AO 91 (Rev. 11/11) Criminal Complaint (approved by US Attorney Romero/RJL)

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.
MINH QUOC NGUYEN

Case No. 23-MJ-528

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 1, 2017 to March 14, 2023 in the county of Philadelphia in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1956(a)(1)(B)(i)	money laundering
18 U.S.C. § 1960	operating an unlicensed money transmitting business
18 U.S.C. § 1028(a)(3)	identity theft

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

/s/ Steven Parker
Complainant's signature

Steven Parker, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/14/2023 at 3:01 pm

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

HON. RICHARD A. LLORET, USMJ
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Steven Parker, Special Agent with the Federal Bureau of Investigation (FBI) being duly sworn, do hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of a criminal complaint and an arrest warrant for MINH QUOC NGUYEN for violations of Title 18, United States Code, Sections 1956(a)(1)(B)(i) (conducting a financial transaction with knowledge that the transaction is designed to conceal the proceeds of the specified unlawful activity), 1960 (unlicensed money transmitting business), and 1028(a)(3) (possession with intent to use or transfer five or more documents or authentication features) relating to his operation of a money laundering enterprise known as ChipMixer. Since August 2017, ChipMixer has been a cryptocurrency platform operating as an online "mixer." In essence, ChipMixer is a money laundering service that is used by its customers to launder bitcoin associated with a crime.

2. The FBI has determined that NGUYEN operated ChipMixer by using aliases and stolen identities from individuals located around the world (including the United States and the Eastern District of Pennsylvania) to purchase and maintain infrastructure, move illicit funds, and avoid law enforcement detection. Since 2017, NGUYEN has knowingly facilitated the laundering of $3 billion worth of bitcoin through ChipMixer. A large percentage of that $3 billion represents the proceeds of ransomware payments, thefts, darknet marketplace payments, nation-state criminal activity, and other illegal activity. In addition, NGUYEN has failed to register ChipMixer with the United States Department of the Treasury as a "money services business" (MSB) through the Financial Crimes Enforcement Network (FinCEN).

3. NGUYEN is a Vietnamese citizen with a date of birth of October 21, 1973. NGUYEN has basic training in cryptographic engineering and previously worked in decrypting communications and cyber reconnaissance. In 2016, NGUYEN earned his Ph.D. in Electronic Engineering in Taiwan.

4. Since 2018, I have been an FBI Special Agent. I am currently assigned to the FBI's Philadelphia Field Office, Cyber National Security Squad, which investigates complex computer intrusion crimes involving advanced persistent threats. I have a Master's degree in Digital Forensics and Cyber Investigations and previously worked as a police officer for a local municipality. I have participated in investigations into criminal offenses involving complex computer intrusions, computer and wire fraud, money laundering, and the distribution of Child Sexual Abuse Material (CSAM). I am familiar with the means and methods used to commit such offenses, including the use and transmission of cryptocurrencies.

5. The statements contained in this affidavit are based on my own knowledge and on information provided to me by other law enforcement officers, witnesses, and responses to legal process. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not set forth all of my knowledge about this matter. All of the emails, comments, posts, and other materials quoted in this affidavit bear the same spelling, punctuation, and grammar as found in the originals of these records. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date asserted. Similarly, where I assert a certain amount of bitcoin or United States currency, I am asserting approximately that amount of currency. In

addition, some of the emails referenced below were written in whole or in part in Vietnamese or another foreign language. Because I am not proficient in those languages, I have relied upon summary translations provided to me by FBI agents, linguists, and contractors who are fluent in the pertinent foreign language. Finally, I reference a number of seized emails in this affidavit. I note that there are discrepancies in the date and time stamp of some of the email communications based on a variety of factors, including the location of the sender or recipient, the location of the email servers, and events occurring in numerous time zones. Thus, the same email seized from different accounts may have different time stamps.

II. DEFINITIONS

6. Based on my training and experience, I am familiar with the following terms:

a. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address in that it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers (ISPs).

b. Virtual Machine: A virtual machine is a computer resource that uses software code (instead of a physical computer) to run programs and applications. One or more virtual machines run on a physical "host" machine. Each virtual machine runs its own operating system.

c. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

d. Domain Name System: The Domain Name System (DNS) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as www.example.com. The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

e. Domain Name Servers: Domain Name Servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which has its headquarters at 21355 Ridgetop Circle, Dulles, Virginia.

f. Domain Registration Lifecycle: Domain names can be registered for periods of one-year up to ten years. At the end of a domain's registration period, it can be renewed. Registrars typically have a grace period of up to 45 days after expiration where the domain can only be renewed by the registrant. After this period, there is another 30-day grace period where the domain is placed in a "pending delete-restorable" status. During this period, the

registrant can still renew the registration, typically for a much higher fee. After this period, the domain is placed in a pending delete status for five days. Finally, the domain name is made publicly available for re-registration.

g. Ransomware: is a type of malicious software program that encrypts the contents of a victim computer or computer network and restricts the victim's ability to use the computer or computer network. In order for the victim to regain access to the computer or computer network, the victim must typically pay a ransom to the attackers in exchange for receiving the required decryption keys. Modern ransomware payments are typically made in cryptocurrency. Ransomware attacks are often orchestrated by a group of people with different responsibilities. For example, one person or group of people might be responsible for writing the ransomware code, while another might be responsible for gaining access to a victim's computer system, executing the attack, and collecting the ransom.

h. Bitcoin (sometimes abbreviated as "BTC"): is one type of virtual currency. Thousands of computers connected via the Internet run Bitcoin software and participate in the Bitcoin network. This software provides all necessary services to transact in bitcoin, including (i) allowing users to create "Bitcoin addresses," roughly analogous to accounts; (ii) injecting new bitcoin into circulation; and (iii) securely transferring bitcoin from one Bitcoin address to another.

To send and receive bitcoin, the parties involved in a transaction use Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique private key. This key is the equivalent of a password or

PIN and is necessary to access the funds associated with a Bitcoin address. Only the holder of a Bitcoin address's private key can authorize transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and can use a unique Bitcoin address for each transaction.

When a sender initiates a bitcoin transaction, the sender transmits a transaction announcement across the peer-to-peer (P2P) Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

A Bitcoin address owner's identity is generally anonymous within the blockchain unless the owner chooses to make information about their Bitcoin address publicly available. Investigators can identify Bitcoin addresses of interest and trace them to exchanges. Many exchanges adhere to Know Your Customer/Anti-Money Laundering laws which require users to verify their identity through submitting photo identification.

The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the addresses and private keys. Wallets can be housed in a variety of forms, including as an

online account associated with a cryptocurrency exchange. Many users back up their virtual currency wallets using "recovery seeds." A recovery seed, also known as a root key, seed phrase, or recovery phrase, is a list of words that, when entered in a specific order into virtual currency wallet software, allows whoever is in possession of the words to reestablish access to virtual assets within the wallet. Additional security safeguards for wallets can include two-factor authorization (such as a password and a phrase). Based on my background, training, and experience, I know that individuals possessing virtual currencies often have safeguards in place to ensure their cryptocurrencies are secured in the event their assets become vulnerable to seizure by law enforcement and/or unauthorized transfer. Additionally, individuals may store copies of their private keys in multiple locations or entrust them to associates who can use the private keys to transfer the funds out of the reach of law enforcement if the main individual is searched or arrested.

Most virtual currency exchanges act as both a trading platform and storage platform. An exchange typically allows trading between the U.S. dollar, other fiat currencies, bitcoin, and other virtual currencies. Many virtual currency exchanges also store their customers' virtual currency in exchange-based wallets that are associated with each customer's account(s). These exchanges act as money services businesses and are legally required to conduct due diligence of their customers and to have anti-money laundering checks in place. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 et seq., and must collect identifying information of their customers and verify their clients' identities.

Because virtual currency exchanges generally collect identifying information about their customers, subpoenas or other appropriate legal process submitted to exchanges can, in some instances, reveal the true identity of an individual responsible for a bitcoin transaction. For this reason, many criminal actors who use Bitcoin to facilitate their illicit transactions look for ways to gain greater anonymity.

As previously stated, while the identity of a bitcoin address owner is generally anonymous, law enforcement can often identify the owner of a particular bitcoin address by analyzing the blockchain. Such analysis can reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many Bitcoin addresses to receive payments from different customers. When the user wants to complete a transaction with the bitcoin that he or she has received (e.g., to exchange bitcoin for other currency or to use bitcoin to purchase goods or services), the user may group those addresses together to co-spend in a single transaction. These groups of co-spending addresses are called “clusters”. Investigators may then conclude that each of the addresses in the cluster are associated to the same user due to the user having access to and using the associated private keys to complete the transaction.

Law enforcement sometimes uses third-party commercial software offered by several different blockchain analysis companies to investigate bitcoin transactions. These companies analyze the Bitcoin blockchain and attempt to identify the individuals or groups involved in transactions. Specifically, these companies create large databases that group Bitcoin addresses into “clusters” through analysis of data underlying Bitcoin transactions. In other words, a cluster is an estimate of all the Bitcoin addresses (and their BTCs) contained in a user’s Bitcoin wallet or wallets.

The methods used by blockchain analysis companies have been independently validated by computer scientists, who have shown they can use "clustering" methods to take advantage of clues regarding how Bitcoin are typically aggregated or split up to identify Bitcoin addresses and their respective account owners. This blockchain analysis software is an anti-money laundering software used by financial institutions and law enforcement organizations worldwide. It has supported many unrelated law enforcement investigations, has been the basis for numerous search and seizure warrants, and has been shown to be reliable when used accurately.

i. Cryptocurrency Mixing Services: The FBI has been investigating the use of cryptocurrency mixing services that launder proceeds of criminal activity. A cryptocurrency "mixer" or "tumbler" is an entity that allows users to commingle or mix different streams of potentially identifiable cryptocurrency. While these services often promote themselves as designed to enhance privacy and anonymity, they are often used to conceal proceeds from illegal transactions by accepting "dirty" bitcoin from users and returning "clean" bitcoin to a wallet address specified by the original user.

Different mixers have various features and processes. Generally, the customer can send cryptocurrency to a specific wallet address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers and sends it through a convoluted series of transactions, making it difficult to track on the blockchain. When a customer makes a request to "cash out" his or her cryptocurrency, the mixer arranges for the funds to be transferred from another address that cannot be traced to the customer.

j. Distributed Denial of Service: Distributed Denial of Service (DDoS) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an

online service, network resource or host machine unavailable to its intended users on the Internet.

k. Tor Hidden Services: Tor (which stands for "The Onion Router") is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers, or "proxies," rendering conventional IP address-based methods of identifying users ineffective. When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, is logged by the website. Thereby, the actual IP address is obfuscated.

The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services take advantage of unique technical features of Tor that conceal the computer server's location. Unlike standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, for example "abc123def456ghi7" followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website by simply looking it up on a publicly available DNS listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service via public lookups. Additionally, as with all Tor communications, communications between users'

computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service. For these reasons, hidden services are often referenced as residing on the "darknet" or "dark web" (compared with ordinary Internet websites that are often referenced as residing on the "clearnet").

l. Darknet marketplace: A darknet marketplace is a website accessible on Tor which is used to anonymously buy and sell illegal goods and services. Darknet marketplaces are most often associated with drug trafficking.

m. Fraud shop: A fraud shop is a criminal website that facilitates the purchase and sale of fraud-related goods and services. Fraud shops are most often associated with trafficking of stolen credit cards, hacked account credentials, and data stolen through network intrusions.

III. THE INVESTIGATION

A. Overview of ChipMixer

7. As part of the FBI's efforts to combat ransomware attacks against victims in the United States, including the Eastern District of Pennsylvania (EDPA), the FBI became aware of a cryptocurrency mixing service known as ChipMixer, operating through the following clearnet domains and Tor sites:

a. clearnet: chipmixer.com

b. Tor: chipmixorflykuxu56uxy7gf5o6ggig7xru7dnihc4fm4cxqsc63e6id.onion

c. clearnet: chipmixer.io

d. Tor: chipmixerwzxtzbw.onion

e. clearnet: chipmixer.club

f. Tor: qw6xpezaqb57xsviksbsbjlrftevt52s7baaxiubwb6mkpwkqcfdppqd.onion

8. ChipMixer customers send their bitcoin to ChipMixer, which then "mixes" it with other ChipMixer users' cryptocurrency, commingling the funds in a way that prevents law enforcement and regulators from tracing transactions. This allows ChipMixer's customers to launder their illicit proceeds and conceal their true identities and activities.

9. The domain chipmixer.com – screenshots of which are shown below – is the functional piece of the ChipMixer infrastructure. Specifically, at its inception in 2017, a user could go to chipmixer.com and choose to either stay on the clearnet site to launder bitcoin or be redirected to the ChipMixer Tor site to launder bitcoin there. Starting in May 2022, the chipmixer.com clearnet site was modified to only redirect a user to the ChipMixer Tor site.

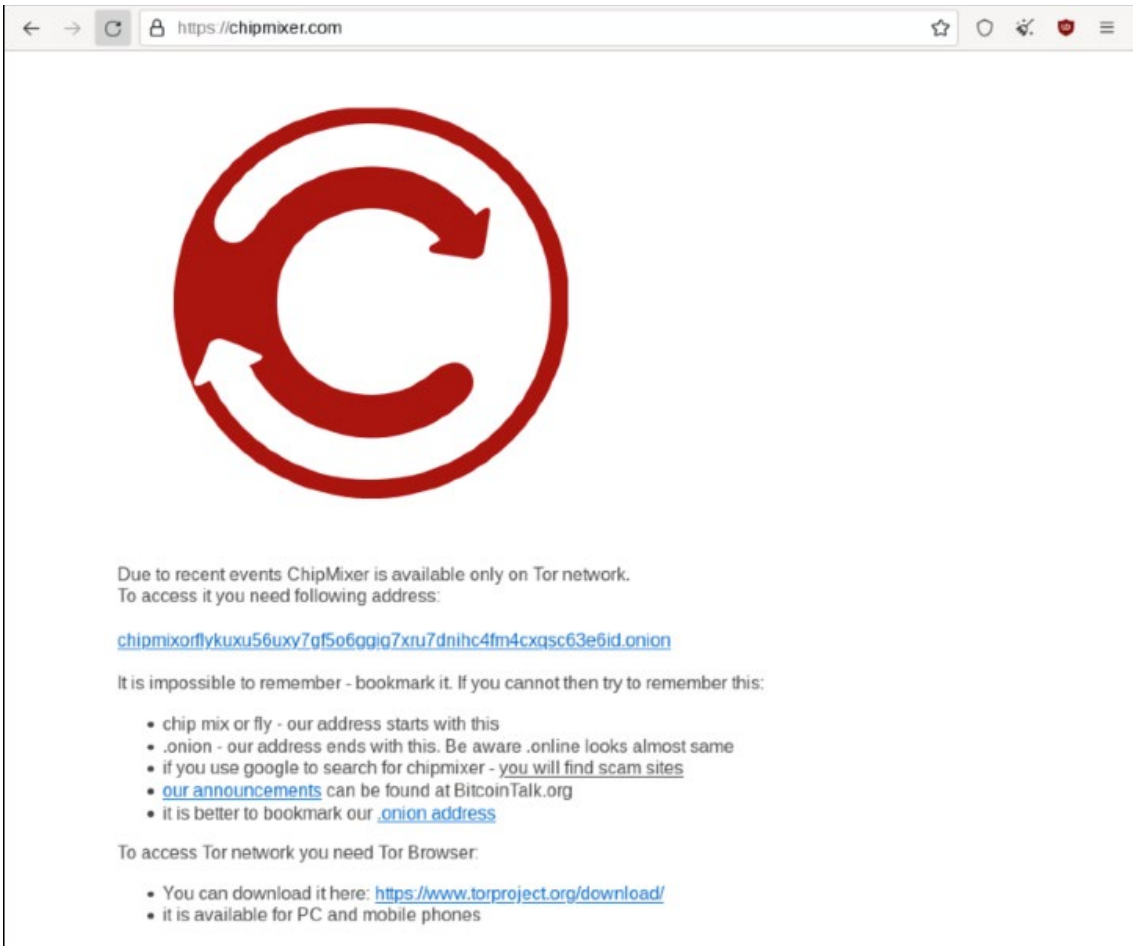

Figure 1: Screenshot of chipmixer.com clearnet website (as of March 10, 2023)

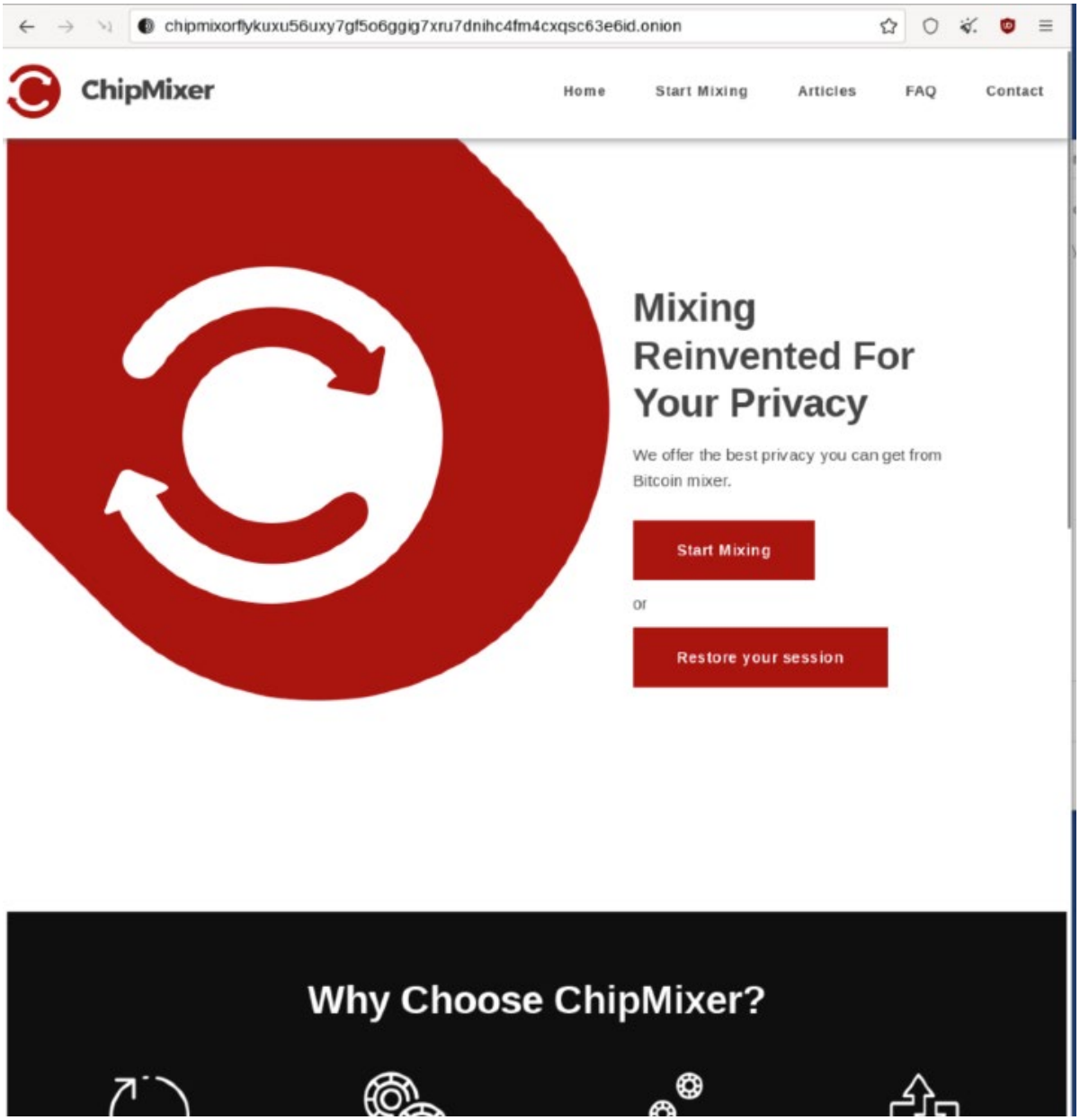

Figure 2: Screenshot of chipmixer.com Tor website (as of March 10, 2023)

10. The domain chipmixer.io was a functional part of the ChipMixer infrastructure in June 2018. However, in November 2018, the functionality was changed to point to

chipmixer.com exclusively. Currently, chipmixer.io does not have any functionality but is still registered to the same user at Namecheap, Inc., a web hosting company, as chipmixer.com.

11. The domain chipmixer.club was registered by the same user at Namecheap as the domains chipmixer.com and chipmixer.io in 2017 for one year. The domain chipmixer.club did have the same functionality as chipmixer.com but contained information forwarding users to an alternate Tor site. The domain chipmixer.club also provided a support email address of chipmixersupport@protonmail.com; whereas the chipmixer@protonmail.com email address is associated with chipmixer.com and the ChipMixer Tor site. According to Namecheap, chipmixer.club is suspended and could be reassigned to another user but is not currently available for registration.

12. In the Spring of 2022, chipmixer.com's webpage was stored at GitHub, an Internet hosting service for software development and version control. ChipMixer also utilizes a GitHub account called "ChipMixer" to promote its operation.

13. Between October 20, 2021, and October 22, 2021, an FBI agent accessed the ChipMixer website located at the domain chipmixer.com. The site describes itself as a bitcoin mixer with the ability to ensure the privacy of customers that wish to prevent the tracing of their Bitcoin transactions through blockchain analysis. The site details the three-step process for using the service:

a. First, the customer sends bitcoin they want to mix to ChipMixer and receives credits the site calls "chips." These chips correspond to pre-existing Bitcoin wallets controlled by ChipMixer. For example, if a customer sent 1 bitcoin to ChipMixer, they would receive several chips that have a combined value of 1 bitcoin.

b. Second, through the ChipMixer website, the customer can perform various optional operations on their chips such as splitting the chips into smaller sized chips, merging them together, or donating them to the ChipMixer service. ChipMixer recommends these actions to further obfuscate the mixing by adding additional customer-generated randomness into the transaction.

c. Finally, the customer withdrawals their chips, resulting in ChipMixer providing the private key to wallets that correspond to the chips. The customer can use this private key to spend the value associated with the wallet.

14. On its website, ChipMixer has a section called "Frequently Asked Questions" (FAQ). One section of the FAQ addresses customer privacy as follows:

> After you've received private key, you can spend them right away without waiting for our transaction. But that's not all. Since your withdrawal is not visible on blockchain, it looks like your chip was moved a few days before your deposit. Time Travel! Third, less spectacular element this method gives you is that you decide when to move those coins next. Few days? Who knows, you are not encumbered with our solution.

Based on my training and experience, ChipMixer is describing some of the privacy features that makes Bitcoin tracing nearly impossible after mixing funds through ChipMixer.

B. ChipMixer is an Unlicensed Money Transmitting Business

15. On October 31, 2021, an FBI Online Covert Employee (OCE) accessed the ChipMixer website from EDPA and used it to "mix" bitcoin. ChipMixer provided the OCE with a Bitcoin address to which to send funds. After the OCE sent funds to the designated address, ChipMixer gave the OCE access to chips that corresponded to the initial amount of credited bitcoin. The OCE directed ChipMixer to withdraw an equivalent balance of funds to another address controlled by the FBI, and ChipMixer did so. During the process, ChipMixer charged a

fee of approximately 2.44% of the total amount of mixed bitcoin. This fee was referred to as a "donation" during the mixing process. ChipMixer did not require the OCE to create an account and did not collect any identifying information about the OCE.

16. An FBI agent analyzed the OCE's activity on the blockchain and confirmed the OCE's initial deposit was sent from the OCE's Bitcoin address to an address controlled by ChipMixer. That FBI agent then verified that the withdrawal to the separate FBI-controlled address also originated from a different address controlled by ChipMixer. The deposit and withdrawal were not otherwise linked through blockchain analysis and had been obfuscated by the transfer through ChipMixer.

17. Based on the ChipMixer transactions on behalf of the OCE as described above, and other ChipMixer transactions I have studied during this investigation, NGUYEN has operated ChipMixer as a money transmitter in the United States. However, based on FBI's review of FinCEN's public website of registered Money Transmitting Businesses, ChipMixer has not registered with FinCEN.

18. Based on my training and experience, I am aware the Bank Secrecy Act requires anyone who owns or controls a money transmitting business to register with the United States Department of the Treasury. See 31 U.S.C. § 5330(a)(1). I am further aware that federal regulations issued pursuant to the Bank Secrecy Act define a "money services business," which include "money transmitter[s]." 31 C.F.R. § 1010.100(ff)(5). Money transmitters are defined broadly to include anyone who "accept[s] . . . currency, funds, or other value that substitutes for currency from one person and . . . transmi[ts] . . . currency, funds, or other value that substitutes for currency to another location or person by any means," as well as "[a]ny other person engaged

in the transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i)(A)-(B). MSBs are required to register with FinCEN, a division of the Department of the Treasury, unless specific exemptions apply. 31 C.F.R. § 1022.380(a)(1). MSBs are required to establish and maintain anti-money laundering programs, to detect and report suspicious transactions, and to collect certain records of customers and customer transactions. I am further aware that bitcoin "mixers" or "tumblers" such as ChipMixer are considered to be MSBs under federal law. *See* U.S. Department of Treasury FinCEN Guidance, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 9, 2019), at 19-20. Specifically, ChipMixer's business model involves ChipMixer accepting bitcoin from users and then transmitting "clean" bitcoin to new wallets for users' onward transfer and use.

19. In recent years, many of ChipMixer's competitor bitcoin mixing services have been shut down by United States and European law enforcement due to criminal money laundering investigations and indictments of mixing service operators. For example, in May 2019, the mixer Bestmixer.io was seized by European law enforcement after it laundered $200 million in cryptocurrency. In April 2021, the mixing service BitcoinFog ceased operation after its alleged operator was arrested and charged with violations of 18 U.S.C. §§ 1956 and 1960. In August 2021, the operator of the darknet mixing service Helix pleaded guilty to violations of 18 U.S.C. § 1956 for laundering over $300 million in cryptocurrency. Following these seizures, ChipMixer assumed the illicit market share and continued to grow in popularity among criminals. As of November 2021, ChipMixer was one of the most widely used mixers to launder criminally derived funds.

C. Blockchain Analysis of ChipMixer

20. The FBI has a contract with a blockchain tracing and analytics company referred to herein as "Company A." Company A provides services to government agencies and private firms allowing for the tracing of cryptocurrency payments. Company A helps track the public movements of cryptocurrency across the public blockchain ledger. Company A has tracked approximately 118,500 bitcoin addresses associated with ChipMixer. The FBI confirmed the ChipMixer addresses involved in FBI's undercover transactions described above were included in Company A's cluster of ChipMixer addresses, verifying the cluster. According to Company A's tracing platform, from August 2017 to March 2023:

a. ChipMixer received 153,732 bitcoin and sent 153,672 bitcoin. Based on the value of bitcoin at the time of the transactions, ChipMixer processed $3 billion worth of transactions.

b. Chipmixer received $185 million and sent $17 million in bitcoin that was directly or indirectly associated with wallets designated as darknet marketplaces.

c. ChipMixer received $35 million and sent $670,000 in bitcoin that was directly or indirectly associated with wallets designated as fraud shops.

21. The FBI has traced ransomware proceeds associated with 37 different ransomware groups to identify the services that ransomware actors used for money laundering. Through this analysis, the FBI found that from August 2017 to March 2023, $17 million in bitcoin was transferred to ChipMixer – directly or indirectly – from wallets associated with ransomware payments. Of this amount, $821,000 in bitcoin was from "Sodinokibi" ransomware wallets, $713,000 in bitcoin was from "Mamba" ransomware wallets, and $2.5 million in bitcoin

was from "Suncrypt" ransomware wallets. Sodinokibi, Mamba, and Suncrypt are all significant ransomware variants that have caused significant damage to victims in the United States and abroad. These victims include hospitals, healthcare service providers, major corporations, and municipal governments. According to the FBI's analysis, ChipMixer was one of the most popular mixing services used by ransomware operators to obfuscate and launder the ransoms paid by victims.

22. Using information reported to FBI from companies victimized by ransomware, numerous specific ransomware payments have been traced through ChipMixer. For example:

a. In May 2021, a manufacturing company was infected with ransomware. The victim paid the attackers worth $11 million in bitcoin in order to recover the victim's systems. Using Company A's bitcoin tracing platform, it was identified that $23,000 in bitcoin of this ransom was sent to ChipMixer.

b. In August 2020, a municipal government was infected with ransomware. This municipality paid the attackers $42,500 in bitcoin in order to recover their systems. Using Company A's bitcoin tracing platform, an agent identified this ransomware payment was sent from the ransom wallet directly to ChipMixer.

23. ChipMixer is also a popular platform for hackers seeking to launder stolen cryptocurrency. I am aware that insecure bitcoin exchanges and cryptocurrency services are commonly hacked, and large amounts of bitcoin are stolen. Stolen bitcoin needs to be "washed" or "mixed" before it can be cashed out at a bitcoin exchange. It is common for hackers to launder stolen bitcoin using mixing services such as ChipMixer. According to Company A's tracking platform, from August 2017 to March 2023, ChipMixer received $721 million and sent $2

million in bitcoin that was directly or indirectly associated with wallets designated as "stolen funds."

24. Funds from several high-profile bitcoin exchange hacks were laundered through ChipMixer. For example:

a. In September 2020, a Singapore-based bitcoin exchange platform disclosed that hackers had stolen over 1,000 bitcoin, then worth $150 million, from the bitcoin exchange platform. In a post to the popular bitcoin message board BitcoinTalk on July 13, 2021, the user "ChipMixer" confirmed the bitcoin exchange platform hackers had "unfortunately" used the ChipMixer service.

b. In May 2019, another major bitcoin exchange platform disclosed hackers had stolen 7,000 bitcoin, worth $40 million at the time. Multiple groups of private sector researchers, specializing in blockchain analysis, traced the funds and independently determined the largest recipient of the funds was ChipMixer.

25. Hydra was a Russian language darknet marketplace that facilitated the sale of illicit items such as narcotics, stolen personal identifying information, malware, hacking services, forged documents, and counterfeit currencies. Hydra allowed buyers to purchase these items using cryptocurrencies, such as bitcoin. The FBI has learned of significant funds traced from Hydra to ChipMixer. According to Company A's tracing platform, as of March 2023, Hydra users conducted over 5,583 transactions directly with ChipMixer, and sent over $37 million worth of bitcoin from Hydra's wallets to ChipMixer. When including funds sent indirectly from Hydra to ChipMixer – for example, funds transferred from a drug vendor's

account on Hydra to the vendor's personal wallet and then on to ChipMixer for laundering – that sum grows to $121 million in bitcoin sent to ChipMixer from Hydra.

26. Through FBI investigations, I have learned that numerous actors – both criminal and nation-state – have utilized ChipMixer's services to launder or obfuscate their funding streams. For example:

a. The Russian Intelligence Services, specifically the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center, military unit 26165 (a/k/a APT28), used ChipMixer to obfuscate the origin of the funds that were used to purchase infrastructure for their "Drovorub" malware.

b. On December 8, 2020, a grand jury in the Central District of California returned an indictment against three members of the Reconnaissance General Bureau ("RGB"), a North Korean military intelligence agency. The three RGB members were charged with being part of a group of North Korean cyber-actors known within the cyber-security community as the Lazarus Group and Advanced Persistent Threat 38 ("APT38"). Lazarus Group and APT38 were charged in a long running conspiracy to commit criminal cyber intrusions, bank, and cryptocurrency heists on behalf of the North Korean regime. One of the charged heists was the August 2020 theft of $11.8 million in cryptocurrency from a victim in New York. The FBI's investigation into the laundering of those funds shows that some of the stolen funds were laundered via Chipmixer. Since that time, Lazarus Group/APT38 have committed additional cryptocurrency heists. In March 2022, over $600 million in Ether was stolen from Axie Infinity's Ronin Bridge, and in June 2020, over $100 million of virtual assets were stolen from Harmony's Horizon Bridge. The FBI has investigated those heists and, in both instances,

determined that Lazarus Group/APT38 was responsible, and made public attribution statements to that effect. The FBI's investigation also shows that the North Korean actors used ChipMixer to launder funds stolen from both Axie Infinity and Harmony.

D. NGUYEN's Efforts to Conceal His Identity and Activities

27. NGUYEN, as the operator of ChipMixer, has gone to great lengths to conceal his true identity and location. ChipMixer maintains a clearnet domain at chipmixer.com, but currently does not have any functionality other than to display a page that directs users to use ChipMixer's Tor-based .onion address. In my training and experience, and as outlined above, anonymization tactics, such as using Tor, are used to make it difficult for law enforcement to track and attribute online activity to specific users. Until May 2022, chipmixer.com was a functional clearnet website that was hosted at a U.S. virtual private server (VPS) provider, DigitalOcean.

28. During the course of the investigation, the FBI has obtained business records from various third-party services used by ChipMixer. These records show that NGUYEN concealed his identity by employing pseudonyms and anonymous email providers such as ProtonMail and India.com. For example:

a. ChipMixer's domains were registered using the name "James Hall," the address 6 Nariman Point, Mumbai, India, and the email address jhall@india.com.

b. ChipMixer set up an account at a hosting provider using the name "Max Archdall." This account leased servers using a PayPal account associated with the name "Max Archdall" and the mailing address 5 Myrtle Street, Merrijig, Australia. Based on FBI database checks and open-source research, this is a fictitious address in Australia.

c. ChipMixer set up another account at a hosting provider using the name "Ronald Boatwright," the address Saharova 41, Riga, Latvia, and the email address rboat77@protonmail.com. ChipMixer used the same fictitious information to set up a PayPal account to pay the hosting provider.

29. The Department of Homeland Security, Homeland Security Investigations (HSI) is also investigating ChipMixer. An HSI special agent attempted to contact ChipMixer's support email address at chipmixer@protonmail.com. However, ChipMixer never responded to HSI's contact. Based on my training and experience, companies which are not engaged in illegal or illicit activity respond to law enforcement contacts or at least direct law enforcement to local authorities if they are not located in the United States. Operators of legitimate financial businesses typically do not attempt to operate their services anonymously and do not use fictitious personas when engaging in legal activities.

E. NGUYEN's Public Posts as "ChipMixer"

30. As explained further below, NGUYEN used the moniker "ChipMixer" on the popular bitcoin message board BitcoinTalk (available at bitcointalk.org). On May 18, 2017, NGUYEN, as "ChipMixer," posted (or caused to be posted) to BitcoinTalk that he was looking for testers for a new bitcoin mixing service. On May 26, 2017, NGUYEN announced in a new thread that he was "Introducing ChipMixer," which he described as "Mixing reinvented for your privacy." Since then, "ChipMixer" has made over 400 posts to BitcoinTalk, the majority of which involve addressing questions about ChipMixer. As of March 2023, NGUYEN's "ChipMixer" account was still active on BitcoinTalk. Further, since May 15, 2017, NGUYEN, using the moniker "chipmixer," has been on the social media platform Reddit, and promoted, or

caused to be promoted, ChipMixer as a mixing platform.

31. NGUYEN frequently posts to both BitcoinTalk and Reddit promoting ChipMixer as a way to conceal bitcoin transactions. In a November 15, 2017 post to BitcoinTalk, NGUYEN advised, "If you want to hide who you are then ChipMixer is a perfect way." In one post explaining the benefits of ChipMixer, NGUYEN offered the following analogy:

> There were 10 people in a room when victim was killed. Each witness has 1/10 chance to be a murderer. We know that one of the ten people who was inside is [user]. … Does that mean we should throw him into jail?

I understand this post to be drawing a parallel to ChipMixer's process of co-mingling users' bitcoins, such that even if law enforcement could determine that someone had used ChipMixer, it would be impossible to connect that user to a specific illegal transaction with any certainty.

32. Throughout posts to BitcoinTalk and Reddit, NGUYEN indicated a familiarity with U.S. anti-money laundering laws while cautioning users against using compliant cryptocurrency exchanges. NGUYEN cautioned readers that "AML/KYC is a sellout to the banks and governments" and repeatedly advised, "please do not use AML/KYC exchanges." I know that "AML" is a common shorthand for "Anti-Money Laundering," which are measures carried out by financial institutions and other regulated entities to prevent financial crimes. I also know that "KYC" is a common shorthand for "Know Your Customer," which is the process that a financial institution uses to obtain information about a customer and verify their identity. KYC falls within AML measures. Additional posts by NGUYEN include:

a. In 2017, NGUYEN commented on a Reddit post regarding the popular U.S.-based exchange Coinbase providing records to the IRS: "That's what KYC exchanges lead to. All your data will be shipped to IRS." Based on my training and experience, I believe that

NGUYEN is referring to the Internal Revenue Service when referencing the "IRS."

b. In June 2017, NGUYEN published a post on Reddit explaining how to use ChipMixer to evade potential cross-border reporting requirements. The post was titled, "Easy way to avoid upcoming US 'declare bitcoin' law."

c. On June 15, 2017, NGUYEN responded to a BitcoinTalk post criticizing money laundering laws and know-your-customer requirements, stating,

> If your money is in a bank, it's like bitcoin on exchange - you don't have private keys. It can be frozen, it can be traced, it can be watched very carefully.
>
> If you have cash, you can do whatever you want. Nobody can invalidate it. Nobody can track it. Except police that can take it from you.
>
> Bitcoins are better. Nobody knows you have it (unless you use KYC exchange), you can exchange it for cash wherever you want.

d. On June 29, 2017, NGUYEN posted a comment regarding the U.S. arrest of the administrator of btc-e, a criminal cryptocurrency exchange. The administrator was charged by a federal grand jury in the Northern District of California in a 21-count indictment alleging the platform laundered over $4 billion worth of cryptocurrency. NGUYEN wrote, "Their admin was arrested because they did not implement Know Your Customer AKA Spy On Your Users procedure and your money was stolen by government." NGUYEN further opined, "Non-KYC exchanges should be trusted. KYC exchanges should not because they are working with governments."

e. On October 6, 2017, NGUYEN posted to BitcoinTalk that, "'Money laundering' is a crime made-up by governments that spy on their citizens."

33. While ChipMixer was experiencing DDoS attacks in September and October 2017, NGUYEN posted to BitcoinTalk explaining why he did not use Cloudflare, a popular

counter-DDoS platform, stating, "In our case, if we would use Cloudflare, Cloudflare would know input addresses and private keys. Cloudflare is US company so it is reasonable to think that any three letter institution could get an access by court order."

F. Details of the Investigation

i. The "James Hall" Persona

34. One of the alias accounts used by NGUYEN to conceal his criminal conduct was "James Hall." Records provided by Namecheap revealed the domain "chipmixer.com" was registered on July 7, 2016. Records revealed the subscriber information for the account was "James Hall," physical address 6 Nariman Point, Mumbai, India, and email address jhall@india.com. FBI database checks and open-source research revealed that address 6 Nariman Point, Mumbai, India is fictitious. Records also revealed the account was logged in numerous times from IP address 45.76.91.219. Open-source research conducted on IP address 45.76.91.219 revealed it resolved to Vultr Holdings. On ChipMixer's website, ChipMixer displayed a point-of-contact as chipmixer@protonmail.com.

35. An international records request for the chipmixer@protonmail.com account revealed there were two accounts linked to the email address chipmixer@protonmail.com: jhallindia@protonmail.com and max.archdall@protonmail.com. Records provided by Namecheap for "chipmixer.com" also revealed the subscriber "James Hall" also registered the domains "chipmixer.io" and "chipmixer.club" on April 27, 2017. A follow-up records request to Namecheap for chipmixer.com revealed that, on December 11, 2019, a login occurred from IP address 45.77.64.64. Open-source research conducted on IP address 45.77.64.64 revealed this IP address resolved to Vultr Holdings. A follow-up records request to Namecheap for

chipmixer.com and chipmixer.io provided a new email address, jhallindia@protonmail.com, for the "James Hall" account.

ii. The "Max Archdall" Persona

36. Another alias account used by NGUYEN to hide his involvement in ChipMixer was "Max Archdall." Records provided by Vultr Holdings for IP address 45.76.91.219 revealed the account was created on April 4, 2017, with the name "Max Archdall," email address max.archdall@gmail.com, and creation IP address 45.76.119.17. The form of payment included both BitPay and PayPal. (Open-source research conducted on IP address 45.76.119.17 revealed this IP address also resolved to Vultr Holdings.) Vultr records revealed that IP address 45.76.91.219 was leased on April 27, 2017. Vultr records also identified two other IP addresses that were leased by the "Max Archdall" account: IP address 45.77.64.64 was leased on September 21, 2017 and IP address 45.76.89.113 was leased on May 11, 2017. Vultr identified the following logins: January 10, 2019 a login occurred from IP address 185.220.101.6, January 10, 2019 a login occurred from IP address 137.74.169.241, and May 23, 2019 a login occurred from IP address 109.70.100.18. Open-source research conducted on these three IP addresses revealed that all three served on Tor relays on the dates of those logins.

37. Records provided by Google for the max.archdall@gmail.com account revealed the account was created on March 29, 2017, with the name "Max Archdall" with a Terms of Service IP address of 45.76.119.17. PayPal records relating to max.archdall@gmail.com revealed that the PayPal account was created on March 29, 2017 with the name "Max Archdall," address 5 Myrtle Street, Merrijig, Vic, Australia 3723, and listed a PayPal Account ID

1356241556304782540. As noted above, the address 5 Myrtle Street, Merrijig, Vic, Australia 3723 is fictitious.

iii. The "Ronald Boatwright" Persona

38. A third alias account used by NGUYEN to hide his involvement in ChipMixer was "Ronald Boatwright." Records provided by Vultr Holdings for IP address 45.76.119.17 revealed the account was created on March 17, 2017, with the name Ronald Boatwright, email address rboat77@protonmail.com, and address Saharova 41, Riga, Latvia. Analysis of the payments to Vultr Holdings by Boatwright identified PayPal as the primary payment method utilized to fund the account.

iv. ChipMixer – IP Address 46.101.124.25

39. According to public records, from September 2021 to March 2022, chipmixer.com was hosted at IP address 46.101.124.25. According to Namecheap records, the IP address 46.101.124.25 was used by the account subscriber to log in on September 7, 2021, and September 25, 2021. Open-source research conducted on IP address 46.101.124.25 revealed that it resolved to DigitalOcean. Records provided by DigitalOcean for this IP address revealed that DigitalOcean "Droplet" (a type of virtual machine) 46.101.124.25 was created by a company called SporeStack on September 8, 2021. Open-source research conducted on SporeStack revealed it is a server reseller, purchasing server space at multiple providers and then reselling that server space to SporeStack customers. SporeStack allows customers to obtain Droplets from DigitalOcean while paying with cryptocurrencies such as Bitcoin and Monero, which DigitalOcean does not accept directly.

v. DigtalOcean/Tor Analysis

40. On November 23, 2021, the FBI served a federal search warrant to DigitalOcean for chipmixer.com, which was located at the IP address 46.101.124.25. DigitalOcean provided the FBI an image of the server. FBI analysis of this server image revealed that it contained minimal information about the administrators, customers, or operations of ChipMixer, and it pointed traffic to a ChipMixer Tor server.

41. Through the course of the investigation, and working in partnership with foreign law enforcement, the FBI identified that another ChipMixer server resolved to IP address 138.201.227.85, hereinafter the "V3 Server." Open-source research conducted on IP address 138.201.227.85 revealed the IP address resolved to Hetzner Online GmbH (Hetzner) in Germany.

vi. The "V3 Subscriber" Persona

42. Records received from Hetzner revealed the individual identified as the subscriber for IP address 138.201.227.85, hereinafter the "V3 Subscriber." The V3 Subscriber was a stolen identity used by NGUYEN to hide his involvement in ChipMixer. The records listed a ProtonMail account, a Google account, and a phone number with a country code of +48 associated with the V3 Subscriber. I have learned that +48 is the country code for Poland.

43. Records provided by Google for the Google account associated with the V3 Subscriber revealed the same name as the V3 Subscriber's name for IP address 138.201.227.85 at Hetzner, an account creation date of March 20, 2021, a recovery phone number with a country code of +380, and Terms of Service IP address which resolved to Ukraine. I have learned that +380 is the country code for Ukraine.

44. On October 12, 2022, the FBI served a federal search warrant to Google for an account which was associated with the V3 Subscriber. The search warrant returns revealed the Google account controlled by the V3 Subscriber received an email from Hetzner on March 20, 2021, confirming the creation of an account at Hetzner.

45. Records provided by PayPal for the V3 Subscriber revealed a PayPal account with ID 2174339753411285516, hereinafter "V3 PayPal Account." Analysis of the V3 PayPal Account's transaction logs identified monthly payments starting in July 2021 being sent from the V3 PayPal Account to Hetzner, which controlled the ChipMixer Tor server, the V3 Server.

46. Transaction log activity for the V3 PayPal Account identified payments to the account from other accounts. I have listed these other accounts below, listing only initials for stolen identities:

Name	Email Address
[M.W.]	Kfhchcgchg01@gmail.com
[R.H.]	ovofoeoskzqnajwkso16@gmail.com
[M.S.]	Agxgxhchch03@gmail.com
[D.N.]	bengocproekdnekqwksk2@gmail.com
[D.P.]	dpine2020h@aol.com
[K.C.]	kcrewell01@yahoo.com
[B.F.]	djekrntofroekskewjjsskkw1@gmail.com
[D.S.]	dschmelper2h@aol.com
[E.O.]	salesequalsone21@outlook.com
MINH NGUYEN	nqminh73@yahoo.com
[R.G.]	rgoodwin2020h@outlook.com
[R.S.]	rsaggio2020h@aol.com

47. Open-source research conducted on the above accounts revealed the identifying information associated with the accounts are primarily United States-based persons, approximately 60-70 years old, except for the account associated with MINH NGUYEN. Commercial database research revealed that some of these persons are deceased. Based on my

training and experience, I believe that NGUYEN stole these individuals' identities to obfuscate their illegal activity and facilitate money laundering.

48. PayPal transaction logs revealed that the above accounts transmitted money between each other. Additionally, these accounts also shared numerous common recipients and senders of PayPal transactions over the life of the accounts. Moreover, PayPal activity logs for these accounts revealed that several IP addresses were common across the accounts. The IP address 107.175.87.18 was identified on seven of the 12 PayPal account activity logs. Open-source research conducted on IP address 107.175.87.18 revealed that it resolved to ColoCrossing. Records provided by ColoCrossing for IP address 107.175.87.18 revealed the IP address was subleased by a subscriber called Virtual Machine Solutions, LLC.

49. The PayPal account with the name "MINH NGUYEN," email address nqminh73@yahoo.com, account ID 1706782211073221952, was the only PayPal account not associated with a U.S.-based identity and associated with an actual bank account on the V3 PayPal Account payments received transaction logs.

50. Further, PayPal transaction logs related to the accounts listed in the table above revealed there were transactions with approximately 70 different users with ProtonMail accounts. The FBI submitted international records requests for subscriber data for these ProtonMail accounts. I believe that NGUYEN used these ProtonMail accounts to continue to obfuscate his control of ChipMixer. Of these accounts, 24 of them listed jamessmithhelp@gmail.com as a recovery email address and nine listed minhoba@ymail.com as a recovery email address.

51. According to PayPal records for the V3 PayPal Account, on December 27, 2022, there was a credit card payment received from MINH NGUYEN, email address

nqminh73@yahoo.com for $150.00 with the comment "Thanks." This transaction demonstrates the fact that NGUYEN is utilizing a personal payment method to fund operational ChipMixer infrastructure.

vii. MINH QUOC NGUYEN

52. Records provided by PayPal for nqminh73@yahoo.com revealed the account was associated with the name "Minh Quoc Nguyen," date of birth October 21, 1973, phone number +84982468445, an address in Hanoi, Vietnam, and a checking account at the Joint Stock Commercial Bank for Foreign Trade of Vietnam. I have learned that +84 is the country code for Vietnam.

53. On August 2, 2022, the FBI obtained an Order pursuant to 18 U.S.C. § 2703(d) for the accounts kcrewell01@yahoo.com and nqminh73@yahoo.com. As noted above, [K.C.] is an alias of NGUYEN to help hide his involvement in the ChipMixer scheme. The kcrewell01@yahoo.com account listed the name [K.C.] as the subscriber, jamessmithhelp@gmail.com as the recovery email address, +233263349724 as the phone number, and +84982468445 as the recovery phone number. The recovery email and recovery phone for kcrewell01@yahoo.com were added via IP address 107.175.87.18 on February 7, 2022. The nqminh73@yahoo.com account listed the name Minh Nguyen Quoc as the subscriber, spookylumusic@protonmail.com as the recovery email address, and the same +84982468445 as the recovery phone number. Yahoo also provided all accounts linked by SMS telephone number +84982468445, which included kcrewell01@yahoo.com, nqminh73@yahoo.com, minhoba@ymail.com, and minhoba@yahoo.com.

54. Records provided by Yahoo for minhoba@ymail.com and minhoba@yahoo.com

revealed the minhoba@ymail.com account listed the name "Minh Nguyen Quoc" as the subscriber, nqminh21@gmail.com as the recovery email address, +84436419503 as the phone number, and again +84982468445 as the recovery phone number. The Yahoo returns also revealed the minhoba@yahoo.com account listed the name "Nguyen Minh" as the subscriber, nqminh21@gmail.com as the recovery email address, and again +84982468445 as the recovery phone number.

55. On October 12, 2022, the FBI served a federal search warrant to Yahoo for the account minhoba@ymail.com. The results revealed an email was received on September 23, 2018, from Virtual Machine Solutions, LLC which described the user of minhoba@ymail.com had leased a server with IP address 107.175.87.18 and provided billing information for the server.

56. On October 12, 2022, the FBI served a federal search warrant to Google for the account jamessmithhelp@gmail.com. James Smith was an alias account used by NGUYEN to hide his involvement in ChipMixer. The jamessmithhelp@gmail.com account listed the name "Smith James" as the subscriber and minhoba@ymail.com as the recovery email address. Google records revealed a June 21, 2022, email from Bitify, a Bitcoin and Litecoin marketplace and auction site, which described a payment of 0.00455231 bitcoin to the account for the item "Bitcoin to PayPal – Pay $100 get 110$ in PayPal" by a user whose moniker is the same as the last name of the V3 Subscriber from Hetzner. According to PayPal records, on June 21, 2022, the V3 PayPal Account received $110 from PayPal account [M.W.], email address kfhchcgchg01@gmail.com.

57. Records from Google for the account jamessmithhelp@gmail.com revealed

location history data. From September 2016 through March 2022, there were 149,027 data points associated to the account that resolved in and around Ha Noi, Vietnam. The location history data is a combination of different sources to include cell, GPS, and Wi-Fi, showing that NGUYEN was physically in Vietnam during these data points.

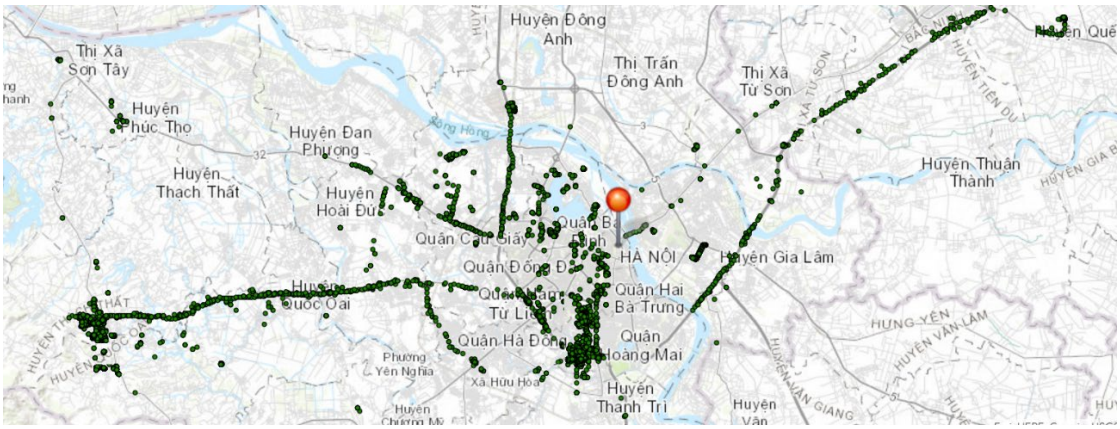

Figure 3: Location Data

58. Records from Google for the account jamessmithhelp@gmail.com revealed an email was received on February 28, 2019, from Bitify describing a payment the account had received for 0.02429444985 bitcoin for the item "Bitcoin To PayPal – Pay $100 get 105$ in PayPal." This payment would be sent to the nominated Bitcoin address 15Nu61zbR1z8tMf6KrD8ekW7mVnhC1c6b2.

59. Search warrant returns from Google for jamessmithhelp@gmail.com revealed searches by NGUYEN for ways to buy personally identifiable information (PII) such as Social Security Numbers (SSN) and date of birth (DOB) records as well as generators that provide randomized PII. For example, the following Google searches were conducted:

a. March 18, 2018: "where to search for ssn free by name"

b. November 19, 2019: "selling ssn dob"

c. July 11, 2022: "ssn dob shop"

d. October 12, 2022: "ssn number generator"

60. In addition, search warrant returns from Google revealed an email received on June 10, 2022, from Premium Technologies (Premium RDP) describing an invoice payment confirmation for certain servers which were leased by the jamessmithhelp@gmail.com account, including the IP addresses 185.127.92.163 and 45.42.200.243. Open-source research conducted on Premium RDP revealed it to be a web-hosting provider that specializes in dedicated server hosting and cloud server services located in the United Kingdom. Open-source research confirmed that RDP stands for "remote desktop protocol," which allows a user to connect from one computer to another computer over a network connection.

61. Search warrant returns for jamessmithhelp@gmail.com revealed that NGUYEN possessed emails which had attachments containing hundreds of email addresses, passwords, stolen identities, credit card numbers, and other personal information. For example, on June 8, 2022, jamessmithhelp@gmail.com sent an email to decrestseo@gmail.com with attachments containing images of driver's licenses of various U.S.-based individuals and the subject line of "Fwd: Info for doc making." FBI database checks revealed the driver's license documents attached to this email were all fraudulent. The body of the email referenced above states,

> Here is the info for the Doc:
>
> Full Name:
> [Victim K.K.]
> Address:
> [A real address in Milwaukee, Wisconsin]
>
> You can make the DOB random.
> Attached are some samples/templates. You can use them if you need.
> You can make Driver license or passport

62. Binance provided records relating to jamessmithhelp@gmail.com, which revealed an account associated with the following identifiers:

Name: MINH QUOC NGUYEN
Phone: +84982468445
Email: jamessmithhelp@gmail.com
Date of Birth: 10/21/1973

Pursuant to KYC verification requirements, NGUYEN supplied Binance with an identification card issued by the government of Vietnam, as pictured below:

Figure 4: Binance KYC – Picture ID Front

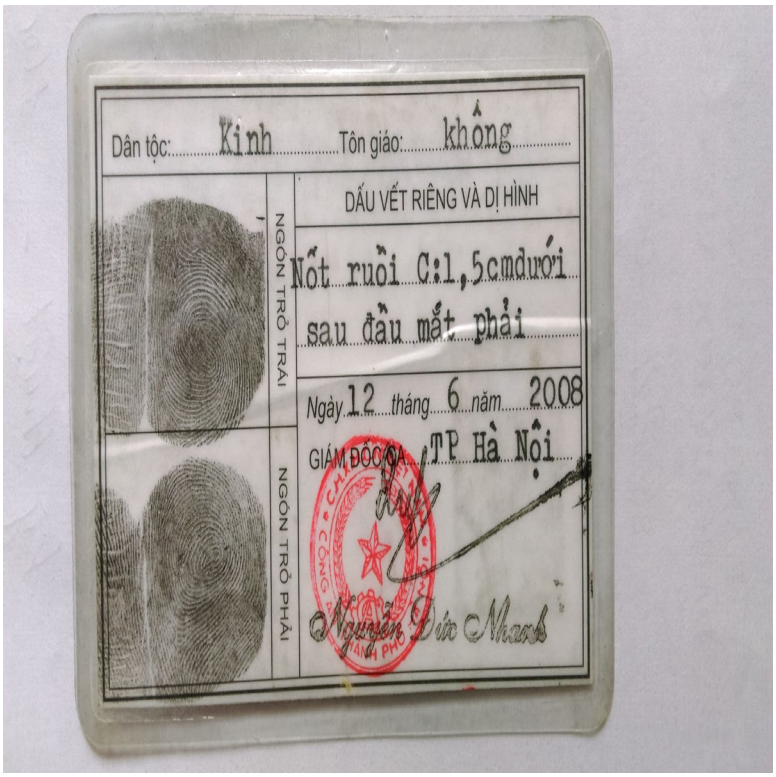

Figure 5: Binance KYC – Picture ID Back

63. Records provided by Binance for jamessmithhelp@gmail.com also revealed the following assets and wallets associated with the account:

Asset Name	Wallet Address
Bitcoin	1BFFuA1naxhQjJxdoJ5LCx3Za4dfZ8uKjk
BNB	bnb136ns6lfw4zs5hg4n85vdthaad7hq5m4gtkgf23
Ethereum	0xf2dca3ddeec78dae2c9cc7686a1f46cab38b2cf8
Litecoin	Ld1dYiBhTFkcK8ZcKD5UJ46F2ubZsAEhJP
Polkadot	127D6hMbhqXspbopf147DQ91hmxSA1ZTe7bXyuMHQnC5NrqF
Ripple	rEb8TK3gBgk5auZkwc6sHnwrGVJH8DuaLh
TetherUS	1LWWrCFKwJLVCQqK92g8HavcxzUjUJJiwV
TRON	TQ9xHTP8gv3QuwdrH3D2LMpZCPqcX9SdYG

64. FBI research determined that Bitcoin address 15Nu61zbR1z8tMf6KrD8ekW7mVnhC1c6b2 used by NGUYEN is associated with over 80 other Bitcoin addresses due to "co-spending" (where multiple lesser-value addresses are used to fund a higher-value transaction) with each other in different transactions, indicating they are in the same wallet, which is referred to as a "cluster." This cluster of Bitcoin addresses sent bitcoin to Remitano 25 times to five specific deposit addresses. Open-source research conducted on Remitano revealed that Remitano is a P2P Bitcoin marketplace for buying and sell bitcoin. Records provided by Remitano for those transactions revealed an account used by NGUYEN with the username "hotpassion." The records also revealed the following Bitcoin addresses associated with the account:

Bitcoin Address
371uxD2XEoswUE5HbuQrZdVh83wxKTRNgJ
37GUdRq2WuNR6akW6Z1eK8X1fWQ9XtyftJ
3Efpc3iVGF1m5nkSvms3qGDz3zJNQ3iEkA
3HiQ5fmhuLjxeKT33XMTf5k8EEsn7jBZLe
3J3V7BMpkscXmbFyUh9wXQHwGM4JTqqtE7
3KX2GoWNGRpdzsdX1R7FiQmBDJgjdFYS2W
3L2VQG9q1iZqv1SFJ4RS5KXaBpZ5p4sgRS

3NmkLpMEFv8RfAqdvRCcSY9997FgF9ntaf
3Nnxwus1oUk52ktxGJHKFiHi1mun2SMjSu
3PjqtRvWE5UD5p4uEAHDowEgPmXX6UKR6J
3QqxuFFsFQraQdknXjoXkEnU12pR9Hj8YV

The records from Remitano also revealed KYC ("Know Your Customer") information including a picture of an individual resembling NGUYEN holding an identification card with the name MINH QUOC NGUYEN and date of birth 10/21/1973. Also included as part of the KYC is a Vietnamese passport (Figure 6) with a picture (Figure 7) resembling the individual in the Binance KYC picture (Figure 4), with the name of MINH QUOC NGUYEN and date of birth 10/21/1973. Also, the picture ID being held in Figure 7 is the same picture ID provided to Binance (Figure 4). The bank account associated is an account at Vietcombank in Vietnam:

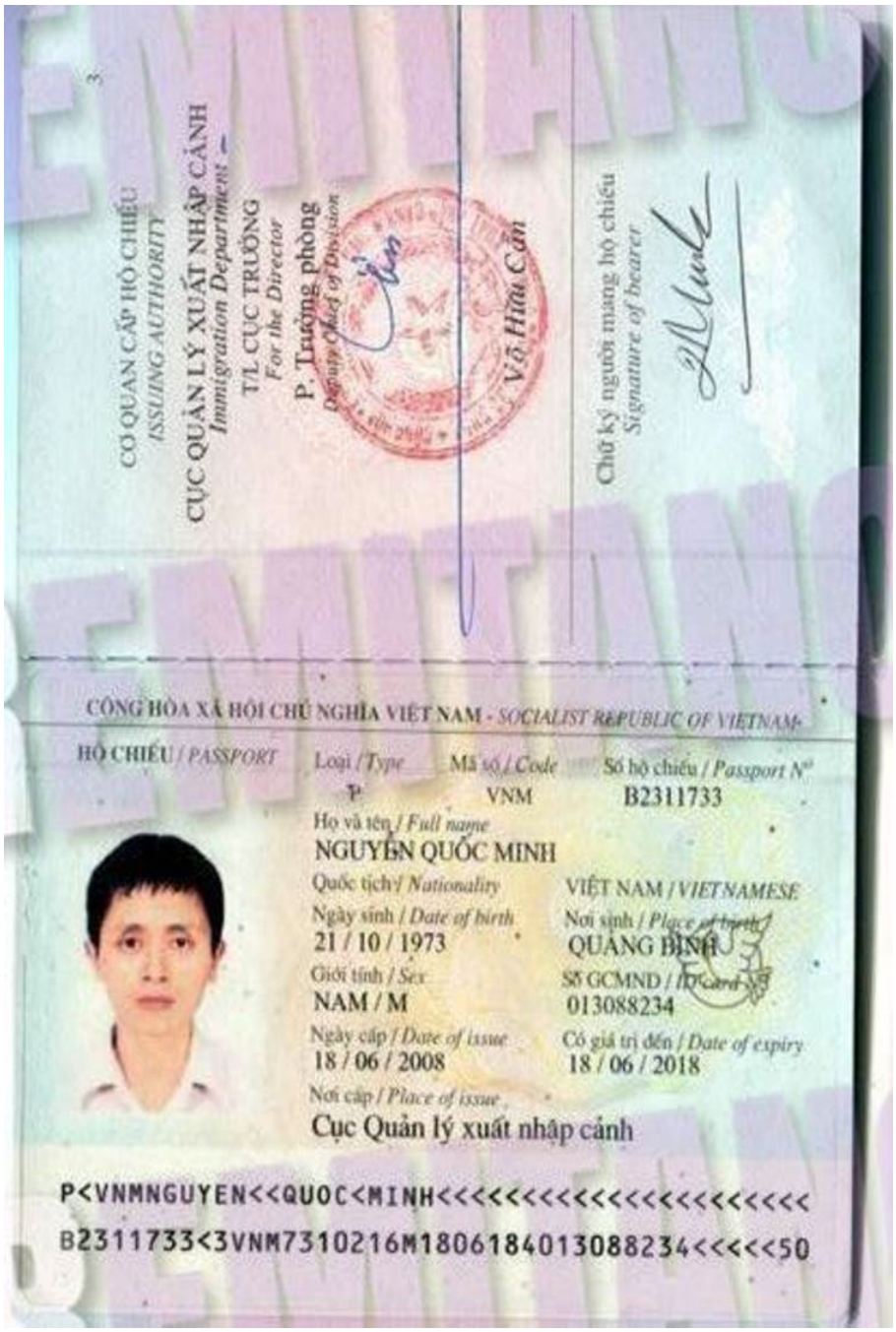

Figure 6: Remitano KYC - Passport

Figure 7: Remitano KYC – Photograph with Picture ID

65. Google records for nqminh21@gmail.com revealed an account that listed date of birth 10/21/1973, recovery email address minhoba@ymail.com, recovery SMS phone number +84982468445, and Terms of Service IP address 58.186.28.118. Open-source research conducted on IP address 58.186.28.118 revealed it resolved to FPT Telecom Company in

Vietnam.

66. On October 12, 2022, the FBI served a federal search warrant on Google for nqminh21@gmail.com. The returns revealed the account received email notifications from several companies, including, but not limited to, Paxful, LocalBitcoins, Binance, LinkedIn, Reddit, PayPal, and Facebook. Google search warrant returns also revealed emails from Paxful on May 23, 2020, showing that an account was created with the name "Bui Thi Nhung," moniker "Newstar2021," and a completed ID verification process. The returns also provided notification emails from Paxful in which NGUYEN was trading PayPal funds for bitcoin on numerous occasions.

67. Google returns for nqminh21@gmail.com further revealed that an account was created on May 24, 2020 at LocalBitcoins with the moniker "Newstar2021" and a confirmation of account verification notifications from the company. The returns provided notification emails from LocalBitcoins in which NGUYEN bought bitcoin in exchange for U.S. dollars, which I believe NGUYEN used to continue to fund ChipMixer's operations.

68. The Google returns for nqminh21@gmail.com also revealed an April 20, 2021 email from Binance which confirmed registration for an account. NGUYEN had 1000 USDT deposited into his Binance account on the day of its creation. ("USDT" is a cryptocurrency called "Tether," which functions as the Internet's Digital Dollar, with each token worth $1.00 USD and backed by $1.00 USD in physical reserves.) The email notifications from Binance revealed that on September 1, 2021, September 5, 2021, and October 30, 2021, NGUYEN made withdrawals from the account utilizing the following cryptocurrencies: LINK, DOGE, ADA, ETH, DOT, LTC, BCH, and EOS. These withdrawals were sent/deposited into the

jamessmithhelp@gmail.com Binance account. On October 27, 2021, the Binance account was limited to withdrawals because the account never completed the account verification process.

69. Records provided by Dropbox for jamessmithhelp@gmail.com and minhoba@ymail.com revealed Dropbox user ID 3136031088 listed the subscriber's name as "David John," email address nqminh73@protonmail.com, and the original email address for the account as jamessmithhelp@gmail.com. The Dropbox user ID 350122839 listed the subscriber's name "Minh David" and email address minhoba@ymail.com.

70. On October 12, 2022, the FBI served a federal search warrant to Dropbox for the accounts jamessmithhelp@gmail.com and minhoba@ymail.com – two accounts controlled by NGUYEN. The search warrant returns revealed these accounts contained information for approximately 100 stolen identities and information used to circumvent fraud detection by companies like PayPal and Google. Each folder within the return typically included PII, documents such as driver's licenses, voice-over-IP (VoIP) account credentials, VPS credentials for a server within the geographic region of the identity, and a digital cookie. These combined elements provided a complete "digital footprint" for each stolen identity. One example was a folder that contained the identity of a victim located in the Eastern District of Pennsylvania. This PII was used by NGUYEN to create a PayPal account which transacted with the nqminh73@yahoo.com PayPal account. This victim was interviewed by the FBI. The victim confirmed that they did not know about, open, or operate, the PayPal or email accounts opened with their PII.

71. On October 12, 2022, the FBI served a federal search warrant to Apple for the account associated with minhoba@ymail.com – another account controlled by NGUYEN. The

results revealed an account with "Minh Nguyen Quoc" as the subscriber, DSID 17110546039, a Vietnam address, day phone +84982468445, verified phone +84582962186, and a billing profile creation IP address of 222.252.88.76. Open-source research confirmed that IP address 222.252.88.76 resolved to Hanoi Post and Telecom Company in Vietnam. The Apple transaction log for this account listed numerous applications utilized by this account, including:

a. Gate.io: Open-source research confirmed that Gate.io is a cryptocurrency exchange based in the Cayman Islands.

b. Remitano

c. Blockchain.com Wallet

d. ZaloPay: Open-source research confirmed that ZaloPay is an e-wallet where users can transfer money, pay for goods through QR codes, and pay bills with credit cards issued by Vietnamese banks.

e. VETC Electronic Toll Collection: Open-source research confirmed that VETC Electronic Toll Collection is an application through the Vietnam Electronic Toll Collection Company to pay tolls, much like E-ZPass in the United States.

f. CoinMarketCap Crypto Tracker: Open-source research confirmed that CoinMarketCap is an application used to track the price of Bitcoin, Ethereum, Litecoin, and numerous other cryptocurrencies.

g. VPN-Super Unlimited Proxy: Open-source research confirmed that VPN-Super Unlimited Proxy is a free proxy VPN.

h. Vietcombank: Open-source research confirmed that Vietcombank is a commercial bank in Vietnam, which is formally known the "Joint Stock Commercial Bank for

Foreign Trade of Vietnam." As noted above, NGUYEN linked his Remitano account to an account at Vietcombank.

i. Reddit

j. Binance

k. Investing.com Cryptocurrency: Open-source research confirmed that Investing.com Cryptocurrency is an application that offers an overview of cryptocurrency markets for tracking prices and exchange rates.

72. Records from Apple for the minhoba@ymail.com account revealed documents and photos which uncovered that NGUYEN has basic training in cryptographic engineering and previously worked in decrypting communications and cyber reconnaissance. In 2016, NGUYEN earned his PhD in Electronic Engineering in Taiwan. The pictures of NGUYEN (a sample provided below in Figures 8-12) resemble the same individual in the pictures for the KYC which was provided by NGUYEN to various companies discussed earlier. Specifically, the background in Figure 8 resembles the background in Figure 7 which was provided as part of the KYC to Remitano:

Figure 8: minhoba@ymail.com Apple Account – Picture 1

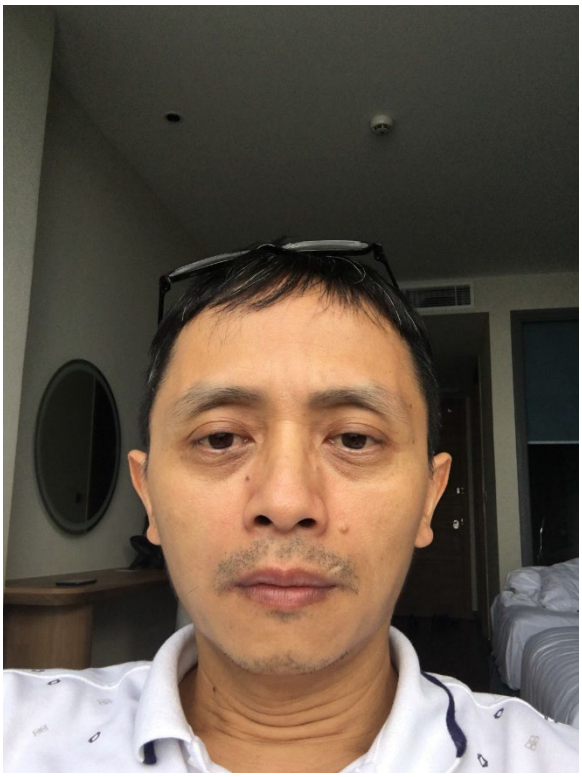

Figure 9: minhoba@ymail.com Apple Account – Picture 2

Figure 10: minhoba@ymail.com Apple Account – Picture 3

Figure 11: minhoba@ymail.com Apple Account – Picture 4

Figure 12: minhoba@ymail.com Apple Account – Picture 5

73. Records provided by LinkedIn revealed active accounts for the following email accounts: jamessmithhelp@gmail.com, minhoba@ymail.com, minhoba@yahoo.com, and nqminh21@gmail.com. These records revealed the following information:

a. The email address jamessmithhelp@gmail.com registered an account on October 13, 2014 from IP address 140.127.112.209 with the profile username "James Smith" and a geo location of Taiwan. (Open-source research on IP address 140.127.112.209 revealed that it resolved to the Ministry of Education Computer Center in Taiwan.)

b. The email address minhoba@ymail.com registered an account on June 28, 2011 from IP address 123.24.236.184 with the profile username "Nguyen Quoc Minh" and a geo location of Vietnam. The account user stated that he was conducting Ph.D. research at Kaohsiung, Taiwan. (Open-source research conducted on IP address 123.24.236.184 revealed that it resolved to the Vietnam Posts and Telecommunications Group in Ha Noi, Vietnam.)

c. The email address minhoba@yahoo.com registered an account on April 2, 2010 from IP address 123.24.209.156 with the profile username "James Minh" and a geo location of Vietnam. The account also listed the Twitter handle @Jame2010 and websites https://MakeMoneyGuides.com, https://health-sex-money.com, and https://businessallianceonline.com. (Open-source research conducted on 123.24.209.156 revealed that it resolved to the Vietnam Posts and Telecommunications Group in Ha Noi, Vietnam.)

d. The email address nqminh21@gmail.com registered an account on February 13, 2014 from IP address 123.16.111.73 with the profile username "James Smith." The account listed the additional email address contact@rambowriter.com, a geo location of United

Kingdom, and the Twitter handle @RamboWriter. The receipts for purchases on LinkedIn listed "Nguyen Quoc Minh" with a billing country of Vietnam. (Open-source research conducted on IP address 123.16.111.73 revealed that it resolved to the Vietnam Posts and Telecommunications Group in Ha Noi, Vietnam.)

74. Records provided by Twitter for @RamboWriter revealed the subscriber name "James Smith" and an email address james@rambowriter.com. The account was created on April 6, 2014 from IP address 60.248.123.154. Open-source research conducted on IP address 60.248.123.154 revealed that it resolved to Chunghwa Telecom Co. Ltd. In Kaohsiung, Taiwan.

viii. NGUYEN's Online Postings

75. Records provided by Reddit for minhoba@yahoo.com and nqminh21@gmail.com revealed active accounts. The account associated with minhoba@yahoo.com was created on November 22, 2008 and listed the username "hotpassion." The account associated with nqminh21@gmail.com was created on May 16, 2021 from IP address 222.252.92.39 and listed the username "Western-Fee-2653." Open-source research on IP address 222.252.92.39 revealed that it resolved to Hanoi Post and Telecom Company in Ha Noi, Vietnam.

76. Open-source research conducted on the username "hotpassion" used by NGUYEN revealed this moniker is also used on BitcoinTalk where the profile advertises exchanging bitcoin for fiat currency from PayPal accounts. For example, the user posted "Bitcoin to PayPal – Pay $170 get 200$ in PayPal." In addition, "hotpassion" included a link on their BitcoinTalk profile to their account on Bitify. The username on Bitify is "LovePayPal" and there are comments listed where users purchased balances from PayPal accounts or reference what appears to be the purchasing of stolen identities and identifying documents.

77. Open-source research conducted on the moniker "minhoba" used by NGUYEN revealed a post on the forum BlackHatWorld (blackhatworld.com). The user "minhoba" posted the following on the forum in February 2009 with the title, "How To Unlimit Your Paypal Acc":

> Hi all,
> I 'm not living in US and my country'paypal acc [sic] can't receive money, so I bought a US verified Paypal account, but after using it for 2 months, it was limitted [sic]. I have some money in this account, but not much. They ask me to provide some personal documents to prove I'm the owner of that US PayPal acc, but I'm not US citizen ! So what should I do now to get my account unlimited ? [sic] I still want to use paypal acc to receive money in some programs that I have spent so much time and energy to promote.
> Thank You for your help. Highly appreciate your reply.
> Regards,
> Nguyen.

78. The user "minhoba" commented in this thread in response to another user's suggestions:

> Thank you all for your help.
> bantoncookies@: Yes, I'm from Vietnam, but I use proxy to log in PP acc. My account use US's profile information and VCC to verify. The reason my acc is limitted [sic] is that I received money daily with small amount of money (the seller told me that), I'm not sure if it was true.
> aj113: I will consider about a new unverified acc.

79. Open-source research conducted on "MINH QUOC NGUYEN" revealed an account on ResearchGate with the name MINH QUOC NGUYEN and a profile picture which resembles NGUYEN. The account states that, between September 2011 to August 2016, NGUYEN was a Ph.D. student in the Department of Electronic Engineering at the National Kaohsiung University of Science and Technology located in Kaohsiung, Taiwan. Open-source research conducted on ResearchGate revealed it is a European social networking site for scientists and researchers to share papers, ask and answer questions, and find collaborators.

ix. The "V2 Subscriber" Persona

80. In November 2022, PayPal provided records for linked accounts associated with NGUYEN, which included PayPal account ID 2238500671084238088, hereinafter "V2 PayPal Account." Records provided by PayPal for this account revealed a name having the initials T.V., hereinafter "V2 Subscriber," and email address tvalek@post.cz. This is another identity stolen by NGUYEN.

81. Records provided by PayPal for NGUYEN's V2 PayPal Account identified accounts associated by "Visitor ID." According to PayPal, a Visitor ID is associated with a device used to log into a PayPal account. Therefore, multiple accounts that log into their account from the same device would have a common Visitor ID. The Visitor ID 6215924230645620704 linked the V2 PayPal Account and the PayPal account 1356241556304782540. The PayPal account 1356241556304782540 is associated with the name "Max Archdall" and email address max.archdall@gmail.com, which were previously discussed as directly associated with ChipMixer and an alias account used by NGUYEN.

82. Records provided by PayPal for NGUYEN's V2 PayPal Account transaction logs identified six accounts which also sent payments to the V3 PayPal Account. Four of the six identified PayPal accounts utilized ProtonMail email addresses. Results provided in response to international records requests for the ProtonMail accounts revealed the recovery email addresses were either minhoba@ymail.com or jamessmithhelp@gmail.com.

83. Records of the transaction logs for NGUYEN's V2 PayPal Account revealed monthly payments to Hetzner, the company which hosted ChipMixer. The V2 PayPal Account subscriber information was associated with an account at Hetzner. Beginning on April 3, 2017, this account leased a server at IP address 136.243.102.235 (hereinafter "V2 Server"). As noted

above, the investigators identified another Hetzner server being used by ChipMixer, 138.201.227.85 ("V3 Server".)

84. The data contained on both V2 Server and V3 Server is directly linked to NGUYEN and ChipMixer. Moreover, the funding for the server is directly attributable to NGUYEN because his personal account sent a PayPal payment from his credit card to the V3 PayPal Account as well as the accounts of stolen individuals that NGUYEN controls.

x. PremiumRDP and SmartHost

85. Pursuant to the Cloud Act Agreement between U.S. and U.K. authorities, a records request was submitted to Premium Technologies for account information associated with jamessmithhelp@gmail.com – an account controlled by NGUYEN as described above. Records provided by Premium Technologies revealed an account created on March 11, 2022, with the name "James Smith," an address of Ha Noi, Vietnam, and telephone number +84982468445. According to Premium Technologies, the email was verified and the payment method was bitcoin. The records also revealed logins or support ticket submissions from the following IP addresses:

a. 03/11/2022: 59.153.240.33

b. 04/19/2022: 14.248.130.210

c. 04/23/2022: 59.153.241.41

d. 04/25/2022: 59.153.235.168

e. 04/29/2022: 59.153.241.230

f. 05/01/2022: 14.248.151.213

g. 06/16/2022: 83.143.107.32

h. 07/13/2022: 59.153.240.94

i. 07/14/2022: 107.173.30.140

j. 07/22/2022: 107.173.30.140

k. 08/02/2022: 107.173.30.140

l. 08/20/2022: 107.155.97.170

m. 08/29/2022: 107.155.97.170

n. 09/22/2022: 107.155.97.170

o. 09/27/2022: 107.155.97.170

p. 10/16/2022: 107.155.97.170

86. Open-source research on IP addresses 59.153.240.33, 59.153.241.41, 59.153.235.168, 59.153.241.230, and 59.153.240.94 revealed they resolved to Mobifone Service Company located in Ha Noi, Vietnam, which is a major Vietnamese mobile network operator. Open-source research on IP addresses 14.248.130.210 and 14.248.151.213 revealed they resolved to Vietnam Posts and Telecommunications Group in Ha Noi, Vietnam. Open-source research on IP address 83.143.107.32 revealed it resolved to SmartHost, LLC (SmartHost), located in Henderson, Nevada. Open-source research on IP address 107.173.30.140 revealed it resolved to Colocrossing, located in Buffalo, New York. Open-source research on IP address 107.155.97.170 revealed it resolved to Hivelocity, Inc. located in Tampa, Florida.

87. Yahoo records produced in response to the Order under 18 U.S.C. § 2703(d) for minhoba@ymail.com, controlled by NGUYEN, revealed logins from the following IP addresses:

a. 03/11/2022: 59.153.240.33

b. 05/01/2022: 14.248.151.213

88. Records provided by Premium Technologies for the jamessmithhelp@gmail.com account controlled by NGUYEN revealed five active servers to include the following IP address: 92.223.93.151, 185.127.92.163, 193.8.172.163, 45.14.114.217, and 45.42.200.243. Two servers were not active and had used the IP addresses 142.132.185.86 and 45.42.202.171. All servers (located in the U.S., Italy, and Germany) were accessed through RDP . The administrators of PremiumRDP stated they subleased the servers from other providers. One of the providers is SmartHost. The FBI identified IP addresses 193.8.172.163, 45.14.114.217, and 45.42.200.243 were subleased to SmartHost.

89. On February 27, 2023, the FBI served a federal search warrant to SmartHost for the servers associated with IP addresses 193.8.172.163, 45.14.114.217, and 45.42.200.243. FBI forensic analysis of the server associated with IP address 45.14.114.217 (217 Server) identified evidence the V3 Subscriber's Protonmail email address was associated with a Microsoft Edge profile on February 8, 2023 at 01:25 a.m. UTC (08:25 a.m. in Ha Noi, Vietnam). Open-source research conducted on Microsoft Edge profiles revealed Microsoft Edge profiles allow multiple users to operate in a shared environment while maintaining access to their personalized browser settings, bookmarks, and extensions. Thus, NGUYEN created a profile in Microsoft Edge for the V3 Subscriber Protonmail email account to isolate and maintain this email address as part of an identity. As noted above, the V3 Subscriber was one of the identities NGUYEN stole to hide his involvement in ChipMixer. FBI's analysis of the 217 Server also revealed that jamessmithhelp@gmail.com (attributed to NGUYEN) was associated with Google Chrome login data and autofill data. Based on my training and experience, this shows that the email address jamessmithhelp@gmail.com was entered into websites using Google Chrome.

90. In addition, FBI's forensic analysis of the 217 Server revealed "RDP Logs," which log remote connections to the server. Most of the IP addresses making connections to the 217 Server resolve back to ISPs in Vietnam. According to open-source databases, other IP addresses were associated with likely proxies or VPNs. Specifically, on February 7, 2023 at 03:19 UTC, there was an RDP account login from the IP address 59.153.241.55. Open-source research on IP address 59.153.241.55 revealed it resolved to MobiFone, located in Vietnam. Records provided by Remitano for NGUYEN's "hotpassion" account revealed there was a login from IP address 59.153.241.55 on February 7, 2023 at 02:33 UTC. This evidence demonstrates NGUYEN's control over these facilities through the common IP address.

91. Moreover, FBI forensic analysis of the 217 Server revealed 42 instances of RDP connections with the IP address 113.190.206.177 from August 14, 2022 to October 24, 2022. Open-source research on IP address 113.190.206.177 revealed it resolved to Vietnam Posts and Telecommunications Group, located in Vietnam. Records provided by Binance for the jamessmithhelp@gmail.com account revealed a device was registered to the account from IP address 113.190.206.177 on September 23, 2022 at 07:26 (UTC) and numerous logins occurred from that IP address from August 13, 2022 to September 23, 2022. This evidence further demonstrates NGUYEN's control over these facilities through the common IP address.

V. CONCLUSION

92. Based on the evidence as outlined above, MINH QUOC NGUYEN controlled ChipMixer through the network of aliases and stolen identities as shown in Figure 13.

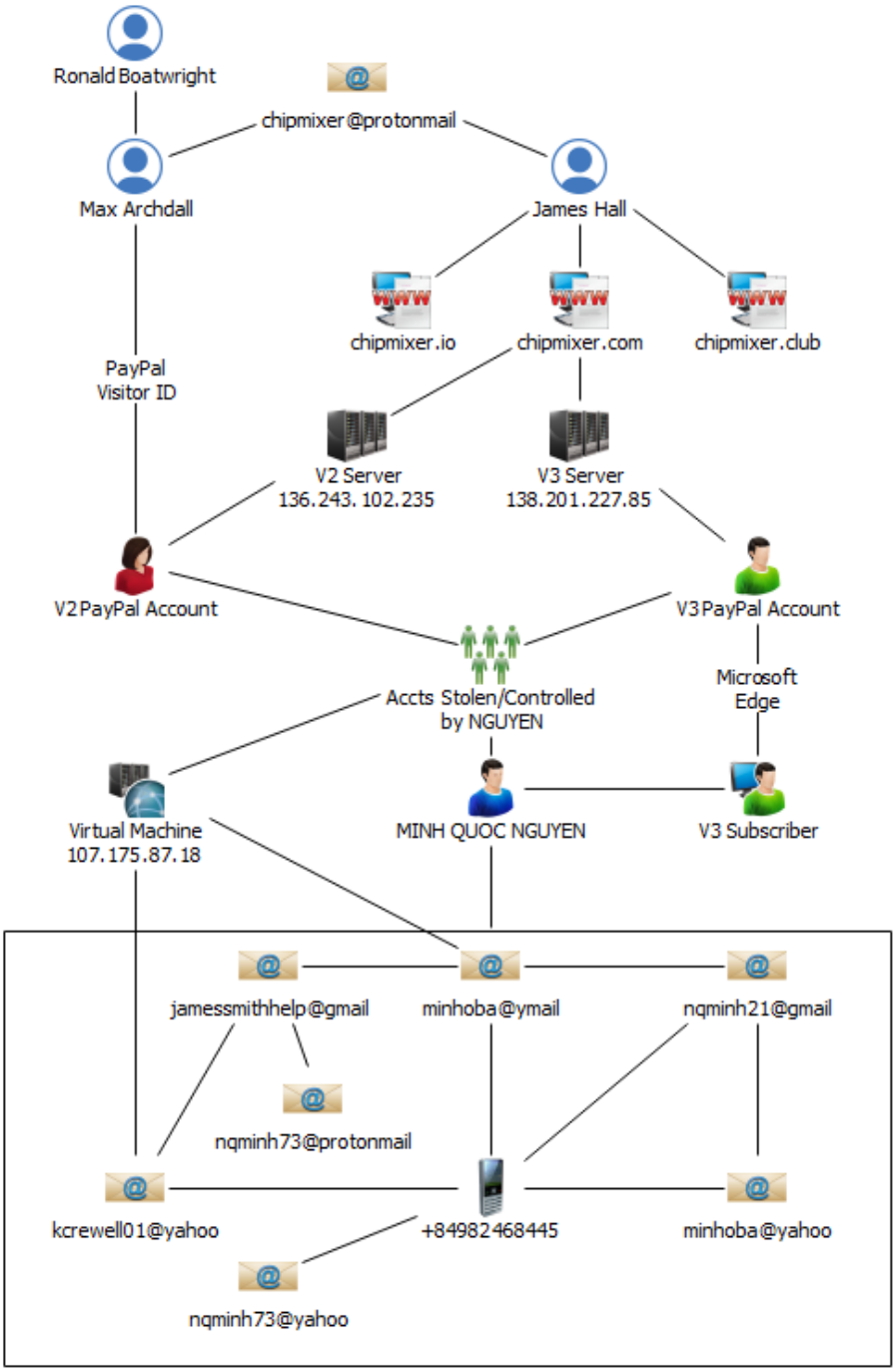

Figure 13: ChipMixer

93. Based on the evidence as outlined above, I have probable cause to believe that MINH QUOC NGUYEN has violated Title 18, United States Code, Sections 1956(a)(1)(B)(i)

(conducting a financial transaction with knowledge that the transaction is designed to conceal the proceeds of the specified unlawful activity), 1960 (unlicensed money transmitting business), and 1028(a)(3) (possession with intent to use or transfer five or more documents or authentication features).

/s/ Steven Parker
STEVEN PARKER
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this
14th day of March 2023.

/s/ The Honorable Richard A. Lloret
HONORABLE RICHARD A. LLORET
United States Magistrate Judge