AlaFile E-Notice

50-CV-2025-900202.00

To: BRIAN KEITH JACKSON
kj@rileyjacksonlaw.com

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF MARSHALL COUNTY, ALABAMA

MICHAEL MASHKEVICH V. OLIVIA AVA ET AL
50-CV-2025-900202.00

The following complaint was FILED on 6/18/2025 10:56:53 AM

Notice Date: 6/18/2025 10:56:53 AM

ANGIE JOHNSON
CIRCUIT COURT CLERK
MARSHALL COUNTY, ALABAMA
424 BLOUNT AVE.
SUITE 201
GUNTERSVILLE, AL, 35976

256-571-7785
angie.johnson@alacourt.gov

ELECTRONICALLY FILED
6/18/2025 10:56 AM
50-CV-2025-900202.00
CIRCUIT COURT OF
MARSHALL COUNTY, ALABAMA
ANGIE JOHNSON, CLERK

State of Alabama Unified Judicial System Form ARCiv-93 Rev. 9/18	**COVER SHEET** **CIRCUIT COURT - CIVIL CASE** (Not For Domestic Relations Cases)	Cas 50 Date of Filing: 06/18/2025 Judge Code:

GENERAL INFORMATION

IN THE CIRCUIT COURT OF MARSHALL COUNTY, ALABAMA
MICHAEL MASHKEVICH v. OLIVIA AVA ET AL

First Plaintiff: ☐ Business ☑ Individual ☐ Government ☐ Other

First Defendant: ☐ Business ☑ Individual ☐ Government ☐ Other

NATURE OF SUIT: Select primary cause of action, by checking box (check only one) that best characterizes your action:

TORTS: PERSONAL INJURY
- ☐ WDEA - Wrongful Death
- ☐ TONG - Negligence: General
- ☐ TOMV - Negligence: Motor Vehicle
- ☐ TOWA - Wantonness
- ☐ TOPL - Product Liability/AEMLD
- ☐ TOMM - Malpractice-Medical
- ☐ TOLM - Malpractice-Legal
- ☐ TOOM - Malpractice-Other
- ☐ TBFM - Fraud/Bad Faith/Misrepresentation
- ☐ TOXX - Other: _____

TORTS: PERSONAL INJURY
- ☐ TOPE - Personal Property
- ☐ TORE - Real Properly

OTHER CIVIL FILINGS
- ☐ ABAN - Abandoned Automobile
- ☐ ACCT - Account & Nonmortgage
- ☐ APAA - Administrative Agency Appeal
- ☐ ADPA - Administrative Procedure Act
- ☐ ANPS - Adults in Need of Protective Service

OTHER CIVIL FILINGS (cont'd)
- ☐ MSXX - Birth/Death Certificate Modification/Bond Forfeiture Appeal/ Enforcement of Agency Subpoena/Petition to Preserve
- ☐ CVRT - Civil Rights
- ☐ COND - Condemnation/Eminent Domain/Right-of-Way
- ☐ CTMP - Contempt of Court
- ☐ CONT - Contract/Ejectment/Writ of Seizure
- ☑ TOCN - Conversion
- ☐ EQND - Equity Non-Damages Actions/Declaratory Judgment/ Injunction Election Contest/Quiet Title/Sale For Division
- ☐ CVUD - Eviction Appeal/Unlawful Detainer
- ☐ FORJ - Foreign Judgment
- ☐ FORF - Fruits of Crime Forfeiture
- ☐ MSHC - Habeas Corpus/Extraordinary Writ/Mandamus/Prohibition
- ☐ PFAB - Protection From Abuse
- ☐ EPFA - Elder Protection From Abuse
- ☐ QTLB - Quiet Title Land Bank
- ☐ FELA - Railroad/Seaman (FELA)
- ☐ RPRO - Real Property
- ☐ WTEG - Will/Trust/Estate/Guardianship/Conservatorship
- ☐ COMP - Workers' Compensation
- ☐ CVXX - Miscellaneous Circuit Civil Case

ORIGIN: F ☑ **INITIAL FILING** A ☐ **APPEAL FROM DISTRICT COURT** O ☐ **OTHER**
R ☐ **REMANDED** T ☐ **TRANSFERRED FROM OTHER CIRCUIT COURT**

HAS JURY TRIAL BEEN DEMANDED? ☐ **YES** ☑ **NO**
Note: Checking "Yes" does not constitute a demand for a jury trial. (See Rules 38 and 39, Ala.R.Civ.P, for procedure)

RELIEF REQUESTED: ☑ **MONETARY AWARD REQUESTED** ☐ **NO MONETARY AWARD REQUESTED**

ATTORNEY CODE:
JAC067 6/18/2025 10:56:50 AM (Date) /s/ BRIAN KEITH JACKSON (Signature of Attorney/Party filing this form)

MEDIATION REQUESTED: ☐ **YES** ☐ **NO** ☑ **UNDECIDED**

Election to Proceed under the Alabama Rules for Expedited Civil Actions: ☐ **YES** ☑ **NO**

ELECTRONICALLY FILED
6/18/2025 10:56 AM
50-CV-2025-900202.00
CIRCUIT COURT OF
MARSHALL COUNTY, ALABAMA
ANGIE JOHNSON, CLERK

DOCUMENT 2

IN THE CIRCUIT COURT OF MARSHALL COUNTY, ALABAMA

MICHAEL MASHKEVICH, on behalf of himself and all others similarly situated, Plaintiff, v. OLIVIA AVA, EMMA MILLER, F.B. LEE, ZHENG WENCHAO, 李波 a/k/a BO LI, SUN QI, হাসান তারেক a/k/a HASAN TAREQ, প্রেমনন্দ সরকার a/k/a PREMANANDA SARDAR, 黄金明 a/k/a JINMING HUANG, ဇေယျာဇေအေးကြည် a/k/a ZEYE AYE KYAW, اسد علي a/k/a ASAD ALI, 吴儒 a/k/a RUDONG WU, 黎威标 a/k/a WEIBIAO LI, 王龑 a/k/a YAN WANG, 郝龙飞 a/k/a LONGFEI HAO, 李佳鹏 a/k/a JIAPENG LI, 刘乌烘 a/k/a WUHONG LIU, MANH CUONG NGUYEN, 王军龙 a/k/a JUNLONG WANG, 郭宗斌 a/k/a GUO ZONGBIN, FICTITIOUS DEFENDANTS "A" – "F", being the true and correct identity of the individuals identified herein if Plaintiff has inadvertently misidentified any of the Defendants; FICTITIOUS DEFENDANTS "G" – "K", being the true and correct identity of the business entities, individuals, and employees, agents, or servants of the same who or that participated in the scam and laundering network at issue herein and whose identities are not currently known to the Plaintiff; FICTITIOUS DEFENDANTS "L" – "Z", being the true and correct identity of the business entities, individuals, and employees, agents, or servants of any of the named or fictitious defendants who participated in the conduct at issue in this case, including any defendants whose identities are currently unknown to Plaintiff who solicited Plaintiff using electronic means, who designed the fake work platforms Plaintiff utilized, who participated in receiving, forwarding, or otherwise disposing of Plaintiff's cryptocurrency, who initiated or opened any of the cyberwallets into which Plaintiff's cryptocurrency was deposited, who had or exercised control over any of the cyberwallets into	Civil Action No. _____ **CLASS ACTION**

which Plaintiff's cryptocurrency was deposited, or who otherwise participated in any way in the "pig butchering" schemes of which Plaintiff was a victim. The identities of Defendants "A"- "Z" are currently unknown to Plaintiff but will be added when Plaintiff ascertains their true identities through discovery.

Defendants.)

COMPLAINT

Class Plaintiff Michael Mashkevich ("Plaintiff"), by and through his undersigned counsel, Riley & Jackson, P.C., brings this Complaint for claims of conversion, civil conspiracy, and related equitable remedies against Defendants, and alleges as follows:

INTRODUCTION

1. Defendants Olivia Ava, Emma Miller, F.B. Lee, Zheng Wenchao, 李波 a/k/a Bo Li, Sun Qi, হাসান তারেক a/k/a Hasan Tareq, প্রেমনন্দ সরকার a/k/a Premananda Sardar, 黄金明 a/k/a Jinming Huang, ဇေယျာဇေးကြည် a/k/a Zeye Aye Kyaw, اسد علی a/k/a Asad Ali, 吴儒 a/k/a Rudong Wu, 黎威标 a/k/a Weibiao Li, 王龑 a/k/a Yan Wang, 郝龙飞 a/k/a Longfei Hao, 李佳鹏 a/k/a Jiapeng Li, 刘乌烘 a/k/a Wuhong Liu, Manh Cuong Nguyen, 王军龙 a/k/a Junlong Wang, 郭宗斌 a/k/a Guo Zongbin, and fictitious defendants ("collectively Defendants") have worked and conspired together, either directly or indirectly, as part of or with individuals and businesses that operate a cryptocurrency scam and laundering network. The Defendants and fictitious party defendants either actively participated in the scams at issue by contacting Mashkevich and other Class Members or were part of the crypto laundering network acting as crypto mules, as owners of crypto wallets used as destinations to blend and cloak stolen crypto, or otherwise. Defendants who were scammers directly interacting with Mashkevich and Class Members and Defendants who were involved in the laundering process are all critical components of the scam at issue, as

DOCUMENT 2

the laundering network transfers stolen crypto along the blockchain, occasionally bridging stolen crypto, and ultimately off-ramping the crypto so that it can no longer be traced. All Defendants acted as part of a larger conspiracy to deprive Mashkevich and the Class Members of their crypto.

2. Defendants, including the fictitious party Defendants, conspired to execute an online theft scheme known as "pig butchering," whereby they used fraudulent representations to steal large amounts of crypto from scores of innocent victims and then laundered the stolen crypto. The Defendants insidiously lure unsuspecting targets into buying cryptocurrency and transferring it to accounts (also known as "wallets") they control. Once transferred, the Defendants steal the cryptocurrency and attempt to render it untraceable by transferring and laundering the funds via a well-established scam network of related wallets operated by the Defendants. The victims suffer a total loss of their cryptocurrency and the funds used to purchase it.

DOCUMENT 2

3. The pig butchering scheme in the instant case relies on confidence scams. The Defendants gain the victims' trust by feigning empathy and telling cleverly disguised lies to induce them to transfer increasing amounts of cryptocurrency to wallets under the Defendants' control. The Defendants first solicit victims by sending boilerplate inquiries about investment opportunities or part-time work. After a person responds to a message, one or more Defendants contact that person and describe the opportunities, all of which have the purported potential of earning the victim significant income by completing seemingly legitimate work tasks for well-known companies or by making seemingly legitimate investments.

4. The Defendants used this specious scheme to lure a common class of victims ("Class Members," or the "Class") to transfer funds to cryptocurrency wallets controlled by the Defendants. The Class in this matter is defined as all persons and entities who, at the suggestion of the Defendants or individuals acting under the Defendants' instruction or control, transferred,

through June 4, 2024, cryptocurrency into one or more of the cryptocurrency wallets identified in Appendix A and other scam wallet addresses controlled by the Defendants as may be identified during discovery, or who had their cryptocurrency deposited into the same wallets by the Defendants. The wallets identified on Appendix A are hereinafter referred to as "the Destination Wallets."

5. Mashkevich has confirmed through various exchanges that the Defendants identified herein own and/or control one or more of the wallets identified on Appendix A.

6. With respect to Mr. Mashkevich specifically, Defendants represented that part-time work Mr. Mashkevich would be doing involved real and legitimate online tasks, including tasks related to software applications at real companies (e.g., Grayphite, Resy, or inMobi) and that anyone can and should confirm the work platform's legitimacy by searching online for the official website of these companies. Defendants represented that other websites they control, which include the names of legitimate companies as part of the website link (e.g., https://www.appgrayphiteglobal.com or https://www.cozyrestaurant-du.com/en/home), are part of the work platform. Defendants further represented that, after training, a person working on a platform will earn commissions based on tasks performed. The commissions are purportedly based on a standardized income schedule with ranges of thousands of dollars per month. Defendants emphasized in standardized language the convenience of the remote work online, the absence of fixed time limits, the flexibility, and the preferred working hours.

7. The Defendants followed a standardized roadmap to persuade Class Members to transfer cryptocurrency to the Destination Wallets controlled by Defendants or their co-conspirators. First, the Defendants requested that Class Members contribute a small amount of funds to set up their respective accounts. Then the Defendants represented that Class Members had

DOCUMENT 2

earned money and permitted Class Members to withdraw that money. The Defendants then represented that Class Members needed to transfer additional funds to their accounts for standardized, boilerplate reasons, including increasing their earning potential, their account balance had gone negative, they owed taxes, or due to a problem with loans from other investment or work platform members. After the Defendants persuaded Class Members to deposit additional cryptocurrency, they stole the cryptocurrency and transferred it along a well-established scam cryptocurrency laundering network—controlled by Defendants, fictitious party Defendants, and their co-conspirators—(the "Laundering Network") until it arrived at various wallets held at cryptocurrency exchanges.

8. The Class Members initially deposit their cryptocurrency into cryptocurrency wallets controlled by the Defendants, which Defendants use to take possession of victims' cryptocurrency. These wallets represent the first node of the Laundering Network Defendants use to conceal their actions. The second node of the Laundering Network involves thirteen pass-through "pivot" wallets (the "Pivot Wallets"). Defendants or their co-conspirators transferred the Class Members' stolen cryptocurrency from the original deposit wallets to the pivot wallets, which served as focus points for aggregating stolen funds from multiple victims before the cryptocurrency was sent to various other wallets in the laundering network, all with the design and intent of blending and cloaking the stolen cryptocurrency.

9. The final node of the Laundering Network involves the reconsolidation of the stolen cryptocurrency into wallets on cryptocurrency exchanges, enabling Defendants or their co-conspirators to convert and liquidate the stolen assets. The Destination Wallets currently holding Class Members' stolen cryptocurrency, as identified in Appendix A, facilitate the conversion of

DOCUMENT 2

these assets into usable fiat or other currencies, thereby permanently placing them beyond the reach of Class Members.

10. Plaintiff is a resident of Albertville, Alabama. Like other similarly situated Class Members, Plaintiff was tricked by one or more Defendants, including persons identifying themselves as Olivia Ava ("Ava"), Emma Miller ("Miller"), and F.B. Lee ("Lee") as part of a common scheme to transfer funds to cryptocurrency wallets controlled by Defendants using the fake work platforms.

11. The scheme with Plaintiff began on or about March 20, 2024, when Defendants first contacted Plaintiff via WhatsApp. Defendants followed the standardized playbook set forth above, luring Plaintiff to transfer progressively greater amounts of money. Defendants represented that Plaintiff's funds were invested in cryptocurrency assets through the fake work platforms. Defendants subsequently blocked Plaintiff from accessing his accounts and transferring funds.

12. After Plaintiff could not recover his funds, he contacted Inca Digital ("Inca"), a cryptocurrency investigation firm, which traced his transactions and confirmed that Defendants were orchestrating a fake work platform scheme. As described below, Inca investigated other transactions involving the fake work platforms and found that these transactions were part of a common scheme to convert Class Member funds.

13. Based on Inca's investigation to date, Defendants' conversion scheme involved transactions during the period from March 20, 2024 through at least the date of the Complaint in case number 2024-900163, included more than 125 Class Member victims, and involved the conversion by Defendants of a minimum of $3.5 million of Class Member funds, with losses potentially higher.

DOCUMENT 2

14. To date, the investigation initiated by Plaintiff has identified the wallet addresses set forth in Appendix A, categorized by cryptocurrency exchange, as part of the common allegations centered around the fake work platforms. Plaintiff requests that this Court issue an Order freezing these wallet addresses.

JURISDICTION AND VENUE

15. Plaintiff lives at 2895 Hustleville Road, Albertville, AL 35951. He works as an independent contractor in digital marketing with a specialization in search engine optimization.

16. Defendants Olivia Ava, Emma Miller, and F.B. Lee contacted Mashkevich on the occasions alleged infra and, upon information and belief, contacted the class members or otherwise actively participated in the pig butchering scams at issue in this case and persuaded Mashkevich and the class members to transfer their cryptocurrency to scam wallets controlled by the Defendants.

DOCUMENT 2

17. Defendant Zheng Wenchao is the owner of OKX wallet TSLj5S3KAfvK8mDtDBisZvWDGUbKUDR16v. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. He uses the following email address: devin2020618@gmail.com. His home address is Banshan Street, Gongshu District, Hangzhou City, Zhejiang Province, China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Zheng Wenchao was nonetheless a

critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

18. Defendant 李 波 a/k/a Bo Li is the owner of Binance wallet TBJh9brKQp8ZvTq6vi5BvU9epdwEP63ysj. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. He uses the following email addresses: lsj2390657138@gmail.com and liboxxdd@gmail.com. He was born in No. 37, Wuli Village 4, Cuiping District, Xuanbin City, Sichuan Province, China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Bo Li was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

19. Defendant Sun Qi is the owner of Gate.io wallet TXV4pAhJSk9BxetRLh2BvTEnyC8xc7VZM8. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Sun Qi uses the following email address: 157797776@qq.com. Upon information and belief, this Defendant perpetrated the

DOCUMENT 2

wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Sun Qi was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

20. Defendant হাসান তারেক a/k/a Hasan Tareq is the owner of Binance wallet TLB95AHgDtns5cohFKicTsE2zpFqcbzMM7. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Hasan Tareq uses the following email address: hasantareq444@gmail.com. Hasan Tareq is a resident of Bangladesh. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Hasan Tareq was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as

DOCUMENT 2

either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

21. Defendant প্রেমনন্দ সরকার a/k/a Premananda Sardar is the owner of Binance wallet TTTkoMc9VuVKTGFQJPxF5pS2f1XV5u5QHJ. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Premananda Sardar uses the following email address: premananda0077@gmail.com. Premananda Sardar is a resident citizen of Bangladesh. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Premananda Sardar was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

22. Defendant 黄金明 a/k/a Jinming Huang is the owner of Binance wallet TNRzzzCZ5x1HPS6LSca2MCamDLoJNQLTdW. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Jinming Huang uses the following email address: kimmyming0000@gmail.com. Jinming Huang is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using

DOCUMENT 2

U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Jinming Huang was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

23. Defendant ဇေယျဝေဆးကြည် a/k/a Zeye Aye Kya is the owner of Binance wallet TBeUKtZxjcR6HmeVXV4TFeFWN3nvDDAqTw. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Zeye Aye Kya uses the following email address: xyeqchen@gmail.com. Zeye Aye Kya is a resident citizen of Myanmar. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding themselves out to be Ava, Miller, and/or Lee. Acting as "Miller," they contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," they contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding themselves out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Zeye Aye Kya was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as

DOCUMENT 2

either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

24. Defendant اسد علی a/k/a Asad Ali is the owner of Binance wallet TDuJLcreNwBzDp3RHrpsoTbhnw9s3QmPb9. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Asad Ali uses the following email address: asad.6064@gmail.com. Asad Ali is a resident citizen of Pakistan. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Asad Ali was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

25. Defendant 吴儒冬 a/k/a Rudong Wu is the owner of Binance wallet THm7R5wHvqx8gZkCX9KS9hjhvUv5TrXU4y. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Rudong Wu uses the following email address: chaoyuet5173@gmail.com. Rudong Wu is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706

DOCUMENT 2

295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Rudong Wu was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

26. Defendant 黎威标 a/k/a Weibiao Li is the owner of Binance wallet TPJV9ayW6YqPK9yddvaMzKwm424ySeJriK. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Weibiao Li uses the following email address: liweibiao@qijianlin.cn. Weibiao Li is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Weibiao Li was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

DOCUMENT 2

27. Defendant 王 龑 a/k/a Yan Wang is the owner of Binance wallet TCzHEWKCgo17CVwbkPFmZorDi9kWkpMbnd. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Yan Wang uses the following email address: 13509881023@139.com. Yan Wang is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Yan Wang was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

28. Defendant 郝 龙 飞 a/k/a Longfei Hao is the owner of Binance wallet TFsZ9UvNYS4tLPWLUzKsGviHsPsWFuKsH8. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Longfei Hao uses the following email address: 563311992@qq.com. Longfei Hao is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one

DOCUMENT 2

of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Longfei Hao was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

29. Defendant 李佳鹏 a/k/a Jiapeng Li is the owner of Binance wallet TGqjuFc8jxfjZBpUuFGnRLAXqzbHzYB4Wm. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Jiapeng Li uses the following email address: 2522830611@qq.com. Jiapeng Li is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Jiapeng Li was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

30. Defendant 刘乌烘 a/k/a Wuhong Liu is the owner of Binance wallet TUjGaqLmBnYythnN5hPNELyJPBBmEcjXdW. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Wuhong Liu uses the following

DOCUMENT 2

email address: 3529155507@qq.com. Wuhong Liu is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Wuhong Liu was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

DOCUMENT 2

31. Defendant Manh Cuong Nguyen is the owner of Binance wallet THEJ47jWuKmwssvvo7hrmw1wyjFbxDR54p. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Manh Cuong Nguyen uses the following email address: a.m.mounther5@gmail.com. Manh Cuong Nguyen is a resident citizen of Vietnam. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Manh Cuong Nguyen was nonetheless a critical and knowing part of the

laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

32. Defendant 王军龙 a/k/a Junlong Wang is the owner of Binance wallet TLN6ayhvQqzFK1KweyNDfMiqMfgrZ2rMg3. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Junlong Wang uses the following email address: 2725649463@qq.com. Junlong Wang is a resident citizen of China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Junlong Wang was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

33. Defendant 郭宗斌 a/k/a Guo Zongbin is the owner of OKX wallet TLXtzgg2Axd7ThhhZRq5LoBLgsUYnx8TpZ. This wallet contains cryptocurrency stolen from Plaintiff and other Class Members as part of Defendants' scheme. Guo Zongbin uses the following email address: g779906708@163.com. Guo Zongbin is a resident citizen of Henan Province China

DOCUMENT 2

with a residence address of No. 12, Guozhuang, Liupen Town, Runan County, Zhumadian City, Henan Province, China. Upon information and belief, this Defendant perpetrated the wrongdoing alleged herein, holding himself out to be Ava, Miller, and/or Lee. Acting as "Miller," he contacted Plaintiff using U.S. phone number (213) 568-8512. Acting as "Lee," he contacted Plaintiff using phone number +44 7706 295178. Lee referenced in his initial WhatsApp message to Plaintiff that "Ava" had suggested Plaintiff would be interested in online work. Alternatively, if this Defendant was not holding himself out as one of the three individuals who persuaded Mr. Mashkevich to transfer his cryptocurrency, Guo Zongbin was nonetheless a critical and knowing part of the laundering network, with ownership over a Destination Wallet that was utilized by the Defendants and Launderers to steal and launder Mr. Mashkevich's and class members' cryptocurrency, serving as either a crypto "mule" or active crypto launderer and covered within the category of Launderers as defined herein.

DOCUMENT 2

34. FICTITIOUS DEFENDANTS "A" – "F", being the true and correct identity of the individuals identified herein if Plaintiff has inadvertently misidentified any of the Defendants; FICTITIOUS DEFENDANTS "G" – "K", being the true and correct identity of the business entities, individuals, and employees, agents, or servants of the same who or that participated in the scam and laundering network at issue herein and whose identities are not currently known to the Plaintiff; FICTITIOUS DEFENDANTS "L" – "Z", being the true and correct identity of the business entities, individuals, and employees, agents, or servants of any of the named or fictitious defendants who participated in the conduct at issue in this case, including any defendants whose identities are currently unknown to Plaintiff who solicited Plaintiff using electronic means, who designed the fake work platforms Plaintiff utilized, who participated in receiving, forwarding, or otherwise disposing of Plaintiff's cryptocurrency, who initiated or opened any of the cyberwallets

into which Plaintiff's cryptocurrency was deposited, who had or exercised control over any of the cyberwallets into which Plaintiff's cryptocurrency was deposited, or who otherwise participated in any way in the "pig butchering" schemes of which Plaintiff was a victim. The identities of Defendants "A"- "Z" are currently unknown to Plaintiff but will be added when Plaintiff ascertains their true identities through discovery.

35. This Court has personal jurisdiction over the Defendants, including those fictitiously named, as the Defendants committed intentional torts directed at a resident citizen of Marshall County, Alabama, converted digital cryptocurrency belonging to a resident citizen of Marshall County, Alabama, solicited Plaintiff through electronic means, engaged in a civil conspiracy intended to steal crypto from an Alabama resident, and otherwise committed the tortious acts alleged herein.

DOCUMENT 2

36. Venue is proper in this Court because Defendants are neither citizens nor residents of Alabama and a substantial part of the events giving rise to the claims occurred in this county, where the Plaintiff resides and was primarily targeted by the Defendants' scheme.

37. The Plaintiff reserves the right to amend this Complaint to include additional parties as Defendants, upon further investigation and discovery of their identities, roles, and residences.

THE INTERNATIONAL PIG BUTCHERING CRISIS

38. Mr. Mashkevich and the putative class members had their cryptocurrency stolen as part of elaborate pig butchering scams, which are primarily perpetrated by Chinese and Taiwanese international crime syndicates operating out of Southeast Asia. According to the FBI, pig butchering scams cost Americans $5.3 billion in 2023 alone, with 40,000 U.S. victims reporting the scams to law enforcement. Various sources estimate that only 15% - 25% of U.S. pig butchering

victims report the crimes, meaning the U.S. likely had a minimum of 160,000 pig butchering victims in 2024.

How Pig Butchering Works

39. Pig butchering scammers conduct an elaborate, long-term psychological attack on their victims with the intent of stealing victims' cryptocurrency through deception. The scammers contact potential victims through social media, dating apps, direct messaging platforms, or text. As just one initial contact example, the potential victims may receive a text from an unknown number that simply says "hello." The scammers are seeking any response, such as the potential victims replying to ask who sent the text because their number is not saved in the target's contacts. From there, the scammers seek to build personal relationships with the targets, manipulating the targets into believing the scammers are potential romantic interests or trusted friends.

40. After the scammers establish trust, they introduce the victim to the idea of investing in or with cryptocurrency or, as in the present case, by earning cryptocurrency doing online work from home. The scammers guide the victims to a fake cryptocurrency trading platform. These websites look legitimate, with polished interfaces and simulated trading data. The scammers never ask the victims to send cryptocurrency to the scammers. Rather, the scammers convince the victims that the victims are controlling their own invested cryptocurrency. The scammers' goals are (a) convince the victims their work from home profits or investments are legitimate, and (b) foster in the victims a "fear of missing out" mindset so the victims continue participating in the scam.

41. After the victims have invested a large sum, the scammers make it impossible for the victims to withdraw their funds. If the scammers believe the victims can be tricked further, explanations may follow to convince the victims to invest even more crypto. For example, the scammers may tell the victims their accounts have been so profitable that the IRS requires the

DOCUMENT 2

victims to pay capital gains tax in advance. As was the case with Mr. Mashkevich, the scammers identify alleged technical issues or processing fees the victims need to pay before the victims' accounts will be unfrozen.

42. At some point, the platform itself will disappear, or the scammer will block the victim. The victims then realize they have been scammed, but their cryptocurrency is gone. The cryptocurrency can then only be retrieved with blockchain analysis and court-ordered wallet freezes to stop the process of cryptocurrency laundering before the cryptocurrency is taken off the blockchain and converted to fiat currency such as Chinese Yen, at which point it cannot be retrieved.

The Second Layer of Pig Butchering Victims

43. Pig butchering scams create financial tragedy for the scam victims, but the international criminal operation is fueled by a second layer of tragedy - the scammers are human trafficking victims. Trafficking victims are lured with promises of legitimate jobs, such as customer service or IT work, often in countries like Cambodia, Laos, or Myanmar. During their recruitment, the traffickers target vulnerable populations, particularly in Southeast Asia, China, and Africa. The victims do not realize they have been trafficked until they arrive at the scam compounds. Their passports and phones are confiscated, and they are forced to work in scam operations.

44. For example, a Vietnamese teenager named Nguyen Thien Kai moved to Cambodia after she was promised a high salary for teaching people how to play online games. But once she crossed the border, she was sent into a basement and instructed to scam people. The 19-year-old realized she had been tricked. "I had hidden my phone and managed to text my family to let them

DOCUMENT 2

know what happened. But then the boss saw my phone and took it," she said. "He read the texts to my family telling them to call the police, and he beat me and sold me to another organization."[1]

45. The trafficked workers must meet high financial quotas by deceiving victims online. If they fail, they face severe punishments, such as beatings or the risk of being sold to other, potentially more brutal, scam syndicates. Trafficked individuals are confined to compounds, often surrounded by armed guards.

46. Former prosecutor Erin West summarized the human trafficking tragedy fueling pig butchering scams during an interview with Ali Rogan of PBS News:

> We have literally never seen a world crisis like this. We've got Americans and people all over the world who've lost all their money. . . . [W]e have human trafficked victims that are forced to do this dirty work . . . . And when they get there, their passports are seized, they're put in buses and they are moved to these compounds where they are surrounded with men with AK47s . . . . The NGOs that I spoke with on the ground in Southeast Asia told me 7 out of 10 women are coming out of there saying that they were sexually assaulted . . . . 300,000 [people] estimated by the United States Institute of Peace are behind held against their will.[2]

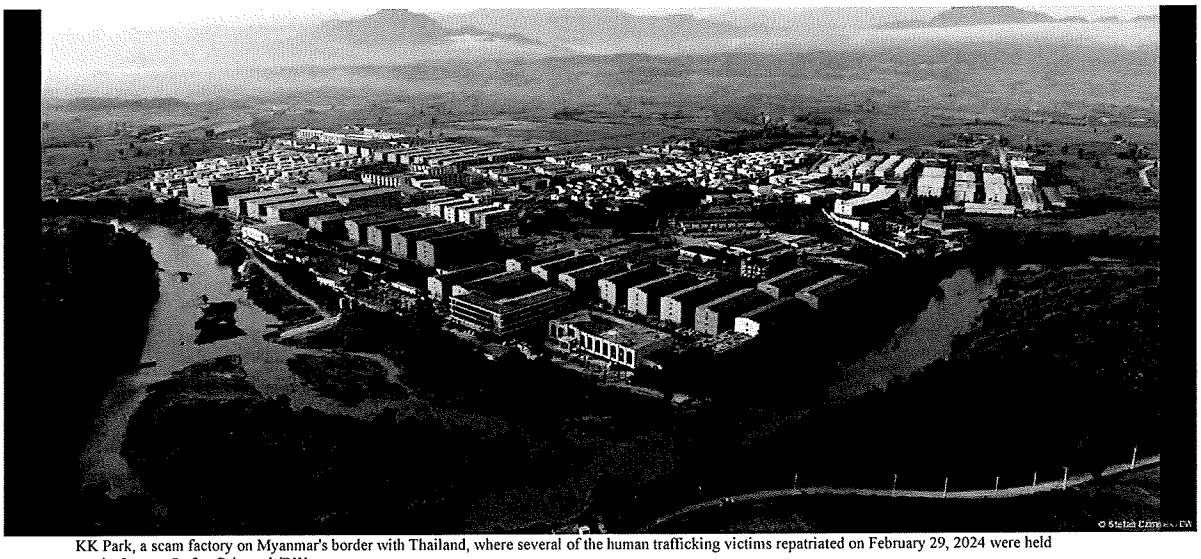
DOCUMENT 2

The Criminal Masterminds Behind Pig Butchering

47. The international crime syndicates operating these scams include but are not limited to the Chinese 14K Triad and the Karen Border Guard Force. Wan Kuok-Koi a/k/a "Broken Tooth" is a reputed Chinese mafia boss who has been sanctioned by the U.S. Government. He is the former head of the Chinese 14K Triad.[3] The 14K Triad is a criminal operation based in Hong Kong with ties to various scam compounds, such as KK Park, an online scam factory on Myanmar's border with Thailand.[4]

---

[1] https://www.abc.net.au/news/2022-09-16/cambodia-human-trafficking-online-scam-pig-butchering/101407862
[2] https://www.pbs.org/newshour/show/how-human-trafficking-victims-are-forced-to-run-pig-butchering-investment-scams
[3] https://www.wsj.com/world/china/china-mafia-broken-tooth-wan-kuok-koi-online-fraud-scam-70c09afb
[4] https://www.dw.com/en/china-repatriates-hundreds-of-scam-factory-survivors/a-68408165



KK Park, a scam factory on Myanmar's border with Thailand, where several of the human trafficking victims repatriated on February 29, 2024 were held captiveImage: Stefan Czimmek/DW

48. In 2018, "Broken Tooth" established the World Hongmen History and Culture Association in Cambodia, which reflects a criminal co-opting of the name of a centuries old Chinese fraternal organization first established in the mid-1600s. Broken Tooth also heads the Dongmei Group based in Hong Kong, which invests in the Saixigang Industrial Zone in Burma (Myanmar).[5] The Saixigang Zone, along with Myanmar's KK Park (pictured above) and other scam compounds, houses industrial-scale cyberfraud operations, engages in human trafficking, and has "clear links to organize crime figureheads Wan (Broken Tooth) Kuok Koi and She Zhijiang."[6] Notably, Myanmar is one of only three countries on the FATF money laundering and terrorist financing black list, along with North Korea and Iran.[7,8]

DOCUMENT 2

[5] https://kh.usembassy.gov/treasury-sanctions-corrupt-actors-in-africa-and-asia/

[6]https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

[7] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

[8] The FATF is the Financial Action Task Force, an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. The FATF black list identifies high-risk jurisdictions subject to a call for action because of their known close association with money laundering and terrorist financing. *See* FN7, *supra*

49. The Karen Border Guard Force (KBGF) is a violent militia that controls much of Myanmar's border areas with China, Laos, and Thailand. The KBGF operates in Myanmar's Karen State and is headed by Colonel San Myint a/k/a Saw Chit Thu. The KBGF has overseen the development of numerous illegal casino operations, which are used as pig butchering scam compounds. The KGBF changed its name in 2024 to the Karen National Army (KNA). The KBGF/KNA is considered a "major node in a network of cyber scam centers . . . in Southeast Asia in which criminal groups are earning billions of dollars."[9]

50. The KGBF/KNA partnered with the Hong-Kong registered Yatai International Holdings Group to generate revenue through companies forced to leave China because of that country's crackdown on illegal casino operations.[10] "Myanmar has become the prime destination for criminal groups", where money laundering and online scam operations relocated after several governments in southeast Asia cracked down on criminal gangs.[11] While an exhaustive discussion of the international criminal gangs perpetrating pig butchering scams is beyond the scope of this filing, the Court's awareness of the global criminal enterprises perpetrating the scam at issue in this case is important for the Court's determination as to appropriate next steps in this litigation.

DOCUMENT 2

Off-Ramping – From Stolen Cryptocurrency to Fiat Currency

51. The goal of the international crime syndicates perpetrating pig butchering cryptocurrency scams is to off-ramp the crypto by moving assets on a blockchain such as Tether or Tron and ultimately off chain to fiat currency such as US dollars or Chinese Yen. If the stolen crypto is anywhere on the blockchain, it can be tracked and frozen. Once the crypto is off-ramped, pig butchering victims have no realistic path to recovery. To accomplish the off-ramping, criminals

[9] https://www.justiceformyanmar.org/stories/the-karen-border-guard-force-karen-national-army-criminal-business-network-exposed
[10] https://www.usip.org/publications/2020/04/chinese-crime-networks-partner-myanmar-armed-groups
[11] https://www.usip.org/publications/2025/01/how-crime-southeast-asia-fits-chinas-global-security-initiative

will send crypto to a digital wallet and instruct the wallet owner to move the crypto to other wallets as part of the laundering process or ultimately to a spot-market trading account, where the crypto can be converted into fiat currency.

52. Laundering large amounts of cryptocurrency requires sophisticated techniques. Money laundering traditionally involves three stages – placement, layering, and integration. Placement is the process of moving the funds away from a direct association with the crime. With cryptocurrency, placement is the movement of crypto out of the "scam wallets" into which the victims unwittingly transferred their crypto. Layering seeks to move the funds in a complex pattern to disguise the trail of funds and frustrate attempts to track the stolen funds. With cryptocurrency, layering involves numerous transactions along the blockchain to disguise where the funds went. Integration is the process of making the stolen funds available to the criminals who stole the funds after the funds have been "washed".[12]

DOCUMENT 2

53. As part of the laundering process, cyber criminals deploy various techniques. such as:

- Smurfing - splitting large sums into smaller amounts that are transferred through multiple transactions
- Exchange hopping - using multiple crypto exchanges to transfer funds across different platforms
- Mixing - blending crypto from multiple sources to obscure the transaction history. Digital banks that offer banking-as-a-service (BaaS) in jurisdictions deficient in their anti-money laundering systems afford criminals the opportunity to "cloak" the stolen crypto by mixing it with legitimate funds

54. The financial technology (FinTech) and cryptocurrency industries pose a significant risk of criminal fraud as there is no comprehensive regulatory framework governing their banking

[12] https://www.unodc.org/unodc/en/money-laundering/overview.html

activities. FinTech and BaaS can offer legitimate business services, but only when they employ robust know your customer (KYC) and anti-money laundering (AML) compliance solutions. The goal of KYC and AML compliance is to identify suspicious behavior such as money laundering and financial terrorism before it occurs. When FinTech and BaaS companies operate without adequate KYC and AML compliance, they are knowingly making themselves available to launder stolen cryptocurrency by mixing and cloaking the stolen funds.

STATEMENT OF FACTS

55. As detailed below, Defendants, fictitious party Defendants, and their co-conspirators followed an especially pernicious version of the "pig butchering" roadmap for cryptocurrency theft. "Pig butchering" victims in the United States have lost billions of dollars and "pig butchering" schemes have been the subject of state and federal government investigation and prosecution.[13]

56. In a typical "pig butchering" scheme, scammers promise victims returns and then fabricate evidence of positive performance on fake websites made to look like functioning cryptocurrency trading venues or investment companies to entice victims to "invest" more money. When the victims have been sufficiently "fattened" with false profits, scammers steal the victims' cryptocurrency, and cover their tracks by moving the stolen property through a maze of subsequent transactions.

57. The Defendants' version of the "pig butchering" scheme involved promises of money in return for work by Class Members, who were enticed to spend time performing online

[13] *See* FinCEN Alert of Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering," U.S. Treasury Financial Crimes Enforcement Network Sep. 8, 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.

DOCUMENT 2

tasks with the expectation of payment. Defendants further promised the Class Members that they could withdraw the money they had earned, but only after making additional payments.

PLAINTIFF IS LURED TO DEPOSIT CRYPTOCURRENCY

58. Plaintiff was contacted by Defendants on or about March 20, 2024 regarding part-time online work. Defendants initially represented that the work involved a company called Grayphite, an international app marketing company where app developers publish their apps. Defendants represented that the work would be remote without any fixed time limits, and that all Plaintiff needed was a phone or computer to begin.

59. Defendants represented that Plaintiff would be compensated based on a standardized commission schedule. Defendants explained that Plaintiff could withdraw money earned, but would be required to replenish funds to "reset" any tasks to be performed in the future. On March 29, 2024, Plaintiff sent an initial deposit of $110 of USDC, a cryptocurrency, from his Coinbase account to an account that Defendants represented was part of the fake work platform.

60. Plaintiff subsequently performed tasks on the fake work platform and received "payments" for these tasks in the sense that his account on the platform showed modest gains. He was permitted to withdraw funds, but was required to replenish funds to receive payments from additional work on the platform. Defendants represented that Plaintiff could make increasing commissions if he deposited increasing amounts, which he did, including deposits of USDC, as well as Bitcoin and Ethereum, two other cryptocurrencies.

61. On April 6, 2024, one or more Defendants acting as "Miller" contacted Plaintiff about an additional related job opportunity that involved similar online work for a company called Resy. On April 7, 2024, Plaintiff began making additional deposits from his Kraken account related to this job opportunity, beginning with a $10 deposit and progressively increasing. Plaintiff made

DOCUMENT 2

deposits from his Kraken account in both Bitcoin and Ethereum. As with Plaintiff's Coinbase deposits, Defendants permitted Plaintiff to withdraw small amounts of money he had "earned" and deposit those funds to his Kraken account, but Plaintiff was required to replenish funds to earn additional amounts. For example, on April 8, Plaintiff made a deposit of $100 from his Kraken account and subsequently withdrew and redeposited $95.14.

62. During April 2024, Plaintiff made progressively increasing deposits and withdrawals. In aggregate, Plaintiff transferred approximately $90,000 to accounts controlled by Defendants.

63. The online scheme that targeted Plaintiff is consistent with other online crypto theft schemes and reflects a methodologically and psychologically sophisticated approach of manipulation and theft.

DOCUMENT 2

64. For example, Plaintiff was first solicited by one or more Defendants acting as "Lee" over the chat application WhatsApp. Defendant contacted Plaintiff to ask if Plaintiff was interested in a part time job. The following is taken from WhatsApp screenshots of the initial chat between Defendants (identified as "Lee FB") and Plaintiff (identified as "Misha"):

> 3/20/24, 10:34 AM - Lee FB Job Interest: Hi I'm Lee and I heard from Olivia Ava that you are interested in a part time job I do. Have you time to learn more?
>
> 3/20/24, 10:53 AM - Misha: Yes please tell me more
>
> 3/20/24, 10:56 AM - Lee FB Job Interest: I'm glad to hear your response! let me introduce the profile of the company to you
>
> 3/20/24, 10:56 AM - Lee FB Job Interest: The name of the company is *Grayphite* This is an international app marketing company where app developers publish their apps on *Grayphite*.
>
> 3/20/24, 10:57 AM - Lee FB Job Interest: This job provides the convenience of remote work without any fixed time limits. It

requires only 1-2 hours to complete and offers flexibility in choosing your preferred working hours.

3/20/24, 10:58 AM - Lee FB Job Interest: All you need is a phone or computer to begin. Workbench operates from 11:00 AM to 11:00 PM(EST Time)

3/20/24, 10:58 AM - Lee FB Job Interest: Is the requirement manageable for you?

3/20/24, 11:17 AM - Misha: Yes.

65. Plaintiff was later solicited by one or more Defendants acting as "Miller," and also to ask if Plaintiff was interested in a part time job. The following is taken from WhatsApp screenshots of the initial chat between Defendants (identified as "Emma") and Plaintiff (identified as "Misha"):

4/6/24, 2:53 PM - ~Emma FB Job: Hello, I'm Emma Miller

Thanks so much Erica for providing me with your contact information. I heard you were interested in a job opportunity I'm working on. <This message was edited>

4/6/24, 2:55 PM - Misha: Hi, yes

4/6/24, 2:55 PM - Misha: See you also have an LA number. Awesome

4/6/24, 3:02 PM - ~Emma FB Job: Haha, are you from Los Angeles?

4/6/24, 3:04 PM - Misha: Lived in west Hollywood for a few years and just kept my number. You still do?

4/6/24, 3:05 PM - ~Emma FB Job: Wow, this is a nice place, nice environment

4/6/24, 3:05 PM - ~Emma FB Job: Since you're interested, I'll walk you through every detail.

4/6/24, 3:07 PM - Misha: Great!

4/6/24, 3:07 PM - ~Emma FB Job: We provide back-end data optimization services for Resy. This position provides remote freelance/part-time/full-time work to complete data optimization work for Resy platform merchants. It only takes

DOCUMENT 2

about 60 minutes a day to complete them all. Have you ever done online part-time work before?

4/6/24, 3:10 PM - Misha: I know exactly what this is as I'm involved with something like that now. If my current system ends up working I'd like to start with you as well.

4/6/24, 3:11 PM - Misha: I know about the cryptocurrency, data optimization stuff and I'm guessing you have a similar pay structure where it's 800 after 5 days, then 1500 after 15, etc... Right?

4/6/24, 3:12 PM - ~Emma FB Job: No, we get paid $900 after completing five working days

4/6/24, 3:12 PM - ~Emma FB Job: Equivalent to our wages, the benefits will be much better

4/6/24, 3:13 PM - Misha: Awesome, but I can't commit to you until I see this one work.

4/6/24, 3:14 PM - Misha: If it does I'll be super excited as I understand the system pretty well now

4/6/24, 3:14 PM - Misha: So I'll get back to you in the next few days ok?

4/6/24, 3:15 PM - ~Emma FB Job: Okay, let me introduce what I do. Resy is an American online restaurant reservation service founded in 2014 by Gary Vaynerchuk, Ben Leventhal, and Michael Montero. As of 2024, 16,000 restaurants around the world can be booked through Resy. Resy was acquired by American Express in 2019. Our job is a workstation that provides comprehensive professional services such as restaurant evaluation, promotion, star rating, ranking, etc. The opening hours of the company's workstation are from 11Am to 11Pm every day. During this period, it can be completed in less than 1 hour. Finish your work for the day.

66. The company Grayphite referenced by one or more Defendants acting as "Lee" and the company Resy referenced by one or more Defendants acting as "Miller" are legitimate businesses, consistent with the typical pattern in online crypto theft schemes of the type perpetrated by the Defendants against the Class.

67. Defendants identify a legitimate business that the target can research and find online, but when the target is engaged and "working", Defendants direct the target to a fake web

DOCUMENT 2

site Defendants have created, which uses the name of the same legitimate business to deceive the target further.

68. Defendants bait the target by explaining the online "work" the target will be doing is legitimate. For example, Defendants explained to Plaintiff over WhatsApp that Plaintiff would be helping optimize apps for data providers. Once the "work" is explained in a way that convinces the target the tasks are legitimate, Defendants then further bait the target with promises of earning revenue for completing simple online tasks, including an explanation of how spending more time on the platform will generate more revenue. One or more Defendants acting as "Lee" and "Miller" both followed this pattern in their communications with Plaintiff.

69. From there, the Defendants "train" the target on how to use the online platform to complete the necessary tasks to earn revenue. One or more Defendants acting as "Lee" and "Miller" separately "trained" Plaintiff, who then began performing what Plaintiff thought were tasks associated with optimizing applications for Grayphite and Resy. In truth, Plaintiff was unknowingly interacting with sham websites designed by Defendants to further their crypto theft scheme. This is a technique consistent across several crypto theft schemes, whether they are couched as app optimization, investments, or otherwise.

70. As Plaintiff began interacting with the sham online platform, Defendants began the next phase of their crypto theft scheme, which involves separating a target from his or her cryptocurrency. In the present case, Plaintiff was being shown online cryptocurrency wallet balances that purportedly reflected Plaintiff's monetary balance in the system. At the beginning of this stage of the scheme, the Defendants allow targets such as Plaintiff to transfer nominal amounts of cryptocurrency into their personal cryptocurrency wallets to advance the illusion that the target is performing real work for real cryptocurrency.

DOCUMENT 2

71. After one or more Defendants acting as "Lee" and "Miller" separately persuaded Plaintiff that he could withdraw his cryptocurrency at any time, Plaintiff began encountering so-called "combination tasks" on the platforms. These new tasks were presented as legitimate app optimization work, but were nothing more than fake interactions designed to lure Plaintiff to deposit more cryptocurrency. These so-called combination tasks caused Plaintiff's "balance" to appear to be negative. One or more Defendants acting as "Lee" and "Miller" then convinced Plaintiff that he needed to transfer greater amounts of cryptocurrency into the system to "free up" his account and enable him to earn higher commissions from performing combination tasks.

72. Over time, Defendants increased the amount of cryptocurrency a target is required to transfer into the system to earn his "commissions". When a target expressed skepticism, as Plaintiff did, Defendants assured the target all was in order and they just needed to continue participating in a work platform. Plaintiff transferred funds from bank accounts and converted them to cryptocurrency, borrowing funds from friends, and extending his financial commitment to what he believed to be legitimate online enterprises. Plaintiff committed additional large amounts, in part because Defendants told Plaintiff that Defendants would help by lending him some of the cryptocurrency he was required to deposit. Defendants then displayed to Plaintiff a sham amount purportedly transferred into Plaintiff's accounts to convince Plaintiff that the individuals who were stealing from Plaintiff were trying to help.

73. Defendants also implemented a "credit score" scheme to persuade a target to deposit additional funds. For example, when Plaintiff tried to withdraw funds from the sham Grayphite platform, but was unable to do so, he reached out to one or more Defendants acting as "Lee" on WhatsApp. One or more Defendants acting as "Lee" told Plaintiff his "credit score" on the platform had dropped to 80%, and he needed to restore his score to access his cryptocurrency.

DOCUMENT 2

Defendants notified Plaintiff that he had two options to restore his credit score. Option 1 was to pay $20,000 ($1,000 per point to restore) and reset his credit score immediately. Option 2 was he could wait 10 months for his score to return to 100%. One or more Defendants acting as "Lee" offered to "help," as follows:

> 4/10/24, 10:20 AM - Lee FB Job Interest: If you choose 1 I will help you and I will go raise money for you. Because I understand now you don't need comfort, but funds
>
> 4/10/24, 10:21 AM - Lee FB Job Interest: If you choose 2, I will wait with you
>
> 4/10/24, 10:21 AM - Lee FB Job Interest: I respect your decision

74. Plaintiff added additional cryptocurrency to his account, purportedly to correct his credit score so he could withdraw the "commissions" he thought he had earned.

75. Another aspect of Defendants' crypto theft scheme involved purported "taxes." For example, Defendants told Plaintiff on April 17, 2024 that he could not withdraw his commissions because he owed "taxes" on them. One or more Defendants acting as "Lee" once again offered to assist Plaintiff, this time by supposedly transferring cryptocurrency into Plaintiff's account.

76. Finally, Defendants' crypto theft scheme involved threats related to alleged law enforcement involvement. For example, one or more Defendants acting as "Lee" communicated with Plaintiff via WhatsApp on April 19, 2024 to convince Plaintiff the FBI was involved because Lee had unwittingly "helped" Plaintiff with funds One or more Defendants acting as "Lee" had borrowed from a friend, only to find out one or more Defendants acting as "Lee" used stolen funds in Plaintiff's account.

77. Plaintiff asked one or more Defendants acting as "Lee" for a copy of the police report, which "Lee" failed to provide. WhatsApp conversations between Plaintiff and one or more Defendants acting as "Lee" continued until April 27, 2024, when Plaintiff concluded that there

DOCUMENT 2

were "[t]oo many bad people and liars stealing money that they don't deserve." Plaintiff also ceased interacting with one or more Defendants acting as "Miller," informing her, "I'm done with all the optimization programs. Lost too much money."

78. In sum, Defendants used a systematic multi-stage crypto theft scheme to target Class Members, including Plaintiff, and lured them to transfer increasing amounts of cryptocurrency as part of fake work platforms. The final step in this scheme, as described below, was identical for Class Members: Defendants stole the funds.

DEFENDANTS CONVERT CLASS MEMBERS' ASSETS

79. Inca's investigation revealed that Defendants used the fake work platforms to convert Class Members' assets, including Plaintiff's assets, and then sent those assets through a web of transactions designed to hide their trail. Inca traced and connected Defendants' transactions, found and followed a trail of transactions, and identified the cryptocurrency wallets that held Class Members' funds.

DOCUMENT 2

80. Inca's investigation involved two phases, each of which is precise, reliable, and replicable. In phase one, Inca "forward traced" the flow of funds from Plaintiff's investment to other cryptocurrency wallets. Inca traced Plaintiff's transactions forward to the wallets set forth in Appendix A, each of which were involved in transactions originating with Class Member wallets.

81. In phase two, Inca "reverse traced" the flow of funds to the above addresses and determined that additional addresses matched Plaintiff's flow of funds as part of a common scheme involving other Class Members. Through this tracing, Inca was able to confirm the identity of wallets involved in cryptocurrency transactions that were part of the common scheme, including the identity of Defendants' wallets that received Class Member funds and accordingly should remain frozen. Those wallets are set forth in Appendix A, categorized by exchange.

82. The bottom line of Inca's analysis is that Class Members' funds converted by Defendants were sent to the cryptocurrency wallets listed in Appendix A. It is these wallets that Plaintiff sought to – and which the Court did – freeze in its June 4, 2024 Order for Temporary Restraining Order and to Show Cause and its June 14, 2024 Preliminary Injunction Order.

CLASS ALLEGATIONS

83. This action may be properly maintained as a class action under state law.

84. The proposed Class is defined as follows: All persons and entities who, at the suggestion of the Defendants or individuals acting under the Defendants' instruction or control, transferred, through June 4, 2024, cryptocurrency into one or more of the cryptocurrency wallets identified in Appendix A and other scam wallet addresses controlled by the Defendants and/or Launderers as may be identified during discovery, or who had their cryptocurrency deposited into the same wallets by the Defendants or Launderers.

DOCUMENT 2

85. Excluded from the Class are individual Defendants and their families; corporate Defendants and their officers, directors and affiliates, if any, at all relevant times; Defendants' legal representatives, heirs, successors or assigns; and any entity in which Defendants have or had a controlling interest. Plaintiff reserves the right to amend or modify the Class in connection with a motion for class certification or as the result of discovery.

86. Based on Inca's investigation, the Class Members are so numerous, and are potentially scattered throughout the world, as to make joinder of all members impracticable, if not impossible. Plaintiff will attempt to ascertain Class Member identities through notice to the original owners of assets contained in the accounts listed in Appendix A to this Complaint, as well as through discovery, including into account records at relevant institutions.

87. The same "pig butchering" scheme, involving the same fake work platforms or fake investment portfolios, was used to victimize all Class Members, so that commonality of the claims predominates. Nearly all factual and legal issues raised in this Complaint are common to each Class Member and will apply uniformly to every Class Member.

88. Plaintiff's claims are typical of those of other Class Members, arise from the same practice or course of conduct as the claims of other Class Members, and are based on the same legal theory. Defendants used the same platforms to perpetrate their scheme and use the same ecosystem of cryptocurrency wallets to hide their tracks. By pursuing his own interests, Plaintiff will advance the interest of the absent class members. Plaintiff, like all other Class Members, sustained damages arising from Defendants' scheme and subsequent transactions to convert stolen property and hide the locations of victims' cryptocurrency assets. Plaintiff and Class Members were, and are, similarly or identically harmed by the same unlawful, deceptive, unfair, systematic, and pervasive pattern of misconduct. Plaintiff is entitled to the same declaratory, injunctive, and other relief as other Class Members.

89. Plaintiff will fairly and adequately represent the Class and protect the interests of the class. By proving his claim, Plaintiff will prove the Class's claims and Plaintiff's interests are thus fully aligned with those of Class Members. There are no material conflicts between Plaintiff's claims and those of other Class Members, including absent Class Members, that would make class certification inappropriate. Plaintiff has retained qualified counsel with relevant experience and will actively monitor this litigation. Counsel selected to represent the Class will fairly and adequately protect the interests of the Class, have relevant experience in complex and class litigation, and are competent counsel for class action litigation. Counsel for the Class will vigorously assert the claims of all Class Members.

DOCUMENT 2

90. Class certification is warranted because litigating these claims on a classwide basis is superior to other ways of adjudicating the claims at issue. For each Class Member to pursue their claim individually would require resource-intensive and time-consuming cryptocurrency tracing, analysis, and investigation through a maze of transactions. This action is properly maintained as a class action in that common questions of law and fact exist as to Class Members and predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy, including consideration of: the interests of Class Members in individually controlling the prosecution or defense of separate actions and/or proceedings; the impracticability or inefficiency of prosecuting or defending separate actions and/or proceedings; the extent and nature of any litigation concerning the controversy already commenced Class Members; the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and the difficulties likely to be encountered in the management of a class action.

DOCUMENT 2

91. Among the numerous questions of law and fact common to the Class are: whether Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and the Class; whether Defendants have a pattern, practice and scheme of "pig butchering" and subsequent digital transactions to convert stolen property and hide the locations of victims' cryptocurrency assets; to what extent Plaintiff and Class Members are entitled to damages; and to what extent Plaintiff and Class Members are entitled to declaratory and injunctive relief. Defendants have consistently acted and refused to act in ways generally applicable to the Class. Thus, final declaratory and injunctive relief with respect to the entire Class is appropriate.

92. Finally, Plaintiff and Class Members have suffered or are at imminent, severe, and unacceptably high risk of suffering, irreparable harm because of Defendants' ability to move funds

at any time, without notice. If Defendants withdraw funds from the wallets set forth in Appendix A, Plaintiff and Class Members will not be able to recover their funds, and will lose their property forever.

FIRST CAUSE OF ACTION
CONVERSION

93. Plaintiff realleges and incorporates by reference all preceding paragraphs.

94. Defendants intentionally and unlawfully took possession of the Plaintiff's and other Class Members' cryptocurrency funds, converting them for their own use.

95. The funds of Plaintiff and all Class Members are or will be specifically identifiable, in that Defendants' wrongful actions alleged herein involve cryptocurrency, which is traceable digital currency.

96. This act of conversion has caused significant financial harm to the Plaintiff and other Class Members.

DOCUMENT 2

SECOND CAUSE OF ACTION
REQUEST FOR INJUNCTIVE RELIEF

97. Plaintiff realleges and incorporates by reference all preceding paragraphs.

98. Plaintiff requests a freeze of all accounts that have transacted through the scam platforms regardless of the nature of the scam, including all cryptocurrency wallets set forth in Appendix A. Such a freeze is necessary to preserve the possibility of restitution for the Plaintiff and other victims.

THIRD CAUSE OF ACTION
CIVIL CONSPIRACY

99. Plaintiff realleges and incorporates by reference all preceding paragraphs.

100. Defendants committed the wrongs alleged herein.

101. In so doing, Defendants engaged in concerted action to accomplish, and combined to accomplish, an unlawful end. Alternatively, Defendants engaged in concerted action to accomplish, and combined to accomplish, a lawful end by unlawful means.

102. Defendants' conspiracy has caused significant financial harm to the Plaintiff and other Class Members.

Wherefore, Plaintiff respectfully requests that this Court continue the preliminary injunction freezing the cryptocurrency addresses set forth in Appendix A, and enter an order awarding: (1) damages in the amount of the value of Plaintiff's and other Class Members' stolen assets at the time of the theft; (2) pre-judgment interest; (3) an injunction ordering the return of any remaining stolen assets or the proceeds derived from the same; (4) attorneys' fees and costs incurred in prosecuting this action; and (5) any other relief that the Court finds just and proper.

DOCUMENT 2

Respectfully submitted,

/s/ Keith Jackson
Robert R. Riley, Jr. (ASB-8310-Y75R)
Keith Jackson (ASB-7519-J66B)
James E. Murrill (ASB-4329-A57M)
Attorneys for Plaintiff

OF COUNSEL:

RILEY & JACKSON, P.C.
3530 Independence Drive
Birmingham, AL 35209
Telephone: (205) 879-5000
rob@rileyjacksonlaw.com
kj@rileyjacksonlaw.com
jay@rileyjacksonlaw.com

Appendix A

Binance

THm7R5wHvqx8gZkCX9KS9hjhvUv5TrXU4y
TTTkoMc9VuVKTGFQJPxF5pS2f1XV5u5QHJ
TLB95AHgDtns5cohFKicTsE2zpFqcbzMM7
TBeUKtZxjcR6HmeVXV4TFeFWN3nvDDAqTw
TCzHEWKCgo17CVwbkPFmZorDi9kWkpMbnd
TFsZ9UvNYS4tLPWLUzKsGviHsPsWFuKsH8
TPJV9ayW6YqPK9yddvaMzKwm424ySeJriK
TNRzzzCZ5x1HPS6LSca2MCamDLoJNQLTdW
TDuJLcreNwBzDp3RHrpsoTbhnw9s3QmPb9
TBJh9brKQp8ZvTq6vi5BvU9epdwEP63ysj
TGqjuFc8jxfjZBpUuFGnRLAXqzbHzYB4Wm
TLN6ayhvQqzFK1KweyNDfMiqMfgrZ2rMg3
TUjGaqLmBnYythnN5hPNELyJPBBmEcjXdW
TTv4AqmaKwMt2SagrSyRyqE7XB6dpLUHyd
THEJ47jWuKmwssvvo7hrmw1wyjFbxDR54p

OKX

TSLj5S3KAfvK8mDtDBisZvWDGUbKUDR16v
TCeLkTvsCb6Tz2ik7xng1YoT9BYdcVxHnr
TJGebBJfUAgs4NUManaRFGQRpoLEwYPj2o
TLXtzgg2Axd7ThhhZRq5LoBLgsUYnx8TpZ
TFwi8cW7CUZ3mVY92hYaQiEoAYr5z1E2Kh
TUxrJsf1ZcRgXpfX9L2VLUCEJ5DUs2mWC7
TKuKfiyMCV65AK4A5YGLP3sgDnzkMc6fdp
TA8C3BnEyVvyPGTTEhcsNZz9jNNm6j8tbi

Gate.io

TXV4pAhJSk9BxetRLh2BvTEnyC8xc7VZM8

KuCoin

TDGGk3yNwo9uEmL69zmdwJwUYaCozZMQuD
TUijurbvTKwCpYzEi3TnC62gRLGCxn7q6T

DOCUMENT 2