CYJAX

Digital Intelligence
Securing the Future

Ten ways to lose your Crypto

Introduction

It is fair to say that cryptocurrencies and Non-Fungible Tokens (NFTs) will have attack surfaces common with any other technology. However, the innovative use of blockchain technology has some unique and interesting vulnerabilities which can and have been exploited by malicious actors. Although many of the scams and exploits detailed in this white paper have a particular focus on "the world of cryptocurrencies", on close analysis many of them have a long history of use.

Before we examine the attack surface in detail, it is imperative for the reader to understand in some depth the technological components which enable the industry built on blockchain technologies.

Blockchain, cryptocurrencies and NFTs: https://www.natlawreview.com/article/blockchain-crypto-nfts-5-minute-primer-to-help-you-understand-basics

Smart contracts:
https://www.natlawreview.com/article/smart-supply-chains-using-smart-contracts

The references for the above topics come from *The National Law Review*. They were deliberately chosen not for brevity but due to the peer-reviewed nature of the articles published, and the expertise of the lawyers in this subject area. There is *a lot* of disinformation on these topics, spewed by charlatans running simple "get rich quick investment schemes" or far more complex, sophisticated and illegal money laundering-related operations.

This article from 2019 paints a particularly bleak reputation of the industry:

> *To many, however, cryptocurrencies appear to be an unregulated, Wild West-like industry replete with bankruptcies, fraud, companies going out of business, price collapses and a general lack of transparency.* [1]

This may be close to the contemporary view of the industry; however, since then there have been government and industry attempts to clean up its reputation, despite Bitcoin (BTC) – the dominant cryptocurrency – being the preferred currency for cyber-criminal ransomware payments. Interestingly, a sub-set of cyber-criminals has evolved: they specialise in attacking and exploiting the technologies that drive the cryptocurrency industry.

It is astounding that as of 2020 "[The] amount defrauded in the crypto space has grown to more than $12 Billion and despite global efforts, 98% of cases going unsolved,"[2] according to Pawel Kuskowski writing in Forbes.

Cyjax has compiled for the first time a detailed analysis of and understanding of the cryptocurrency industry attack surface.

1 https://www.investopedia.com/how-bitcoin-s-shaky-reputation-is-limiting-the-spread-of-blockchain-4690557#:~:text=The%20biggest%20barrier%20to%20retail,Facebook%20(FB)%20and%20Fidelity.

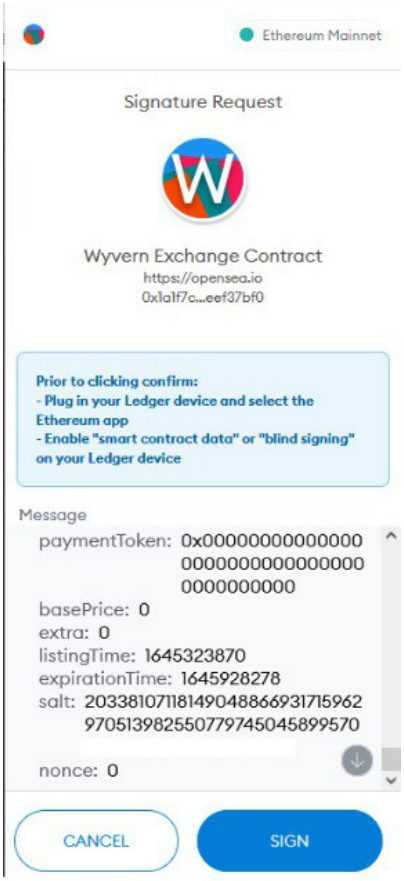
2 https://www.forbes.com/sites/pawelkuskowski/2020/09/17/how-to-trace-stolen-crypto/?sh=a2e057045e6c

The threat actors ask for your money

Unsurprisingly, an "Ice Phishing" attack can be delivered in any number of ways specifically targeted at cryptocurrency users. This attack essentially uses social engineering techniques to lure victims into transferring funds or losing control of their wallets and currency. The attack often seeks to confuse the victim by leveraging the technical nature of cryptocurrency. Its success rate can be significant. Cardify suggests: "Regardless of experience level, the majority of investors (83.1%) report moderate or low levels of cryptocurrency knowledge."[3] This situation makes easy pickings for malicious actors.

The attack on OpenSea[4]

- In this attack the malicious actors took advantage of OpenSea's decision to migrate their listings to the new smart contract.
- They sent out a cloned version of the migration email but with modified links which would persuade the victim to sign a transaction migrating their NFTs from their wallet to one operated by the malicious actor.
- In total over $2 million worth of NFTs was stolen.



Source:
https://twitter.com/isotile/status/1495234655154577408

A far more successful version of this attack took place on BadgerDAO, where poor cyber-security measures led to a malicious modification on the customer-facing platform and a major windfall for the threat actors.

The attack on BadgerDAO[5]

- Malicious actors exploited the Badger smart contract front-end infrastructure to inject malicious scripts.
- This script requested users to sign transactions, granting the ERC-20* approvals to the attacker.

3 https://www.cardify.ai/reports/crypto
4 https://blog.checkpoint.com/2022/02/20/new-opensea-attack-led-to-theft-of-millions-of-dollars-in-nfts/
5 https://www.coindesk.com/business/2021/12/10/badgerdao-reveals-details-of-how-it-was-hacked-for-120m/

- This enabled the malicious threat actor to transfer funds from the victim's account.

** The ERC-20 approval standard permits an address to give an allowance to another address to be able to retrieve tokens from it. This receiver returns the remaining number of tokens that the spender will be allowed to use on behalf of the owner.*

Hack the smart contract

A smart contract is a self-executing program which is stored on a blockchain and only executes when certain permissions are met. Smart contracts are permissionless, meaning that anyone can write and deploy one to the blockchain network. These smart contracts have become targets for malicious actors trying to actively exploit the code running on the blockchain networks. Some smart contracts are used for relatively simple processes, while in other cases entire businesses are using them.

Compromise of the smart contract code can place the management of the financial assets in the hands of a malicious actor, and once the modified code executes, the action cannot be reversed.

Research detailed in the report: *Finding, The Greedy, Prodigal, and suicidal [smart] contracts at Scale*[6] suggests that one in 20 smart contracts deployed on blockchain networks is at risk of compromise, with the result of locking funds indefinitely, leaking funds to arbitrary users and smart contracts – before execution – which can be killed by an unauthorised user.

The Parity multi-sig Ethereum wallet hack[7]

- Parity produced multi-signature (multi-sig) wallets which were responsible for managing Ethereum cryptocurrency.
- These wallets were represented by smart contracts which would require more than one private key for the transfer of money.
- The malicious actor exploited the **delegatecall** and **fallback** functions within the multi-sig smart contract, which enabled the attacker to transfer funds without the need for a key.

The DAO Ethereum blockchain hack[8]

- In 2016 a Decentralised Autonomous Organization (DAO) named "The DAO" was launched on the Ethereum blockchain. A DAO is an organisation that runs entirely through smart contracts.
- By running entirely through smart contracts, decisions are made by the code or by voting organisation members, removing centralised control.
- The aim was to allow users to vote in a democratic manner on which Ethereum projects to fund.
- However, an exploit within the **fallback** function used in the code enabled an attacker to steal 3.6 million Ethereum.*

** This was so monumental to recover that a hard fork was required, leading to the inception of Ethereum Classic and Ethereum.*

Design and infrastructure flaws

When cryptocurrencies are invented, there is a design process behind them, as with any software product. This means that elements of this design process can be vulnerable to attacks just like any other software. This can include the code behind the blockchain, the design of the blockchain or the hardware it relies on.

Attacking the blockchain network itself can result in devastating attacks taking place. Exploiting this network can allow for the integrity of the entire blockchain to be compromised. This means that not only do the

6 https://arxiv.org/pdf/1802.06038.pdf
7 https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/
8 https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-origins-of-the-dao

threat actors have opportunities to gain directly from the potential compromise of accounts, but they may be able to cause disruption and the potential collapse of the cryptocurrency, which may allow the malicious actors to short the cryptocurrency through investment mechanisms.

The Wormhole attack[9]

- In early 2022 a DeFi platform named Wormhole was hit in an attack that resulted in the loss of $326 million dollars.
- The attacker found a bug within the platform's code where the site was not properly validating input accounts, and so was able to spoof guardian signatures.
- This issue was picked up in the open-source project, and fixes were being made for deployment, so it is likely that the attacker found the exploit on the public GitHub.

The 51% attack[10]

- Although not a direct error in a blockchain, the blockchain's inherent design has a flaw.
- The flaw exploits the design principle of letting the system of the majority decide on the narrative and the correctness of the blocks written to the blockchain network.
- When over 51% of the blockchain's mining power is owned by a single entity, it is possible to change the validity of the chain or rewrite existing blocks.
- The larger currencies, such as Bitcoin and Ethereum, make this nearly impossible and prohibitively expensive to achieve, requiring thousands of mining devices.
- Lesser-known coins without a diversified pool of mining power can suffer this attack.

Coin Exchange Attacks

Cryptocurrency exchanges are the infrastructure used to transfer and exchange- as the name suggests – cryptocurrency, and in many cases to fiat currency. From as early as 2010 with the founding of Mt. Gox, crypto exchanges have been targets for cyber criminals and malicious nation state actors due to the lucrative prizes open to them from gaining unauthorised access.

In 2021 over 20 exchange compromises resulted in the hacker escaping with over $10 million; in at least six of those cases the attackers left with over $100 million.[11]

Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency – [US] Government Seized $3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange[12] *****

Case 1:22-mj-00022-RMM Document 1-1 File Case: 1:22-mj-00022
Assigned to: Judge Meriweather, Robin M.
Assign Date: 2/7/2022
Description: COMPLAINT W/ ARREST WARRANT

STATEMENT OF FACTS

** Please see the Statement of Facts PACER case document in relation to the activities of ILYA "DUTCH" LICHTENSTEIN, a citizen of Russia and the United States, and his wife, HEATHER MORGAN, included as Appendix "A" to this white paper*

9 https://www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html
10 https://www.coindesk.com/tech/2019/12/02/the-vertcoin-cryptocurrency-just-got-51-attacked-again/
11 https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870
12 https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

Binance loses $40 million in attack[13]

- Binance, the largest global exchange, suffered an attack in 2019 where over $40 million worth of cryptocurrency was lost.
- Hackers stole API keys, 2FA codes and other information as part of the attack.
- The attackers stole the contents of one of Binance's "Hot Wallets"* and were able to remove the $40 million before alarms were triggered and any further withdrawals were made.
- This forced Binance to consider conducting a roll-back on the network; however, this was not done as it would have ruined their credibility.

** A hot wallet refers to a virtual currency wallet that is accessible online, and it facilitates cryptocurrency transactions between the owner and end-users.*

Crypto.com loses $34 million[14]

- In early 2022 crypto.com revealed that a flaw on its platform resulted in 483 of its users being affected.
- Over $34 million of cryptocurrencies was withdrawn without authorisation.
- This occurred after there was a bug in the company's 2FA that enabled the attacker to approve transactions without the need to use it.

Attack the Protocol

On 9 May 2022 a highly sophisticated attack was conducted against Fortress, a decentralized finance (DeFi) lending protocol with an algorithmic money market to create a synthetic Stablecoin* It suffered an oracle price manipulation attack that resulted in the loss of all its funds.[15]

The exact nature of the protocol attack is still under investigation by the firm but from the article some interesting facts emerge:

> *After exploiting the protocol, the attacker bridged all stolen funds to Ethereum (ETH) before depositing them into the popular crypto mixer Tornado Cash, Etherescan transactions show.*[16]

It is clear the malicious actors were sophisticated and understood how to quickly launder the purloined funds using a crypto mixer service.

> *Blockchain security firm Blocksec detailed that the Chain oracle used by Fortress lacked power verification, which enabled anyone to hijack it.*
>
> *"The `submit` function of the Chain oracle can be called by anyone and doesn't have a power verification," BlockSec said on Twitter, adding that the attacker called this function and changed the price of the project's native token FTS directly.*[17]

The malicious actor had the ability to understand the protocol's weakness – the lack of a power verification requirement within the DeFi submit function and how that might be leveraged to "vote for a proposal that added the FTS token as collateral." Subsequently, the attacker was able to use FTS 100 as collateral to borrow all other assets in the protocol."[18]

** Stablecoin is a digital currency that is pegged to a "stable" reserve asset like the U.S. dollar or gold.*

13 https://www.wired.com/story/hack-binance-cryptocurrency-exchange/
14 https://www.businessinsider.in/cryptocurrency/news/crypto-com-confirms-483-users-lost-34-million-in-hack/article-show/89034893.cms
15 https://cryptonews.com/news/defi-lending-protocol-fortress-loses-all-funds-oracle-price-manipulation-attack.htm
16 Ibid
17 Ibid
18 Ibid

Stablecoins are designed to reduce volatility relative to unpegged cryptocurrencies like Bitcoin.[19]

Gain unauthorised access to the customer's cryptocurrency wallet

Malware is one of the most common tools within a malicious actor's arsenal. Many malware families which specialise in info stealing and credential grabbing can become a threat to the customer's cryptocurrencies. As the popularity of crypto wallets to manage the customer's crypto assets grew, malicious actors developed specific capabilities for stealing keys and passphrases to gain access.

Some wallets, however, were poorly designed or could be manipulated into revealing their contents due to software vulnerabilities, so direct attacks on certain wallets were easily accomplished.

Threat actors often look for quick and simple wins, dropping malware into a compromised system which scans for crypto wallets and executing simple exploit code. This type of automated wallet attack enables the malicious actors to automate the process of exploitation and emptying of the wallet.

Ever Surf wallet vulnerability[20]

- In 2022, a vulnerability was discovered in the Ever Surf wallet that could allow an attacker full control over the victim's wallet.
- This wallet software was for the Everscale blockchain and would allow the attacker to decrypt private keys and seed phrases.
- This would enable the threat actor to steal the currency within the wallet and lock the victim out of the account.

Arkei Infostealer malware attack[21]

- In 2022 an infostealer known as Arkei was discovered specifically targeting cryptocurrency wallets alongside other information such as passwords, cookies and tokens.
- This malware is config file-based, enabling the threat actor to customise it to each targeted device.
- The malware includes loader capabilities used for installing additional malware, increasing the capabilities for further exploitation.

Launch a cryptojacking attack

Cryptojacking is the concept of stealing resources from other machines to mine cryptocurrency. This enables threat actors to make a profit from the cryptocurrency without the need to pay for the hardware or the significant power resources to mine coins.

Cryptojacking started as an alternative to adverts when CoinHive developed a technique where services could ask to use a specific amount of the user's CPU compute while accessing a website to mine cryptocurrency. This was implemented by sites such as Pirate Bay in 2017. Cryptojackers took this and expanded it to become a malware that would function in the same way without the user's consent.

Cryptojacking malware enables threat actors to gain instant profits by compromising other machines to use as mining resources. By removing the hardware costs – for Async Mining devices and/or high-end video cards – they could increase the profit margins of a compromised system. As time progressed the malware used in these attacks became harder to detect.

The term cryptojacking has developed into a broad family and different types of attacks unleased by malicious actors to create cryptocurrency through illicit means:

19 https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin
20 https://www.itsecuritynews.info/critical-vulnerability-identified-in-ever-surf-blockchain-wallet/
21 https://blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer

- Bypass electrical meter to steal electricity to use to mine cryptocurrency.[22]
- Hijack visiting computers to a compromised website and make them mine cryptocurrency.[23]
- Break into hosted computers and servers and cause them to mine cryptocurrency.[24]

TeamTNT cloud-based attacks[25]

- Threat actor TeamTNT is a cryptojacking focused group which targets Kubernetes clusters and Linux servers for cryptojacking – especially cloud-based infrastructure.
- The operators are also an adopter of "plug the hole" techniques where they patch the vulnerability they used to exploit the system in order to maintain access and prevent further exploitation from other threat groups.
- This attack hijacks and can spawn more mining systems leveraging cloud-based infrastructure, making the victim pay to mine crypto and bringing in large profits to the Team TNT wallets.

Execute a dusting attack

A dusting attack is where small amounts of cryptocurrency are sent to a large number of wallets to defeat the efforts to track and trace the wallet addresses in the hope of deanonymising the owners and origin of funds. The attack works when a small amount of crypto funds stays in the victims' accounts and is then used to create another transaction. If all these transactions can be collated together, a task which takes serious efforts, the result can yield the other wallet addresses, allowing for deanonymisation of the owner to take place.

This kind of attack has been used to target large holders of cryptocurrency. If such a holder was deanonymised it could lead to them being targeted by threat actors or in some cases law enforcement investigating criminal money laundering. Deanonymisation can also be used for other activities that are not necessarily attacks. These include targeted ads, spamming and other targeted network attacks.

Litecoin dusting attack 2019[26]

- On 10 August 2019, a dusting attack was carried out on the Litecoin network.
- This was discovered after 50 Binance addresses received a total of 0.00000546 LTC, which led to the suspicion of a dusting attack from the wallet LeEMCDHmvDb2MjhVHGphYmoGeGFvdTuk2K
- A statement was released showing that the person behind the attack owned a mining pool based in Russia, and claimed they intended to advertise their pool.
- The interesting part of this attack is that even if the origin of the dusting attack is not malicious, the public nature of blockchain enables anyone to investigate the sending and receiving wallets over time.

SIM swap attack

A SIM swapping attack is used to gain access to a victim's smart phone. This involves a malicious actor transferring a user's SIM card information to their own phone, allowing them to take control of the target's phone number. This is often done by attackers contacting the victim's phone provider using information that they have obtained to convince the mobile phone company to transfer the victim's SIM card to the SIM card they control.

This attack is relevant to cryptocurrency as it is used to bypass Multifactor Authentication (MFA). Most

22 https://en.bitnovosti.com/2018/12/27/taiwan-man-was-arrested-for-stealing-3-25-million-in-electricity-to-mine-crypto-currencies/
23 https://techcrunch.com/2018/02/12/ico-snafu/?guccounter=1
24 https://www.enterprisetech.com/2017/10/09/aws-cloud-hacked-bitcoin-miners/
25 https://www.cadosecurity.com/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
26 https://cointelegraph.com/news/understanding-litecoins-dusting-attack-what-happened-and-why

providers and wallet services require MFA authentication before logging in or transferring funds. This attack unfortunately looks like a legitimate transaction and recovery of the stolen funds may be impossible.

Hamilton Police investigate SIM swap attack[27]

- In 2021 a victim had $46 million CAD stolen in a SIM swapping attack.
- At the time this was the single largest crypto theft from an individual.
- Some of the stolen currency was used to purchase a rare username in the gaming community.

Conduct a crypto scam

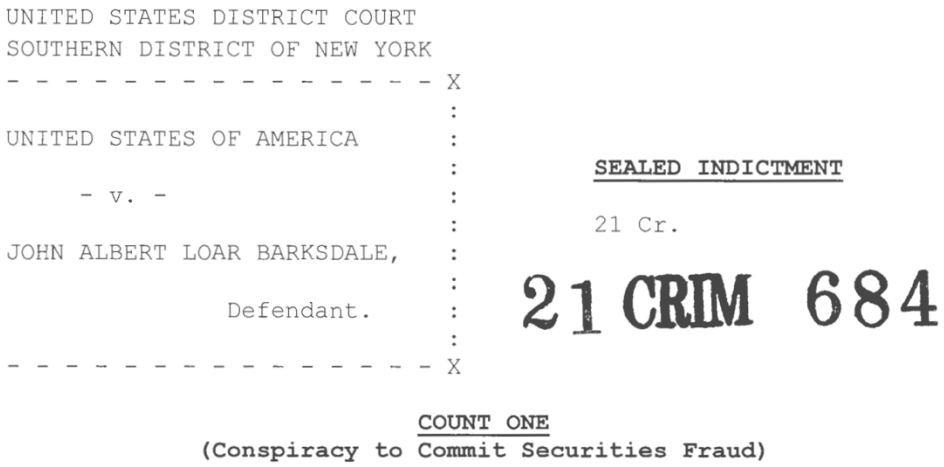
In 2021, cryptocurrency scams reached a new high of $14 billion stolen. That was almost double the previous year's losses of $7.8 billion.[28]

Multiple scam coins have been pushed to victims with tokens such as SQUID scamming yielding over $3 million dollars after the price skyrocketed and the developers disappeared.

We have seen multiple influencers and famous people sharing crypto scams and other coins in what is known as a "pump and dump" to inflate the price and then sell at the high. Other scams include coin-doubling, which is often shared by hacked high-profile accounts. These often promise that any amount donated will be doubled and sent back.

These schemes are quick and easy ways to make money. Scam coins are currently a legal grey area and legislation is struggling to keep up. The people running these scams are difficult to pin down and prosecute, with many of those promoting them getting away and evading justice.

- Crypto Pyramid Scam: DOJ Charges Mining Capital Coin CEO In $62M Fraud Scheme[29]
- Two siblings were charged in a global $124 million crypto fraud operation[30] *



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOHN ALBERT LOAR BARKSDALE,

Defendant.

SEALED INDICTMENT

21 Cr.

21 CRIM 684

COUNT ONE
(Conspiracy to Commit Securities Fraud)

** Please see the Criminal Indictment of JOHN ALBERT LOAR BARKSDALE included as Appendix "B" in this white paper*

27 https://hamiltonpolice.on.ca/news/arrest-made-in-46-million-dollar-cryptocurrency--theft/
28 https://time.com/nextadvisor/investing/cryptocurrency/common-crypto-scams/
29 https://bitcoinist.com/crypto-pyramid-scam-doj-charges-mining-capital/
30 https://www.protocol.com/bulletins/ormeus-crypto-fraud

Double your Bitcoin[31]

- In 2020 some high-profile Twitter accounts were compromised and used to promote a Bitcoin-doubling scam.
- The threat actor received almost $117,000 in illicit funds.
- Accounts including those belonging to Elon Musk, Jeff Bezos and Barack Obama were compromised and used in the attack.
- The threat actor was quickly arrested.

OneCoin Scam[32]

- Between the fourth quarter of 2014 and the third quarter of 2016 alone, OneCoin Ltd. generated €3.353 billion in sales revenue and earned “profits” of €2.232 billion.
- Incredibly, the OneCoin never existed in the first place, with the entire firm being a pyramid scam from the beginning.

Conclusion

The nexus between traditional financial services and the digital currency eco-system has provided ample opportunity for cyber-criminals to adapt their attacks to this new and lucrative environment. In the case of digital currency, the eco-system has exposed numerous avenues of attack which have their origins in “bank heists” and confidence games – now called social engineering attacks.

In addition to the adoption or evolution of cyber-criminal attacks, we also see traditional cybercrime activities such as vulnerability exploitation and unauthorised access leveraged to attack the entire eco-system, from individual customers through to exchanges and coin creation.

31 https://www.buzzfeednews.com/article/skbaer/teen-arrested-twitter-hack-bitcoin-scam
32 https://www.theverge.com/2019/3/8/18256662/us-onecoin-leader-arrested-cryptocurrency-pyramid-scheme

The recent price crash of TerraUSD and its sister currency Terra Luna, a Stablecoin[33], is an example of how the cryptocurrency industry is subject to traditional forms of potential market manipulation and the powerful trading capabilities of hedge funds and investment banks. This massive event where "the entire crypto market has been slashed by more than half since November, falling to $1.2 trillion from $2.9 trillion, according to data from CoinMarketCap."[34] will have far reaching consequences. With calls for regulation and more scrutiny over the activities of major players in the largely unregulated cryptocurrency industry, the industry may find itself subject to far more operating guidelines and regulations.[35]

Thus, the cryptocurrency threat landscape now consists of a combination of traditional bank fraud activities adapted by malicious cyber actors and traditional cybercrime activities. The realisation of this new hybrid attack surface or convergence of criminality will require agile defences, a knowledge-based awareness of both traditional banking fraud techniques, and cyber defence techniques appropriate to risk.

This will drive several key changes within organisations working in the digital currency space.

1. Adoption of, certification and adherence to a cyber-security framework such as ISO 27001 (EU/UK) or NIST (USA)
2. A Software Development Life Cycle (SDLC) focusing on security and contemporary threat models
3. Convergence of Anti-Money Laundering (AML) investigation capabilities with cyber defence teams, coordination and cross communication of activities
4. More robust and rigorous cyber defence activities and controls
5. An aggressive "scam" awareness and best practice security advice campaign for both customers of the services and the organisation's end-users
6. Terms & Conditions modified to aggressively indemnify and reduce potential litigation against the organisation and company officers
7. An appropriately amount of and wide-ranging cyber, company director, and business interruption insurance coverage
8. Awareness of significant changes in legislation and regulation of cryptocurrencies and Know Your Customer (KYC) requirements
9. Adherence to General Data Protection Regulation (GDPR) and various US privacy regulations and cyber security requirements such as the New York Department of Financial Services (NYDFS) and the California Consumer Privacy Act (CCPA) (if applicable)
10. A cyber threat intelligence function to identify and anticipate threat actor activity in the crypto industry and the general financial services industry

These ten steps are high-level objectives which an organisation should have in place ideally before activity within the cryptocurrency eco-system is considered.

Joe Wrieden
Intelligence Analyst

33 https://www.buzzfeednews.com/article/richardnieva/crypto-terra-luna-stablecoin-explainer
34 Ibid
35 https://news.coincu.com/88043-the-crash-of-luna-and-ust/

Appendix A

 Case: 1:22-mj-00022
Assigned to: Judge Meriweather, Robin M.
Assign Date: 2/7/2022
Description: COMPLAINT W/ ARREST WARRANT

STATEMENT OF FACTS

1. Your affiant, Christopher Janczewski, is a Special Agent assigned to the Internal Revenue Service, Criminal Investigation (IRS-CI). As a Special Agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code, Sections 1956 and 1957), the Bank Secrecy Act (including relevant parts of Title 31, United States Code), and related offenses. I have experience investigating crimes involving virtual currency,[1] as further described below. I also am experienced in analyzing and tracing virtual currency transactions. Currently, I am tasked with investigating the laundering of funds stolen from a virtual currency exchange ("Victim VCE") in 2016. As a Special Agent, I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws.

2. The facts and information contained in this Affidavit are based on my personal knowledge and observations, information provided to me by others,[2] and a review of documents and records. This Affidavit does not contain each and every fact known to the Government. It contains only those facts I believe are sufficient to support a finding of probable cause that ILYA "DUTCH" LICHTENSTEIN, a citizen of Russia and the United States, and his wife, HEATHER MORGAN, a citizen of the United States, committed the following offenses: Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); and Conspiracy to Defraud the United States, in violation of 18 U.S.C. § 371.

I. Introduction

3. IRS-CI, the Federal Bureau of Investigation (FBI), and Homeland Security Investigations (HSI) have been investigating the theft of funds from a well-known virtual currency exchange[3] ("Victim VCE") that was hacked in 2016. Victim VCE is one of the world's largest virtual currency exchanges and allows customers to buy, sell, and store various types of virtual currency.

---

[1] Virtual currency is a digital form of value that is circulated over the Internet and is not backed by a government. Bitcoin (BTC) is one of the most popular forms of virtual currency.

[2] The information contained in this affidavit includes information provided by private entities that the U.S. Government believes to be reliable. In August 2020, Victim VCE announced a sizable reward related to the return of the stolen funds. Specifically, Victim VCE offered up to 5% of any property recovered. The total potential reward money exceeds $400 million. The U.S. Government understands that Victim VCE has indicated that some portion of the reward could be made available even where the information provided indirectly leads to the recovery of funds (*e.g.*, where a company provides information to the U.S. Government, that is then able to locate and restrain the funds based on that information). Entities who provided information to the U.S. Government in this matter may therefore be financially motivated. The U.S. Government vetted any leads as appropriate, with consideration given to the potential financial motivation. The U.S. Government is not a party to any agreement between Victim VCE and private individuals or entities and has not been a part of discussions regarding potential rewards.

[3] A virtual currency exchange ("VCE") is a business that allows customers to buy, sell, or trade virtual currency. Many VCEs also store virtual currency on behalf of their customers. VCEs doing business in the United States are regulated by the U.S. Department of Treasury and are required to establish anti-money laundering (AML) programs—that is, controls designed to detect and deter money laundering.

4. In or around August 2016, a hacker breached Victim VCE's security systems and infiltrated its infrastructure. While inside Victim VCE's network, the hacker was able to initiate over 2,000 unauthorized BTC transactions, in which approximately 119,754 BTC was transferred from Victim VCE's wallets[4] to an outside wallet (Wallet 1CGA4s[5]). At the time of the breach, 119,754 BTC was valued at approximately $71 million. Due to the increase in the value[6] of BTC since the breach, the stolen funds are valued at over $4.5 billion as of February 2022.

5. U.S. authorities traced the stolen funds on the BTC blockchain.[7] As detailed below, beginning in or around January 2017, a portion of the stolen BTC moved out of Wallet 1CGA4s in a series of small, complex transactions across multiple accounts and platforms. This shuffling, which created a voluminous number of transactions, appeared to be designed to conceal the path of the stolen BTC, making it difficult for law enforcement to trace the funds. Despite these efforts, as explained further below, U.S. authorities traced the stolen BTC to multiple accounts controlled by ILYA "DUTCH" LICHTENSTEIN, a Russian-U.S. national residing in New York, and his wife HEATHER MORGAN.

6. The 2017 transfers notwithstanding, the majority of the stolen funds remained in Wallet 1CGA4s from August 2016 until January 31, 2022. On January 31, 2022, law enforcement gained access to Wallet 1CGA4s by decrypting a file saved to LICHTENSTEIN's cloud storage account,[8] which had been obtained pursuant to a search warrant. The file contained a list of 2,000 virtual currency addresses, along with corresponding private keys.[9] Blockchain analysis confirmed that almost all[10] of those addresses were directly linked to the hack. Between January 31, 2022, and February 1, 2022, law enforcement obtained approval to execute a lawful seizure supported by probable cause under exigent circumstances and used the private keys from LICHTENSTEIN's file to seize Wallet 1CGA4's remaining balance of approximately 94,636 BTC, worth $3.629 billion. On February 2, 2022, the government requested, and on February 4, 2022, a court issued a seizure warrant authorizing the seizure of those funds. Those funds remain secured in the U.S. Government's possession.

---

[4] The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets are used to store and transact in virtual currency. A wallet may include many virtual currency addresses, roughly equivalent to anonymous account numbers.

[5] BTC wallets and clusters in this affidavit will be referred to by the first six characters of the BTC address associated with the wallet or cluster.

[6] The trading value of BTC fluctuates over time, depending on market demand.

[7] The BTC blockchain is a public transaction ledger that includes a record of every BTC transaction that has ever occurred.

[8] A cloud storage account allows users to store computer files in a remote location, rather than saved to their own devices.

[9] Each virtual currency address has a corresponding private key, which is roughly equivalent to a complex password or PIN code and which is needed to spend any virtual currency contained in the address.

[10] More specifically, all of the 2,000 addresses either contained BTC directly linked to the hack of Victim VCE (*i.e.*, was exclusively funded from the hack) or did not contain any virtual currency at all (*i.e.*, they contained a balance of zero and had never been used to transact in virtual currency).

II. Tracing the Stolen BTC to LICHTENSTEIN and MORGAN

A. Summary

7. During the investigation, and as further described below, special agents traced the stolen funds as follows:

a. **First**, to Wallet 1CGa4s, an unhosted wallet[11] containing over 2,000 BTC addresses (which were saved, along with their associated private keys, in LICHTENSTEIN's cloud storage account), where the stolen funds remained dormant until January 2017;

b. **Second**, to accounts at the darknet market AlphaBay;[12]

c. **Third**, to seven interconnected accounts at a U.S.-based VCE ("VCE 1"), as well as accounts at additional VCEs ("VCE 2," "VCE 3," and "VCE 4");

d. **Fourth**, to various unhosted BTC wallets; and

e. **Fifth**, to accounts owned by LICHTENSTEIN and MORGAN at six other VCEs ("VCE 5," "VCE 6," "VCE 7," "VCE 8," "VCE 9," and "VCE 10").

Close financial analysis and other evidence revealed that all of the above laundering activity was conducted by LICHTENSTEIN and MORGAN.

8. In conducting these transactions, and as described further below, LICHTENSTEIN and MORGAN employed numerous money laundering techniques, including: (1) using accounts set up with fictitious identities; (2) moving the stolen funds in a series of small amounts, totaling thousands of transactions, as opposed to moving the funds all at once or in larger chunks; (3) utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; (4) layering the stolen funds by depositing them into accounts at a variety of VCEs and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; (5) converting the BTC to other forms of virtual currency, including anonymity-enhanced virtual currency,[13] in a practice known as "chain hopping"; and (6) using U.S.-based business accounts to legitimize activity.

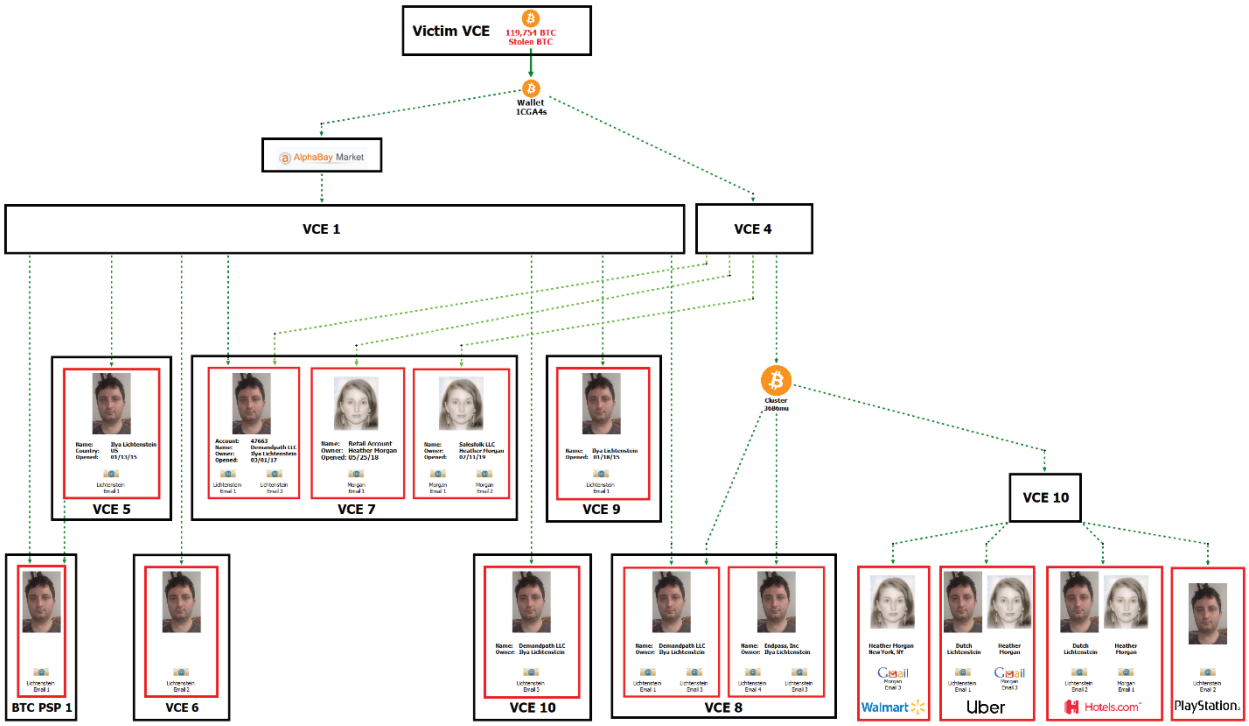
---

[11] BTC wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are called "unhosted" wallets.

[12] A darknet market is an ecommerce platform through which vendors can sell illegal goods and services, such as illegal narcotics, stolen financial information, and hacking tools. Darknet markets typically allow users to create accounts and deposit, store, and withdraw virtual currency from those accounts, in order to buy and sell items on the site. AlphaBay was one of the largest darknet markets and operated from December 2014 through July 2017.

[13] Anonymity-enhanced virtual currency, also called anonymity-enhanced cryptocurrency (AECs) or privacy coins, are virtual currency alternatives to BTC which endeavor to provide greater anonymity when making transactions.

9. The chart[14] below is a simplified[15] illustration of how the stolen BTC moved in a series of transactions from Victim VCE to accounts connected to LICHTENSTEIN and MORGAN:



10. As summarized in the above chart, law enforcement traced the stolen funds through thousands of transactions to over a dozen accounts in the true name of LICHTENSTEIN, MORGAN, and/or their businesses. Law enforcement was also able to determine that numerous accounts set up with fictitious personas and involved in the laundering were, in fact, controlled by LICHTENSTEIN and MORGAN. Several key examples of this tracing—but by no means every example—are included in the subsequent subsections.

[14] Charts within this affidavit that display the symbol of an orange circle with a "B" and two lines running vertically through that "B" is a representation of BTC. The symbol of an orange and grey circle with a white M running through it is a representation of Monero (XMR), an anonymity-focused virtual currency discussed later in this complaint.

[15] Because the stolen BTC was transferred and split up so many times, condensing all the transaction information into one chart would be impractical. The charts within this affidavit do not depict all known transactions, or even all transactions related to the activity depicted. Rather, they are meant to be illustrations of the general flow of the stolen BTC from one point to another.

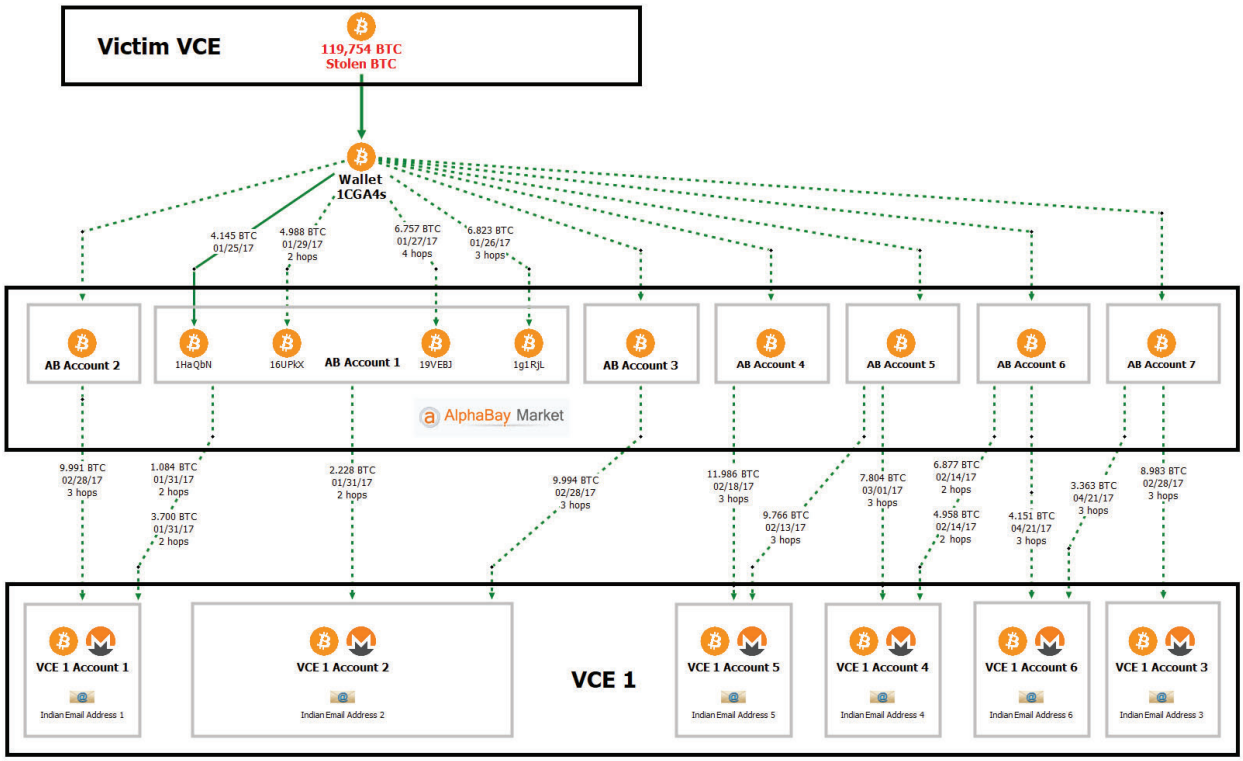
B. AlphaBay Pass-Through Activity

11. The early movement of the stolen funds involved extensive layering activity that employed the peel chain technique.[16] As part of this layering, a portion of the stolen funds were deposited gradually (an indication of peel chain activity) into AlphaBay accounts.

12. The AlphaBay accounts were used as a pass-through for the stolen BTC. Depositing and withdrawing BTC at AlphaBay allowed LICHTENSTEIN and MORGAN to break up the stolen BTC trail on the blockchain. After being moved into accounts at AlphaBay, the stolen BTC was withdrawn, layered, and ultimately deposited into VCEs around the world, as described in pertinent part immediately below.

C. Tracing the Stolen funds through AlphaBay to VCE 1, 2, 3, and 4

13. The chart below shows part of the movement of the stolen funds from Victim VCE to AlphaBay (abbreviated "AB" in some places), and then from AlphaBay to VCE 1:[17]



[16] A "peel chain" occurs when a large amount of BTC sitting at one address is sent through a series of transactions in which a slightly smaller amount of BTC is transferred to a new address each time. In each transaction, some quantity of BTC "peel off" the chain to another address (frequently, to be deposited into a VCE), and the remaining balance is transferred to the next address in the chain. In my training and experience, I know that it is common for money launderers to rely on a peel chain to obstruct the movement of the illicit money.

[17] As previously stated, showing all of the hops and connections between accounts in a single chart would make these charts very difficult to read. Throughout this affidavit, each chart is used to highlight pertinent transactions for the purpose of showing the flow of funds and establishing probable cause.

14. As depicted in the chart above, a portion of funds laundered through AlphaBay were sent to six VCE 1 accounts ("VCE 1 Account 1" through "VCE 1 Account 6"). Records from VCE 1 showed that these six accounts were all registered using email addresses hosted by the same India-based email provider. Those records also showed that there were two other similar accounts at VCE 1 registered using an email address from that same India-based provider: "VCE 1 Account 7" and "VCE 1 Account 8."

15. The relevant VCE 1 accounts were registered in the names of third parties unrelated to LICHTENSTEIN and MORGAN. VCE 1 was unable to verify the identities of any of the listed account owners. Specifically, in February and March 2017, VCE 1's employees requested that the registered accountholders for seven of the accounts provide additional identifying information to verify their account ownership. VCE 1 did not receive a response to these requests. As a result, VCE 1 froze[18] the accounts. In total, the accounts contained over $186,000 U.S. dollars' worth of virtual currency at the time, in or around April 2017.[19]

16. The above-referenced eight VCE 1 accounts shared notable commonalities leading investigators to believe that they were owned by the same individual. Specifically, overlapping subsets of the accounts: (1) were tied to similarly styled email addresses hosted by the same India-based provider; (2) were accessed by the same IP addresses; (3) were created around the same time period surrounding the hack of Victim VCE in or around August 2016; (4) were engaged in similar trading patterns entailing chain hopping[20] to anonymity-enhanced virtual currency; and/or (5) were abandoned following a request for additional know-your-customer (KYC)[21] information. The connection among the VCE 1 accounts was further confirmed upon reviewing a spreadsheet saved to LICHTENSTEIN's cloud storage account. The spreadsheet included the log-in information for accounts at various virtual currency exchanges and a notation regarding the status of the accounts. Six of the VCE 1 accounts referenced above were included in the spreadsheet, with a notation indicating "FROZEN." In other words, LICHTENSTEIN possessed a document with the login information for the accounts at VCE 1 that received funds traceable to the hack of Victim VCE and that reflected his knowledge that the accounts had been frozen.

17. Further blockchain analysis revealed that stolen funds moved through AlphaBay were also sent to accounts at a foreign VCE ("VCE 2") and a U.S.-based VCE ("VCE 4"). Those accounts were registered using an email address associated with the above-referenced India-based email provider. The log-in details for those accounts at VCE 2 and VCE 4, including the VCE's name and the email address hosted by the India-based provider, were included in the spreadsheet found in LICHTENSTEIN's cloud storage account.

---

[18] As part of their anti-money laundering practices, financial institutions may "freeze" funds or accounts—that is, disable withdrawals—where they suspect the accounts are being used for illegal activity.

[19] The funds contained within VCE 1 Accounts 1 through 8 (excluding VCE 1 Account 6) have been seized by law enforcement pursuant to a separate investigation.

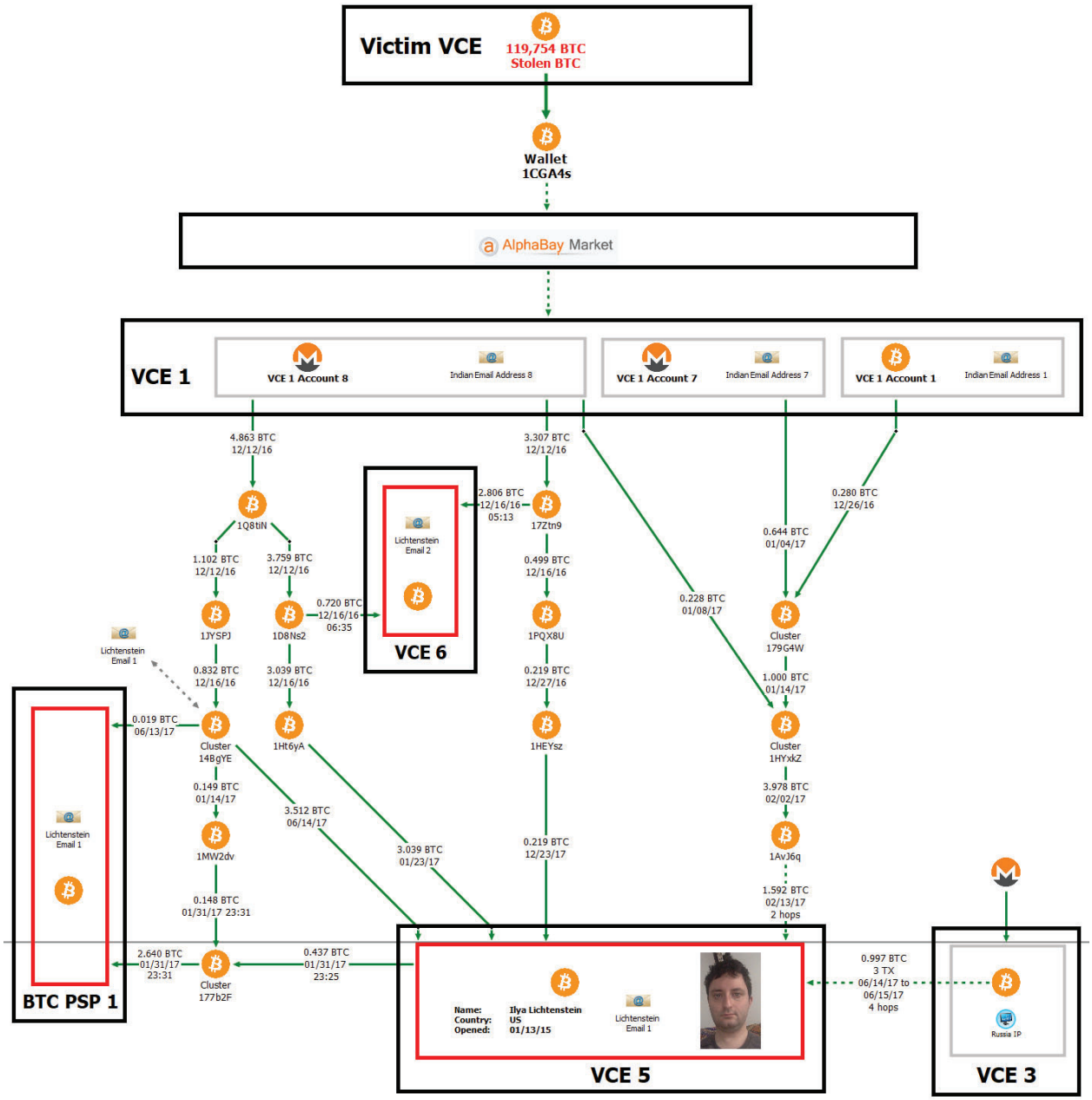
[20] Chain-hopping is a money laundering technique involving converting one form of virtual currency to another, making the transaction paths more difficult to track.

[21] Know-your-customer (KYC) information is information about customers and their activities that financial institutions collect as part of their AML procedures.

18. The account at VCE 2 converted BTC to Dash, another form of virtual currency. Shortly thereafter, two accounts at VCE 4 received Dash deposits. Those VCE 4 accounts were registered to emails contained in the account spreadsheet located on LICHTENSTEIN's cloud storage account.

D. Following the Stolen Funds to an Account at VCE 5 in the Name Ilya LICHTENSTEIN

19. Special agents continued to trace the stolen funds moved through VCE 1 prior to the accounts being frozen by VCE 1. The funds were sent to various locations, including through multiple unhosted BTC addresses to an account at another U.S.-based VCE ("VCE 5") in LICHTENSTEIN's name ("Lichtenstein's VCE 5 Account"). As illustrated below, the withdrawals from multiple VCE 1 accounts merge together as they flow through a peel chain and ultimately fund a deposit on or about February 13, 2017, to Lichtenstein's VCE 5 account (as well as other deposits in January, June, and December 2017):



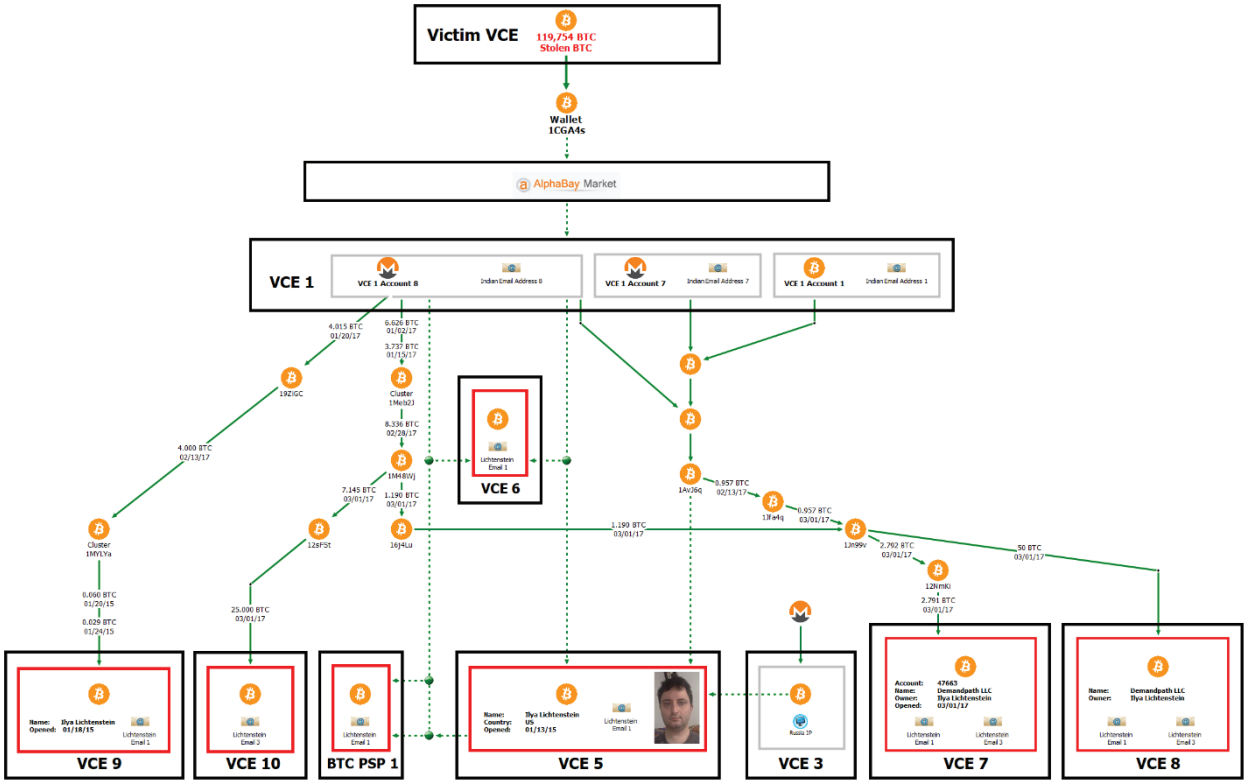
20. Records from VCE 5 showed that Lichtenstein's VCE 5 Account was opened on or about January 13, 2015, in his name and using his address at the time in San Francisco. The account was verified with photographs of LICHTENSTEIN's California driver's license and a selfie-style photograph. The account was registered to an email address containing LICHTENSTEIN's first name ("Lichtenstein Email 1"). Search warrants for the contents of the Lichtenstein Email 1 account confirmed that LICHTENSTEIN controlled the account, as well as a related account which included LICHTENSTEIN's nickname ("Lichtenstein Email 2").

21. Lichtenstein's VCE 5 Account was used to purchase gold from a precious metals dealer through a U.S.-based virtual currency payment service provider ("BTC PSP 1").[22] In conducting the transaction, LICHTENSTEIN provided his true home address for shipment.

E. Tracing the Stolen Funds to LICHTENSTEIN and MORGAN's Accounts at Additional VCEs

i. Overview of LICHTENSTEIN's Activity

22. Additional funds traced to the Victim VCE theft were also sent to LICHTENSTEIN's accounts at five more VCEs: "VCE 6," "VCE 7," "VCE 8," "VCE 9," and "VCE 10." Specifically, the chart below shows that a portion of the stolen funds flowed from VCE 1 Account 1, VCE 1 Account 7, and VCE 1 Account 8, through multiple transactions into accounts at VCE 7, VCE 8, VCE 9, and VCE 10:



23. Records obtained from the various VCEs showed that the accounts were opened in LICHTENSTEIN's name and/or the name of LICHTENSTEIN's businesses. Many of the accounts were verified with additional information and/or identification documents provided by LICHTENSTEIN. For example, in a KYC verification email from VCE 10 in 2019, LICHTENSTEIN wrote to representatives from VCE 10 that he has "been investing in and mining [BTC] since 2013, so the source of funds would be those early crypto assets."

[22] BTC PSP 1 is a VCE service that accepts virtual currency on behalf of a merchant and then remits payment to the merchant in fiat currency, such as the U.S. dollar. This allows a merchant to offer BTC as a means of payment for customers without requiring the merchant itself to handle the BTC.

24. Between the 2016 hack and the present, LICHTENSTEIN and MORGAN further engaged in a diverse array of virtual currency transactions, including transacting in numerous altcoins, liquidating BTC through a BTC ATM,[23] and purchasing non-fungible tokens (NFTs).[24]

ii. The Flow of Funds from Accounts at VCE 4 to LICHTENSTEIN and MORGAN

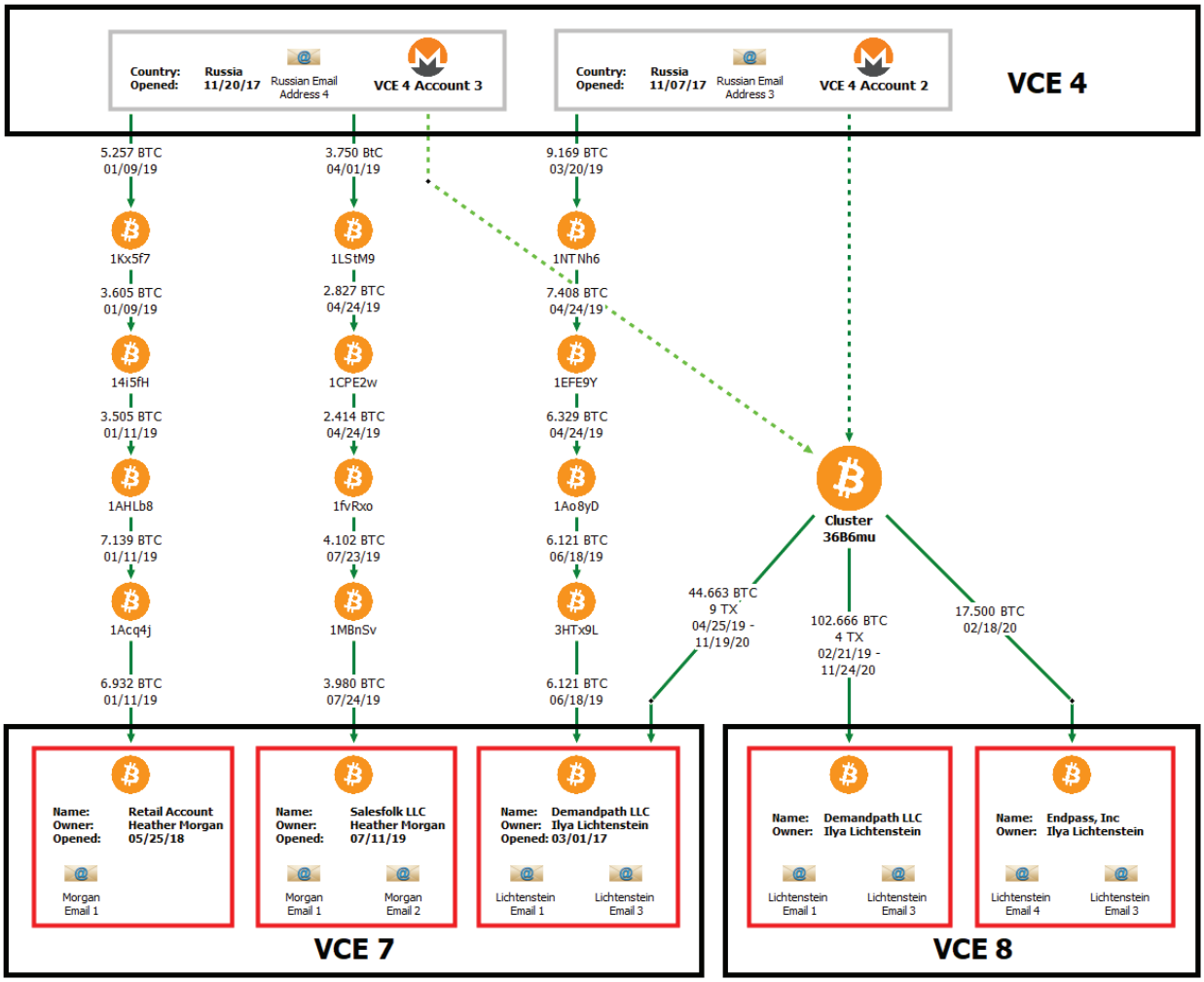
25. After scrutinizing the above-referenced flow of stolen funds into the multiple accounts connected to LICHTENSTEIN at VCE 5, VCE 6, VCE 7, VCE 8, VCE 9, and VCE 10, investigators analyzed (via publicly available information on the BTC blockchain and records obtained from the VCEs) all of the transactions into each of LICHTENSTEIN's accounts, and discovered the following:

a. A large portion of BTC deposited into LICHTENSTEIN's VCE accounts was traced back to two accounts at VCE 4. These accounts are referenced below as "VCE 4 Account 2" and "VCE 4 Account 3."

b. These two accounts at VCE 4, as depicted below, also sent funds into accounts registered to MORGAN and into another account registered to a business owned by LICHTENSTEIN called Endpass, Inc. ("Endpass").

[23] Bitcoin Automated Teller Machines (ATMs)—also called BTMs, convertible virtual currency kiosks or crypto ATMs—are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. BTC ATMs are types of VCEs and are regulated by FinCEN.

[24] Non-fungible tokens (NFTs) are blockchain-based digital units used to transfer or validate ownership of unique items, such as artwork.



26. Records from VCE 4 showed that VCE 4 Account 2 was created on or about November 7, 2017, and was registered in the name of a Russian national and under a Russian email address. VCE 4 Account 2 was entirely funded by approximately 13,200 XMR,[25] via approximately 21 transactions that took place between in or around November 2017 and March 2019.

27. Another account at VCE 4 ("VCE 4 Account 3") was created on or about November 20, 2017, and was registered in the name of another Russian national and under another Russian email address. VCE 4 Account 3 was entirely funded by approximately 6,870 XMR, via approximately 10 transactions that took place between in or around November 2017 and April 2019.

[25] Monero (XMR) is a virtual currency designed to increase users' anonymity.

28. When employees from VCE 4 attempted (via email) to verify the identity of the individual listed as the owner of VCE 4 Account 2, the account owner represented to employees from VCE 4 that the source of funds was the owner's investments. Employees from VCE 4 followed up with the owner of VCE 4 Account 2 and asked the owner to provide a bank or investment statement to support that the source of funds within the account was from the owner's investments. The owner did not respond and never contacted VCE 4 again. As a result, VCE 4 froze VCE 4 Account 2. In the end, the owner of VCE 4 Account 2 abandoned the account with approximately $155,000 worth of virtual currency in it.

29. When employees from VCE 4 attempted to verify the identity of the individual named on the account for VCE 4 Account 3, the owner never responded. VCE 4 froze that account. It had no balance at the time, as all of the funds had been withdrawn previously.

30. The XMR deposited into VCE 4 Account 2 and VCE 4 Account 3 was all converted to BTC and then withdrawn, consistent with chain hopping. The same method was used to liquidate the funds from the VCE 1 accounts as described above.

iii. Deposits into MORGAN's Accounts at VCE 7

31. According to records provided by VCE 7 (and as illustrated above in paragraph 25), VCE 4 Account 3 deposited BTC into two accounts owned by MORGAN: one account in MORGAN's name ("Morgan's VCE 7 Account") and one in the name of her company, SalesFolk LLC ("SalesFolk") ("Morgan's SalesFolk VCE 7 Account"). MORGAN responded to VCE 7's requests for KYC verification by using SalesFolk email addresses in MORGAN's name (Morgan Email 1) and initials (Morgan Email 2). In those communications, MORGAN sent SalesFolk's incorporation documents and advised VCE 7 that she was the sole owner of SalesFolk. Records from VCE 7 also indicated that another email address containing MORGAN's name (Morgan Email 3) was connected to the two accounts under MORGAN's name and company details at VCE 7.

32. As described in more detail below, MORGAN advised representatives from VCE 7 that SalesFolk accepted BTC as payment from customers. However, special agents were unable to corroborate MORGAN's statement with any actual payment details or publicly available information about SalesFolk's acceptance of BTC as payment, with one exception, an account in SalesFolk's name at BTC PSP 1. That account received approximately $130,000 worth of virtual currency from a single company ("Shell Company 1"), which claimed to operate out of Hong Kong. The payment was purportedly for advertising services. However, Shell Company 1 had no website, and investigators were unable to identify any legitimate business activity by Shell Company 1, much less any advertising.

iv. LICHTENSTEIN and MORGAN's Misrepresentations to VCE 7

33. According to the records provided by VCE 7, LICHTENSTEIN's VCE 7 Account and MORGAN's two VCE 7 accounts (Lichtenstein's VCE 7 Account, Morgan's VCE 7 Account, and Morgan's SalesFolk VCE 7 Account) shared logins from the same IP addresses that

investigators geo-located to New York. In total, their three accounts at VCE 7 received around $2.9 million worth of BTC for the approximate period of March 1, 2017, to October 24, 2021, all after the hack of Victim VCE. Nearly all of the BTC received was converted to fiat currency and withdrawn to U.S. financial institution (USFI)[26] accounts held by MORGAN and LICHTENSTEIN. Business records show that the three primary financial accounts used by MORGAN to receive fiat currency that had been converted from BTC were all opened after the hack of Victim VCE.

34. Records from VCE 7 also showed that MORGAN and LICHTENSTEIN both provided false information to VCE 7 in relation to their accounts. More specifically, as part of VCE 7's AML/KYC policies, employees from VCE 7 asked LICHTENSTEIN various questions about his source of funds, his business, and the nature of his account at VCE 7 (Lichtenstein's VCE 7 Account). According to records provided by VCE 7, LICHTENSTEIN represented via email to VCE 7 that he would be using his VCE 7 account to trade only his own virtual currency that he had acquired as a result of his early investment in BTC. Specifically, on February 27, 2017, LICHTENSTEIN wrote the following to representatives from VCE 7: "Hi, I'm a tech entrepreneur and [BTC] early adopter since acquiring my first BTC in 2011. I'm looking to diversify a bit ahead of the ETF decision and sell about 100BTC. Please let me know the next steps to move forward. All trades I would execute are from my own personal funds, the LLC is simply there to manage my trading assets."

35. As noted above, according to the public blockchain and records obtained from VCEs, the primary source of funding for LICHTENSTEIN's VCE 7 account came from the aforementioned VCE 4 accounts (*i.e.*, the VCE accounts tied to Russian identity documents), opened after the hack of Victim VCE, not from early investment earnings.

36. In response to a VCE 7 representative's request for additional information about his company Demandpath LLC, LICHTENSTEIN stated that Demandpath LLC was a "simple single-member LLC," and so it did not have "articles of incorporation or a board of directors." LICHTENSTEIN also stated that he was the "sole beneficiary with 100% ownership."

37. As noted above, MORGAN had two accounts at VCE 7: a retail account and an institutional account. MORGAN represented via email to VCE 7 that she would be using her accounts at VCE 7 to receive funds from her business clients and also to transact with her own virtual currency. MORGAN claimed that the source of digital assets that would be deposited in her institutional account would be virtual currency that she had received in 2014 and 2015 from LICHTENSTEIN. This claim is belied by the blockchain, which shows that her virtual currency accounts received the bulk of deposits from the above-referenced accounts at VCE 4 and received none from identifiable business clients. This fraud is documented as follows:

a. On August 28, 2018, MORGAN reached out to VCE 7 representatives in regard to her retail account, asking for a limit increase (*i.e.*, she wanted to transact in higher

[26] Though VCEs are financial institutions under the Bank Secrecy Act, USFI is used in this affidavit to refer to non-VCE financial institutions, such as banks.

volume and was being blocked from doing so). MORGAN stated, "I tried to do a withdrawal for $8000 to my bank account that I sold in order to pay some upcoming bills, and was told that I could only transfer $500 a day via ACH or $15,000/month via wire."

b. Then, in or around June 2019, MORGAN applied for her institutional account. On June 27, 2019, a representative from VCE 7 reached out to MORGAN for information about how her business (SalesFolk) interacts with virtual currency and how her new institutional account would be used. MORGAN responded: "SalesFolk has some B2B customers that pay with cryptocurrency. Additionally, I also have some personal cryptocurrency of my own that I would like to sell to finance the development of some new software that we are beginning to build. Because the company is an LLC taxed as an S corp it has pass-through taxation and I am the sole owner. I was going to use some of my personal crypto to fund out new software projects."

c. On July 1, 2019, MORGAN stated that SalesFolk was not a financial institution, and so she does not manage her customers' money in any way. "[SalesFolk's customers are] just B2B companies buying software and/or sales/email marketing consulting services from us, typically around $8500 or less per contract/invoice, so we haven't been doing any KYC on them."

d. On July 2, 2019, a representative from VCE 7 asked MORGAN some follow-up questions about how MORGAN came to own the digital assets that would be deposited into her new institutional account. Morgan stated, "My boyfriend (now husband) gifted me cryptocurrency over several years (2014, 2015,), [sic] which have appreciated. I have been keeping them in cold storage."

e. On January 15, 2020, a representative from VCE 7 reached out to MORGAN for monthly funding amounts, trading volume, and transactional activity for the account going forward. MORGAN replied that she anticipated that monthly funding activity would be approximately "10-30K USD" and the trading volume would be "10-20k on average."

f. As previously stated, although MORGAN advised representatives from VCE 7 that SalesFolk received virtual currency from some of her customers, investigators were not able to locate anything on the SalesFolk website referencing accepting or dealing with cryptocurrency. While it is possible that SalesFolk received virtual currency, based on my experience, companies that do offer virtual currency as a payment method or in conjunction with another service often advertise it to attract more business. To date, investigators have not identified any evidence that SalesFolk in fact received any such virtual currency payments from purported SalesFolks customers, other than the payments from Shell Company 1 discussed above. Based on my training and experience, it appears that MORGAN actually switched her VCE 7 account to a business account from a personal account in order

to receive less scrutiny from VCE 7 about her transactions as she liquidated her BTC in greater volume.

38. In sum, MORGAN and LICHTENSTEIN each advised VCE 7 that the source of the BTC deposited into their accounts came from their own investments dating to before 2015. However, detailed blockchain analysis, as illustrated in part above, revealed that the primary source of the BTC was the VCE 4 accounts that were opened in 2017 after the hack. These facts contradict MORGAN's and LICHTENSTEIN's representations to VCE 7 about the source of the funds.

39. Records obtained from other VCEs and traditional financial institutions revealed that MORGAN and LICHTENSTEIN made similar deceptive statements to other financial institutions over the course of their conspiracy.

v. Deposits into LICHTENSTEIN's and MORGAN's Accounts at VCE 8

40. According to records provided by VCE 8, two accounts at VCE 8 were owned by LICHTENSTEIN, with one in the name of Demandpath ("Lichtenstein's VCE 8 Account 1") and the other in the name of Endpass ("Lichtenstein's VCE 8 Account 2").

41. The records also showed that LICHTENSTEIN represented via email to VCE 8 that he would be using his VCE 8 account to trade virtual currency that he had acquired as a result of his early investment in BTC and altcoins.[27] In reality, according to VCE 8 records and the blockchain, LICHTENSTEIN's VCE 8 Account 1 received the bulk of its funds directly, and indirectly, from the above-referenced VCE 4 accounts.

42. A review of Demandpath's public website revealed that it consists of approximately two sentences of text about the company, an address in New York, and a contact email account. No other public information about Demandpath could be located.

43. According to records provided by a USFI ("USFI 5"), from approximately November 2018 to August 2019, Endpass had a bank account at USFI 5. These records also showed that LICHTENSTEIN and MORGAN had multiple other business accounts at USFI 5.

44. LICHTENSTEIN and MORGAN provided statements and certain documentation to support opening their USF1 5 accounts, representing that customer payments into the account would be processed by a U.S.-based financial services and software-as-a-service company. A review of the transactions in and out of this account, as supported by the business records and the BTC blockchain, indicate that the purported Endpass account was not used for this purpose at all, as it conducted zero transactions via this financial services business. Rather, for the period of March 2018 to October 2020, the bulk of the funds received were from approximately five wires from VCE 8, totaling over $758,000. The only other significant deposit to the account was an

[27] Altcoin is a term used for virtual currency other than BTC.

approximately $11,000 U.S. Small Business Administration Paycheck Protection Program (PPP) loan advance provided in response to the COVID-19 crisis.

vi. Following the Flow of Funds from Cluster[28] 36B6mu to Accounts Owned by LICHTENSTEIN and MORGAN

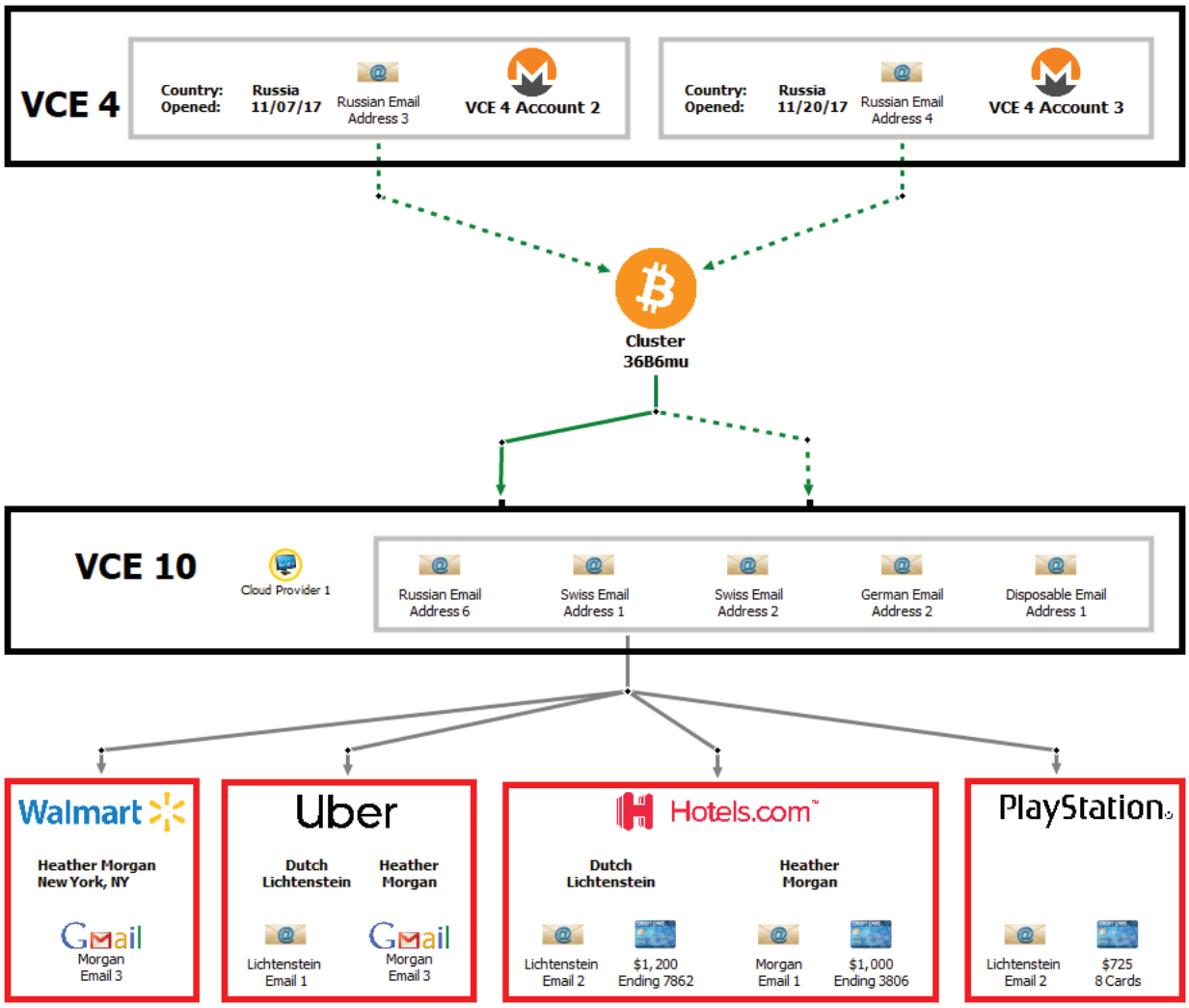
45. While conducting detailed blockchain analysis, investigators observed the importance of a specific BTC cluster ("Cluster 36B6mu"). This cluster was frequently used as an intermediary cluster between VCEs withdrawing BTC and VCE accounts owned by LICHTENSTEIN and MORGAN. This is shown in more detail below.

46. From on or about February 11, 2019, to December 14, 2020, approximately 177.116 BTC flowed through Cluster 36B6mu. A major funding source of Cluster 36B6mu was VCE 4 Account 2 and VCE 4 Account 3. The destination of BTC sent by Cluster 36B6mu was ultimately accounts owned by LICHTENSTEIN and MORGAN.

47. On or about May 3, 2020, Cluster 36B6mu sent approximately 0.057 BTC directly to VCE 10. VCE 10 is a business that sells prepaid gift cards in exchange for BTC. Records from VCE 10 showed that this specific transaction was for the purchase of a $500 gift card to Walmart from an account registered with an email address hosted by a provider in Russia and conducted via an IP address resolving to a New York City-based cloud service provider ("Cloud Provider 1"). Records from Cloud Provider 1 showed that the IP address was leased by an account in the name of LICHTENSTEIN and tied to Lichtenstein Email 1.

48. The chart below shows the movement of funds from Cluster 36B6mu to VCE 10 and the purchase of the $500 gift card:

[28] A cluster is a grouping of addresses believed to be contained within a single wallet.



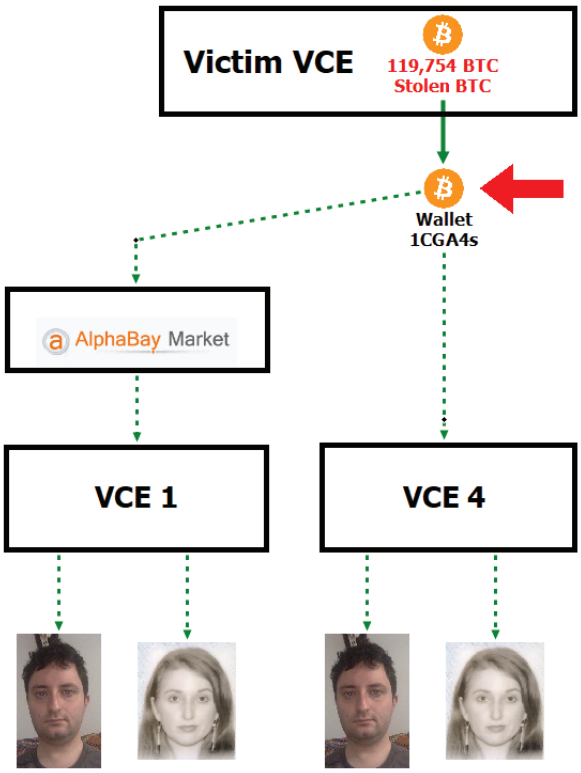
49. Records showed that portions of the $500 gift card were then redeemed through three transactions for personal items via the Walmart iPhone application. Each of the three redemptions were conducted online under MORGAN's name, using one of MORGAN's email addresses, and providing MORGAN and LICHTENSTEIN's home address for delivery.

50. Cluster 36B6mu directly sent BTC to VCE 10 for the purchase of prepaid gift cards on approximately 16 occasions, including the one described above. Although the VCE 10 accounts were registered with multiple email addresses, all but one transaction was conducted from the same Cloud Provider IP address owned by LICHTENSTEIN.

III. LICHTENSTEIN's Cloud Storage Account

51. Lichtenstein Email 2 was held at a U.S.-based provider that offered email as well as cloud storage services, among other products. In 2021, agents obtained a copy of the contents of the cloud storage account pursuant to a search warrant. Upon reviewing the contents of the account, agents confirmed that the account was used by LICHTENSTEIN. However, a significant portion of the files were encrypted.

52. On or about January 31, 2022, law enforcement was able to decrypt several key files contained within the account. Most notably, the account contained a file listing all of the addresses within Wallet 1CGA4s and their corresponding private keys. Using this information, law enforcement seized the remaining contents of the wallet, totaling approximately 94,636 BTC, presently worth $3.629 billion, as described above. The chart below singles out, with an arrow, Wallet 1CGA4s:



53. LICHTENSTEIN's cloud storage account also contained the account spreadsheet, discussed in the preceding subsections, detailing the log-in information and status of accounts at numerous VCEs, including a notation of which accounts had been frozen or emptied. As explained above, many of these accounts received stolen funds from Victim VCE.

54. Furthermore, LICHTENSTEIN's cloud storage account also contained a folder named "personas." The "personas" folder contained biographical information and identification documents for numerous individuals. The account also included a text file named "passport_ideas" that included links to different darknet vendor accounts that appeared to be offering passports or identification cards for sale.

55. LICHTENSTEIN's cloud storage account contained a folder holding data files for numerous financial institutions with notes that appear to be reconnaissance of potential laundering avenues. For example, a document for Alfa-Bank describes the bank as a "sketchy Russian oligarch bank" and includes notes about log-in procedures.

IV. LICHTENSTEIN and MORGAN's Actions Obstructed Lawful Functions of FinCEN

56. Based on my training and experience, I am aware that the Bank Secrecy Act (BSA) and its implementing regulations require financial institutions, including VCEs, to establish and maintain programs designed to detect and report suspicious activity, and to maintain certain records "where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 31 U.S.C. § 5311. Among other things, VCE and USFIs are required to comply with regulations requiring them "to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1). Specifically, VCEs and USFIs must "file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation." 31 C.F.R. § 1022.320(a)(1). This requirement may be triggered by transactions believed to involve funds derived from illegal activity or intended to hide or disguise funds or assets derived from illegal activity; transactions that serve no business or apparent lawful purpose, and for which the VCE knows of no reasonable explanation after examining the available facts; or transactions that involve the use of the virtual currency exchange to facilitate criminal activity. *Id.* § 1022.320(a)(2)(i), (iii), (iv). Such reports are commonly known as Suspicious Activity Reports ("SARs").

57. The Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of Treasury, is responsible for the implementation, administration, and enforcement of the Bank Secrecy Act. FinCEN's mission is "to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence." FinCEN is headquartered in Washington, D.C.

58. At the time of the relevant activity described above, USFI 5, VCE 1, VCE 4, VCE 5, VCE 7, VCE 8, VCE 9, and VCE 10 were financial institutions doing business in the United States, subject to the Bank Secrecy Act, and were registered with FinCEN. According to records provided by two VCEs, LICHTENSTEIN expressed his knowledge of these regulations in communications with the VCEs, telling one VCE that he chose to do business with it "to ensure that I am trading fiat in a regulated, compliant exchange," and telling another VCE that his sources of funds included "other regulated cryptocurrency exchanges." MORGAN similarly conveyed familiarity with these regulations, advising VCE 7 that, because SalesFolk was not a financial institution managing customers' funds, "we haven't been doing any KYC on [SalesFolk customers]."

59. During the course of the conspiracy, LICHTENSTEIN and MORGAN repeatedly provided false information to and deceived the VCEs and other financial institutions regarding the source of their funds and the nature of their transactions. One purpose of these deceptions was to frustrate the VCEs' due diligence efforts and thereby prevent the transmission of SARs mandated under the Bank Secrecy Act to FinCEN and the U.S. Department of the Treasury in Washington, D.C. A sample of such deceptions are included in the paragraphs above.

V. Conclusion

60. Based on the foregoing, your affiant submits that there is probable cause to believe that ILYA "DUTCH" LICHTENSTEIN and HEATHER MORGAN violated 18 U.S.C. § 1956(h), which makes it a crime in relevant part to conspire to conduct or attempt to conduct a financial transaction involving the proceeds of specified unlawful activity, knowing that the property involved in the financial transaction represents the proceeds of some form of unlawful activity, and knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity. For purposes of this section, specified unlawful activity includes wire fraud, in violation of 18 U.S.C. § 1343, and computer fraud and abuse, in violation of 18 U.S.C. § 1030.

61. Your affiant submits there is also probable cause to believe that ILYA "DUTCH" LICHTENSTEIN and HEATHER MORGAN violated 18 U.S.C. § 371, which makes it a crime in relevant part for two or more persons to conspire to defraud the United States, or any agency thereof, in any manner or for any purpose, and to do any act to effect the object of the conspiracy.

Christopher Janczewski
Special Agent
IRS-Criminal Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 7th day of February 2022.

Robin M. Meriweather
2022.02.07 11:11:48
-05'00'

ROBIN M. MERIWEATHER
U.S. MAGISTRATE JUDGE

Appendix B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA

- v. -

JOHN ALBERT LOAR BARKSDALE,

Defendant.

- - - - - - - - - - - - - - - - X

SEALED INDICTMENT

21 Cr.

21 CRIM 684

COUNT ONE
(Conspiracy to Commit Securities Fraud)

The Grand Jury charges:

Overview

1. From in or about 2017 through at least in or about October 2021, JOHN ALBERT LOAR BARKSDALE, the defendant, and his relative ("CC-1") perpetrated a scheme to sell a new cryptocurrency token named Ormeus Coin (asset symbol "ORME") through false representations. Ormeus Coin was offered to investors throughout the world, including in the United States and the Southern District of New York, through enrollment packages sold by Ormeus Global, a multi-level marketing company controlled by BARKSDALE and CC-1, various digital currency exchanges, and directly from BARKSDALE and his associates.

2. Through a series of white papers, in-person roadshows, online webinars and videos, social media platforms, and other marketing materials approved by JOHN ALBERT LOAR BARKSDALE, the

defendant, and CC-1, BARKSDALE and CC-1 falsely represented, among other things, that Ormeus Coin was a digital money system secured by a $250 million cryptocurrency mining operation, which was one of the biggest such operations in the world. In order to support the false representations regarding the size and value of cryptocurrency mining assets that purportedly secured the value of Ormeus Coin, BARKSDALE approved marketing materials that falsely depicted photos of a purported Ormeus Coin mining facility, deceptively referenced an "Ormeus Reserve Vault" ("ORV") that stored over 3,000 Bitcoin purportedly derived from Ormeus Coin's mining operations that was represented as securing the value of Ormeus Coin, and falsely stated that Ormeus Coin's mining revenues exceeded $5 million on a monthly basis. In truth, Ormeus's mining operations never approached a value close to $250 million and never produced revenues exceeding one million dollars in any month, and the Bitcoin stored in the "Ormeus Reserve Vault" belonged to a third party.

3. Numerous investors, including at least one investor in the Southern District of New York, purchased enrollment packages through Ormeus Global and purchased Ormeus Coin through digital currency exchanges or directly from JOHN ALBERT LOAR BARKSDALE, the defendant, and his associates based at least in part on BARKSDALE's false representations regarding the size, value, and

purported profitability of the cryptocurrency mining assets controlled by Ormeus Global and Ormeus Coin, as well as the purported security that the ORV provided to the value of Ormeus Coin. Through this scheme, from in or about June 2017 through at least in or about April 2018, Ormeus Global raised at least approximately $70 million from the sale of enrollment packages to more than 8,000 investors around the world. From in or about June 2017 through at least in or about October 2021, Ormeus Coin was sold to at least approximately 12,000 investors, including at least over 200 U.S.-based investors. At its peak, Ormeus Coin had a market capitalization of approximately $52 million in or about January 2018.

Background on Ormeus Global, Ormeus Coin, and Relevant Entities

4. At all times relevant to this Indictment, Ormeus Global S.A. ("Ormeus Global") was a multi-level marketing company formed in Panama and based in Hong Kong that was primarily controlled by JOHN ALBERT LOAR BARKSDALE, the defendant, who also served as the spokesperson for Ormeus Global. Ormeus Global was the issuer of Ormeus Coin. Ormeus Global also offered various bundles of goods and services referred to as "enrollment packages" that were sold to, and through, direct sales agents, or "members." Members earned commissions from 7% to 20% for recruiting other investors to

purchase enrollment packages from Ormeus Global. The enrollment packages varied in cost from $999 for a "Bronze" package to $250,000 for a "Platinum Founder" package. Each package included, among other purported benefits, a share of the proceeds generated by a proprietary cryptocurrency trading bot that was represented to earn a return of up to 160%, a "short-term mining contract" which entitled the investor to a percentage of mining revenue until the investor recouped the cost of the package, and a certain quantity of "free Ormeus Coin." Because Ormeus Global and Ormeus Coin were intertwined, they were often referred to together simply as "Ormeus."

5. At all times relevant to this Indictment, Ormeus Coin was an ERC-20 compliant smart contract-based token on the Ethereum blockchain.[1] Ormeus Coin was first offered for sale in or about June 2017 on a Hong Kong-based cryptocurrency exchange controlled by JOHN ALBERT LOAR BARKSDALE, the defendant, and CC-1, and later on other cryptocurrency exchanges or directly from BARKSDALE and his associates. In marketing materials approved by BARKSDALE, Ormeus Coin was represented to be a

[1] The Ethereum blockchain is a decentralized blockchain with smart contract functionality that can facilitate the creation of tokens that can be bought, sold, and traded. ERC-20 is the technical standard for smart contracts used to create new fungible tokens on the Ethereum blockchain.

stable, next-generation digital currency and store of value backed by real-world cryptocurrency mining assets and cryptographically linked to a publicly identifiable currency vault called the "Ormeus Reserve Vault" or "ORV." The ORV was represented to be a multi-signature wallet address where mined cryptocurrencies were deposited to secure the value of Ormeus Coin and which could be publicly verified. BARKSDALE publicly represented that the value of Ormeus Coin would increase every day based on the value of the ORV and as Ormeus's cryptocurrency mining capacity increased over time.

6. At all times relevant to this Indictment, Ormeus Coin was represented to be primarily backed by a reserve of Bitcoin (asset symbol "BTC"), a digital currency in use since 2009 that has been the most widely used and highly valued cryptocurrency in circulation to date. Bitcoin can be transferred from one Bitcoin address to another via a transaction recorded on Bitcoin's blockchain or public ledger. Bitcoin maintains its blockchain and provides for new Bitcoin to enter the economy through a consensus mechanism known as "mining." High-powered computers called "miners" that are part of Bitcoin's network engage in complex resource-intensive verifications of recent Bitcoin transactions and aggregate them into "blocks" that are added to the blockchain and can be publicly verified. As part

of this process, a miner that succeeds in adding a new block of transactions to the blockchain is rewarded with a predetermined set of newly issued Bitcoin. Other cryptocurrencies relevant to the scheme, including Dash and Litecoin, can be similarly mined.

7. At all times relevant to this Indictment, Digital Skynet Limited ("Skynet") was a Hong Kong-based company formed in or about July 2017 that entered into cryptocurrency mining-related agreements on behalf of Ormeus Global and Ormeus Coin. JOHN ALBERT LOAR BARKSDALE, the defendant, was the chief executive officer ("CEO") of Skynet and CC-1 was an authorized signatory for Skynet.

THE FRAUDULENT SCHEME

Materially False and Misleading Statements that Ormeus Coin Was Backed By a $250 Million Cryptocurrency Mining Operation

8. Beginning at least in or about November 2017, JOHN ALBERT LOAR BARKSDALE, the defendant, began speaking publicly about Ormeus's purported $250 million cryptocurrency mining operation. For example, in a webinar on or about November 7, 2017, BARKSDALE claimed that Ormeus had a contract that would result in the delivery of over $250 million worth of miners over the next 36 months and would be signing the contract in the next several weeks. Subsequently, on or about November 17, 2017, BARKSDALE, as the CEO of Skynet, entered into an agreement with

other individuals pursuant to which Ormeus Global agreed to pay a total of $250 million in Bitcoin to Skynet, which would be used to purchase mining equipment from a third party (the "Mining Supplier"). In or about December 2017, BARKSDALE directed the transfer of approximately $10 million in Bitcoin for the purchase of mining equipment for Ormeus to the Mining Supplier, but no mining equipment procured with that payment was put into operation until at least in or about March 2018.

9. Despite knowing that no mining equipment pursuant to the agreement with the Mining Supplier had actually been procured or put into operation, JOHN ALBERT LOAR BARKSDALE, the defendant, and CC-1 reviewed and approved the release of a "White Paper" on or about February 8, 2018, titled "Ormeus Coin: The Tokenization of Industrial Cryptocurrency Mining" (the "White Paper"), which was posted to Ormeus Coin's website. The White Paper stated that Ormeus Coin is a "ground-breaking digital money system secured by one of the biggest industrial cryptocurrency mining operations in the world" and "cryptographically linked to a publicly identifiable currency vault [the ORV] funded by a USD $250 million North American mining business powered by green energy." The White Paper claimed that "Ormeus Coin has already commenced its cryptocurrency mining operation through private investment and

is not seeking public money through an ICO [Initial Coin Offering]." The White Paper also stated that Ormeus would use 40% of the mining revenue to acquire additional mining equipment, that another 40% of the mining revenue would be deposited and stored in the ORV and publicly displayed, that 10% of mining revenue would be used to buy back Ormeus Coin in order to maintain a stable value, and that the remaining 10% percent of mining revenue would be used for back-end software development.

10. The White Paper included the following photograph labeled "Actual Photo of Ormeus Coin Mining Facility," which appeared to depict a vast facility containing rows of cryptocurrency mining equipment belonging to Ormeus Coin:

In reality, the facility depicted was an actual data center containing cryptocurrency mining equipment located in Montana,

but it was entirely owned and operated by a third party (the "Third-Party Mining Facility"). At the time this photograph was used to create the false appearance that Ormeus owned and operated a large mining facility, the Third-Party Mining Facility hosted at most no more than two rows of miners for Ormeus. This same photograph was used multiple times in marketing materials throughout early 2018 to create the false impression that it was a photo of an Ormeus mining facility. For example, in a Facebook post by Ormeus Global on or about January 22, 2018, the same photograph of the Third-Party Mining Facility was used in a post to announce a contest to "WIN a trip to tour the Ormeus Mining facility and more!"

11. After the release of the White Paper on or about February 8, 2018, marketing materials approved by JOHN ALBERT LOAR BARKSDALE, the defendant, continued to represent that Ormeus Coin was backed by a $250 million cryptocurrency mining operation through at least in or about April 2018. For example, on or about February 9, 2018, Ormeus Coin ran an advertisement on a jumbotron in Times Square in Manhattan, New York, which proclaimed, in a caption above a giant ORME symbol, "$250 Million Cryptocurrency Mining Farm Revealed in Legal Audit by Ormeus Coin." On or about February 12, 2018, a photograph of the Times Square advertisement was posted to Ormeus Global's

Twitter account with the caption "Live from New York City, Ormeus Coin Advertising its $250 million Cryptocurrency Mining Farm in Times Square, Manhattan!" Further, in a press release dated on or about April 12, 2018, Ormeus Coin claimed that its "highly-rated digital currency is secured by a reserve vault that is anchored to the company's USD$250 Million crypto mining operations."

12. In truth, Ormeus Coin's cryptocurrency mining operations never approached a value close to $250 million. The false statements about Ormeus Coin's purported $250 million cryptocurrency mining operation approved by and caused to be disseminated by JOHN ALBERT LOAR BARKSDALE, the defendant, helped to generate interest in and sell Ormeus Global's enrollment packages and Ormeus Coin.

Materially False and Misleading Statements that the Ormeus Reserve Vault Reflected Actual Mining Revenue

13. The White Paper released in or about February 2018 that was approved by JOHN ALBERT LOAR BARKSDALE, the defendant, and CC-1 claimed that revenue from Ormeus's mining operations would be stored in the ORV and publicly verifiable through proof of asset technology and self-executing smart contracts. As explained in the White Paper, the purpose of the ORV was to ensure "that Ormeus Coin stays linked to the real-world assets,

transparent for all to see, without susceptibility to fraud, hacking, or tampering." A link to the ORV website was posted to Ormeus Coin's website. On a tab on the ORV website labeled "Bitcoin Mining," the ORV website represented that a majority of the current ORV was backed by Bitcoin.

14. Beginning in at least September 2018, JOHN ALBERT LOAR BARKSDALE, the defendant, and CC-1 began privately negotiating with an individual with significant Bitcoin holdings ("Individual-1") to display Individual-1's Bitcoin holdings on the ORV website so that it would be appear that those assets belonged to and were securing Ormeus Coin. Prior to the completion of those negotiations, on or about November 15, 2018, BARKSDALE caused Ormeus Coin's Facebook account to post the following message: "It has been confirmed that 40% of profits from ongoing production at the mining centers are now permanently linked to a 'gold-standard' Ormeus Reserve Vault (ORV) which supports the stability of the coin. An unalterable smart contract system currently verifies regular deposits from the mining, which is cryptographically linked to the publicly identifiable currency vault."

15. The negotiations with Individual-1 culminated in an agreement on or about January 30, 2019, executed by CC-1 on behalf of Skynet, Individual-1, and an executive of Ormeus

Global, pursuant to which, among other things, Individual-1 authorized Skynet to display Individual-1's Bitcoin wallet in the ORV. Thereafter, from at least in or about January 2019 through at least in or about October 2021, the ORV website displayed that the ORV consistently contained approximately 3,081 Bitcoin in purported mining revenue, which was valued at between approximately $10 million and $188 million, depending on the value of Bitcoin during the period. Contrary to the marketing materials set forth above, the Bitcoin assets in the ORV were owned and controlled by Individual-1, and were not generated by Ormeus's mining operations and did not belong to Ormeus, JOHN ALBERT LOAR BARKSDALE, the defendant, or CC-1. Those Bitcoin assets therefore did not secure the value of Ormeus Coin.

16. Despite knowing that the Bitcoin assets depicted in the ORV actually belonged to Individual-1, JOHN ALBERT LOAR BARKSDALE, the defendant, continued to falsely represent through in or about 2019 that those Bitcoin assets consisted of mining revenue generated by Ormeus. For example, during an "Ask Me Anything" Facebook Live session with BARKSDALE that was posted to Ormeus's YouTube channel on or about July 10, 2019, BARKSDALE walked potential investors through the ORV website and falsely claimed that the approximately 3,081 Bitcoin shown on the

website were "the BTC that we've mined. Obviously, it's a phenomenal amount of BTC." The ORV website continued to falsely represent that the ORV contained approximately 3,081 Bitcoin from mining through at least in or about October 2021.

Materially False and Misleading Statements that Ormeus's Mining Operations Generated Over $5 Million in Monthly Revenue

17. Beginning in or about February 2018, JOHN ALBERT LOAR BARKSDALE, the defendant, caused Ormeus Coin to issue false public statements claiming that its mining operations were generating over $5 million in current monthly revenue. For example, the White Paper issued in or about February 2018 claimed that Ormeus Coin's "CURRENT AUDITED MINING REVENUE (SPRING 2018)" consisted of $3.4 million in monthly revenue from Bitcoin mining, $1.6 million in monthly revenue from Litecoin mining, and $350,000 in monthly revenue from Dash mining, for a total monthly revenue of $5.4 million. Then, on or about March 3, 2018, BARKSDALE used his personal Facebook account to post a link to an article which stated that a "recent independent legal and financial audit published by a leading attorney at law revealed Ormeus Coin is currently making $5.4 million per month from mining, which will increase to $6.7 million in the next two months." Finally, on or about March 26, 2018, Ormeus Coin issued a press release that claimed it had "significant North

American data centers in the Midwest and upstate New York already making almost USD$7 Million per month." Contrary to these public claims, Ormeus's mining operations did not produce revenues exceeding one million dollars in any month.

Statutory Allegations

18. From in or about 2017 through at least in or about October 2021, in the Southern District of New York and elsewhere, JOHN ALBERT LOAR BARKSDALE, the defendant, and others known and unknown, willfully, and knowingly combined, conspired, confederated and agreed together and with each other to commit offenses against the United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

19. It was a part and object of the conspiracy that JOHN ALBERT LOAR BARKSDALE, the defendant, and others known and unknown, willfully and knowingly, directly and indirectly, by the use of the means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, would and did use and employ, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section

240.10b-5, by: (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

Overt Acts

20. In furtherance of the conspiracy and to effect the illegal objects thereof, JOHN ALBERT LOAR BARKSDALE, the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. On or about February 8, 2018, BARKSDALE reviewed and approved the release of the White Paper that falsely represented that Ormeus Coin's "current audited mining revenue" was $5.4 million.

b. On or about February 12, 2018, BARKSDALE authorized an advertisement on a jumbotron in Times Square in Manhattan, New York, which falsely represented that Ormeus Coin had a $250 million cryptocurrency mining farm.

c. On or about July 10, 2019, BARKSDALE falsely claimed that Ormeus had generated approximately 3,081 Bitcoin from mining as displayed on the ORV website.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Securities Fraud)

The Grand Jury further charges:

21. The allegations set forth in paragraphs 1 through 17 are realleged and incorporated by reference as if fully set forth herein.

22. From in or about 2017 through at least in or about October 2021, in the Southern District of New York and elsewhere, JOHN ALBERT LOAR BARKSDALE, the defendant, willfully and knowingly, directly and indirectly, by the use of the means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, in connection with the purchase and sale of securities, used and employed manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section 240.10b-5, by: (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which

they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, to wit, BARKSDALE solicited investments in Ormeus Global enrollment packages and Ormeus Coin through materially false and misleading statements and omissions regarding the size and value of Ormeus's cryptocurrency mining operations and the revenue generated by those operations.

(Title 15, United States Code, Sections 78j(b) & 78ff; Title 17, Code of Federal Regulations, Section 240.10b-5; and Title 18, United States Code, Section 2.)

COUNT THREE
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

23. The allegations set forth in paragraphs 1 through 17 are realleged and incorporated by reference as if fully set forth herein.

24. From in or about 2017 through at least in or about October 2021, in the Southern District of New York and elsewhere, JOHN ALBERT LOAR BARKSDALE, the defendant, and others known and unknown, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

25. It was a part and an object of the conspiracy that JOHN ALBERT LOAR BARKSDALE, the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, BARKSDALE and others engaged in a scheme to solicit investments in Ormeus Global enrollment packages and Ormeus Coin through materially false and misleading statements and omissions regarding the size and value of Ormeus's cryptocurrency mining operations and the revenue generated by those operations, and used and caused the use of interstate wire communications in furtherance of those acts.

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

COUNT FOUR
(Wire Fraud)

The Grand Jury further charges:

26. The allegations set forth in paragraphs 1 through 17 of this Indictment are realleged and incorporated by reference as if fully set forth herein.

27. From in or about 2017 through at least in or about October 2021, in the Southern District of New York and elsewhere, JOHN ALBERT LOAR BARKSDALE, the defendant, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce writings, signs, signals, pictures and sounds for the purpose of executing such scheme and artifice, to wit, BARKSDALE solicited investments in Ormeus Global enrollment packages and Ormeus Coin through materially false and misleading statements and omissions regarding the size and value of Ormeus's cryptocurrency mining operations and the revenue generated by those operations, and used and caused the use of interstate wire communications in furtherance of those acts.

(Title 18, United States Code, Sections 1343 and 2.)

FORFEITURE ALLEGATION

28. As a result of committing one or more of the offenses alleged in Counts One through Four of this Indictment, JOHN ALBERT LOAR BARKSDALE, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c),

any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

29. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code,

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

(Title 18, United States Code, Section 981,
Title 21, United States Code, Section 853, and
Title 28, United States Code, Section 2461.)

[redacted]

FOREPERSON

No. 9 2021

Damian Williams/JV

DAMIAN WILLIAMS
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOHN ALBERT LOAR BARKSDALE,

Defendant.

SEALED INDICTMENT

21 Cr. ___

(Title 15, United States Code, Sections 78j(b) and 78ff; Title 17, Code of Federal Regulations, Section 240.10b-5; and Title 18, United States Code, Sections 371, 1343, 1349, and 2.)

DAMIAN WILLIAMS
United States Attorney.

A TRUE BILL

Foreperson.

[redacted]

11/9/21 Filed indictment under seal, arrest warrant issued.
K. N. Fox
USMJ

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com