC, and 19:19:07 UTC, there were five logins to **TARGET ACCOUNT rafa0george@gmail.com** using IP addresses 200.68.136.72 and 187.252.201.166. On February 4, 2022 at 00:42:40 UTC,

SANCHEZ' Binance account received a deposit of Dai. These funds were traced back to BOLANOS' Binance account. On February 4, 2022 at 15:49:45 UTC, 15:53:18 UTC, 15:53:19 UTC, and 20:41:11 UTC, there were four logins to **TARGET ACCOUNT rafa0george@gmail.com** using IP addresses 200.68.161.27 and 187.252.201.166. On February 6, 2022 at 21:20:20 UTC, SANCHEZ's Binance account received a deposit of Dai. These funds were traced back to BOLANOS' Binance account. On February 6, 2022 at 08:05:47 UTC, there was one login to **TARGET ACCOUNT rafa0george@gmail.com** using IP address 187.252.195.34. On February 16, 2022 at 02:45:08 UTC and 13:29:51 UTC, SANCHEZ's Binance account received two deposits of Dai. These funds were traced back to BOLANOS' and MEDINA's Binance accounts. On February 16, 2022 at 02:35:31 UTC, there was one login to **TARGET ACCOUNT rafa0george@gmail.com** using IP address 187.252.195.34. From February 19, 2022 to March 6, 2022, there were four more deposits of Dai, USDT, and ETH in SANCHEZ's Binance account. These funds were traced back to BOLANOS's and MEDINA's Binance accounts. Your affiant is unable to see if there are corresponding **TARGET ACCOUNT** logins because the date range of activity ended February 18, 2022. Based on your affiant's training and experience, your affiant believes SANCHEZ's Binance account was receiving some of the laundered Solana that was stolen from investors of the BAC NFT rug pull scam. Your affiant knows criminals will use methods such as chain-hopping and moving the illicit cryptocurrency through multiple accounts in an attempt to make it harder for law enforcement to trace or follow before it is ultimately sent to their account where they can liquidate it into a fiat currency or send to other co-conspirators. Based on the conversion of the Solana to Dai, USDT, and ETH and then the movement of the DAI, USDT, and ETH through various accounts before reaching SANCHEZ's Binance account, it appears to your affiant that SANCHEZ was attempting to

obfuscate the true origin of the Dai, USDT, and ETH which was the BAC NFT rug pull scam. Based on your affiant's training and knowledge, your affiant knows cryptocurrency exchanges such as Binance will send emails to a user's account email to confirm trades, account logins, or other account activity. Your affiant believes this **TARGET ACCOUNT** was being used to facilitate the movement of the stolen cryptocurrency and will contain evidence of the **TARGET OFFENSES** such as emails, location history, photographs and other documentation used during the Binance account registration process and the subsequent laundering of the stolen cryptocurrency.

TARGET ACCOUNT NHOCBOXMR@GMAIL.COM

33. Analysis of the account activity collected from the **TARGET ACCOUNT nhocboxmr@gmail.com's** Google account and Binance account revealed the following. TUAN's Binance account used the Gmail address nhocboxmr@gmail.com during the registration process. Based on your affiant's training and knowledge, he knows cryptocurrency exchanges such as Binance will send emails to a user's account email to confirm trades, account logins, or other account activity. IP log in activity revealed multiple **TARGET ACCOUNT** log ins during the month of September 2021 and October 2021 which was the timeframe in which the BAC NFT rug pull occurred. Tracing of the BAC scam funds revealed large amounts of cryptocurrency deposited into TUAN's Binance account. Your affiant believes this **TARGET ACCOUNT** was being used to facilitate the movement of the stolen cryptocurrency and will contain evidence of the **TARGET OFFENSES** such as emails, location data, photographs and other documentation used during the Binance account registration process and subsequent laundering of the stolen cryptocurrency.

SUMMARY OF PROBABLE CAUSE

34. Based on the patterns of the illicit cryptocurrency deposits and corresponding

TARGET ACCOUNT logins, as well as the use of the **TARGET ACCOUNTS** during the registration of the Binance accounts used in the BAC NFT rug pull, there is probable cause to believe that the **TARGET ACCOUNTS**, namely, the Google accounts associated with the email addresses cryptoxiaomi@gmail.com, edilsonbersai@gmail.com, rafa0george@gmail.com, and nhocboxmr@gmail.com will contain evidence and instrumentalities of the above-described NFT rug pull scheme, in violation of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1956 (Money Laundering) (the **TARGET OFFENSES**).

35. For **TARGET ACCOUNT** cryptoxiaomi@gmail.com, the Government is seeking records for the time period of account inception (September 8, 2021) to the present. It appears this **TARGET ACCOUNT** was created for the sole purpose of facilitating the above-described NFT rug pull scheme. Records from account inception to present may allow law enforcement to confirm or deny the identity and location of the account user. They will also provide information about the user's long-term patterns of communication and relationships with other persons, including potential co-conspirators. Further, because the account appears to have been created to facilitate illegal activity, the same account may also be used to facilitate additional or ongoing frauds and are likely to continue to receive relevant messages from victims, co-conspirators, and financial institutions and virtual currency exchangers being used in the criminal activity.

36. For **TARGET ACCOUNT** edilsonbersai@gmail.com, the Government is seeking records for the time period of account inception (July 2, 2021) to the present. It appears this **TARGET ACCOUNT** was created for the sole purpose of facilitating the above-described NFT rug pull scheme. Records from account inception to present may allow law enforcement to confirm or deny the identity and location of the account user. They will also provide information about the user's long-term patterns of communication and relationships with other persons, including

potential co-conspirators. Further, because the account appears to have been created to facilitate illegal activity, the same account may also be used to facilitate additional or ongoing frauds and are likely to continue to receive relevant messages from victims, co-conspirators, and financial institutions and virtual currency exchangers being used in the criminal activity.

37. For **TARGET ACCOUNT** rafa0george@gmail.com, the Government is seeking records for the time period of January 1, 2020 to the present. Based on the above-mentioned IP address analysis, it appears the user of this **TARGET ACCOUNT** has access to the other two **TARGET ACCOUNTS** and appears to have a larger role in facilitating the above-described NFT rug pull scheme. Records from January 1, 2020 to the present may allow law enforcement to confirm or deny the identity and location of the account user. They will also provide information about the user's long-term patterns of communication and relationships with other persons, including potential co-conspirators. Further, because the account appears to have been created to facilitate illegal activity, the same account may also be used to facilitate additional or ongoing frauds and are likely to continue to receive relevant messages from victims, co-conspirators, and financial institutions and virtual currency exchangers being used in the criminal activity.

38. For **TARGET ACCOUNT** nhocboxmr@gmail.com, the Government is seeking records for the time period of January 1, 2020 to the present. Based on the above-mentioned Binance analysis, it appears the user of this **TARGET ACCOUNT** had large amounts of BAC scam funds deposited in his Binance account and appears to have a larger role in facilitating the above-described NFT rug pull scheme. Records from January 12020 to the present may allow law enforcement to confirm or deny the identity and location of the account user. They will also provide information about the user's long-term patterns of communication and relationships with other persons, including potential co-conspirators. Further, because the account appears to have

been created to facilitate illegal activity, the same account may also be used to facilitate additional or ongoing frauds and are likely to continue to receive relevant messages from victims, co-conspirators, and financial institutions and virtual currency exchangers being used in the criminal activity.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

1. Google is the provider of the internet-based account(s) identified by **cryptoxiaomi@gmail.com, edilsonbersai@gmail.com, rafa0george@gmail.com, and nhocboxmr@gmail.com.**

2. Google provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google LLC services, such as instant messages and remote photo or file storage.

3. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.

4. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google

subscribers can also use that same username or account in connection with other services provided by Google.[15]

5. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

6. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing, voice calls, video chats, SMS text messaging, and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Like e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches,

[15] For Google, the services may include: electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

browsing history, and various other types of information on Google's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

7. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

8. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a

particular user account for cellular data or voice services, and some identifiers are assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.

9. Google also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's Google account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as Google) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the

application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of Google are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's Google account via the mobile application.

10. Based on my training and experience, I know that providers such as Google use cookies and similar technologies to track users visiting Google's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to Google. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as Google may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a Google account and determine the scope of criminal activity.

11. Based on my training and experience, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that

evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.

12. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. In summary, based on my training and experience in this context, I believe that the computers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers), as well as Google-generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

14. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and

experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).[16]

[16] At times, internet services providers such as Google can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of Google's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

15. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within the user-generated content created or stored by the Google subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, e-mail accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because e-mail accounts and similar Google accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

16. I respectfully request, pursuant to Rule 41 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. I submit that Trial Attorney Keven Lowell, an attorney for the United States, can identify my voice and telephone number for the

Court.

CONCLUSION

39. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING AND DELAYED DISCLOSURE

40. I further request that this Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court, except that the government may provide a copy of the search warrant to Google for compliance with this Court's Order. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure might give targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify others (including, but not limited to, accomplices), or otherwise seriously jeopardize the investigation.

41. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that this Court issue an Order commanding Google not to notify any person (including the subscribers or customers of the accounts listed in the attached warrant) of the existence of the attached warrant for a period of one year, with leave for the government to reapply to this Court for an extension of this Order upon a showing of good cause.

Respectfully submitted,

_____
Brandon Dreyer
Special Agent, Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this _____ day of _____, 2022.

_____
The Honorable Alexander F. MacKinnon
United States Magistrate Judge