AlaFile E-Notice

50-CV-2024-900163.00

To: ROBERT R. RILEY JR.
rob@rileyjacksonlaw.com

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF MARSHALL COUNTY, ALABAMA

MICHAEL MASHKEVICH V. OLIVIA AVA ET AL
50-CV-2024-900163.00

The following complaint was FILED on 6/4/2024 9:34:31 AM

Notice Date: 6/4/2024 9:34:31 AM

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

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

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: 06/04/2024
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:
RIL012

6/4/2024 9:34:29 AM
Date

/s/ ROBERT R. RILEY JR.
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
6/4/2024 9:34 AM
50-CV-2024-900163.00
CIRCUIT COURT OF
MARSHALL COUNTY, ALABAMA
ANGIE JOHNSON, CLERK

IN THE CIRCUIT COURT
OF MARSHALL COUNTY, ALABAMA

MICHAEL MASHKEVICH, on behalf of himself and all others similarly situated,	)	
	)	Civil Action No. _____
Plaintiff,	)	
	)	CLASS ACTION
V.	)	
	)	
OLIVIA AVA, EMMA MILLER, and F.B. LEE,	)	

FICTITIOUS DEFENDANT "A", being the true and correct identity of the individual identified herein as Defendant Olivia Ava; FICTITIOUS DEFENDANT "B", being the true and correct identity of the individual identified herein as Defendant Emma Miller; FICTITIOUS DEFENDANT "C", being the true and correct identity of the individual identified herein as Defendant F.B. Lee; FICTITIOUS DEFENDANTS "D" – "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.

	)
Defendants.	)
	)

COMPLAINT

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

INTRODUCTION

1. This case involves a cryptocurrency scam in which Defendants promise their victims they will be paid for performing standardized online work, and then steal their money.

2. The cryptocurrency scam is centered around fake work platforms. Defendants solicit victims by sending boilerplate inquiries about part-time work. After a person responds to a message, one or more Defendants contact that person about a fake work platform and describe the purported work as involving activities such as clicking buttons, online data optimization, and performing tasks involving the use of various software applications.

3. Defendants represent that the work involves 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 represent 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 represent 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 emphasize in standardized language the convenience of the remote work online, the absence of fixed time limits, the flexibility, and the preferred working hours.

4. Defendants used these fake work platforms to lure a common class of victims ("Class Members," or the "Class") to transfer funds to cryptocurrency wallets controlled by Defendants. The Class in this matter is defined as all persons and entities whose funds were unlawfully taken by Defendants through the date of this Complaint, and whose stolen cryptocurrency is contained in the wallets set forth in Appendix A, or in other cryptocurrency accounts controlled by Defendants as set forth in Appendix A.

5. Defendants followed a standardized roadmap to persuade Class Members to transfer cryptocurrency to wallets controlled by Defendants. First, Defendants requested that Class Members contribute a small amount of funds to set up their respective accounts. Then Defendants represented that Class Members had earned money for work performed and permitted Class Members to withdraw that money. Defendants then represented that Class Members were required to transfer additional funds to their accounts for standardized, boilerplate reasons, including when their credit score had dropped, their account balance had gone negative, they owed taxes, or due to a problem with loans from other work platform members. After Defendants persuaded Class Members to deposit additional funds, they stole the money and transferred it to wallets they control.

6. Plaintiff is a resident of Albertville, Alabama. Like other similarly situated Class Members, Plaintiff was tricked by one or more individuals, 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.

7. 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.

8. 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.

9. 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 this Complaint, 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.

10. 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

11. 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.

12. Defendants are persons who perpetrated the wrongdoing alleged herein. The true identities of Ava, Miller, and Lee are currently unknown and are subject to ongoing investigation. Miller contacted Plaintiff using U.S. phone number (213) 568-8512. Lee 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.

13. FICTITIOUS DEFENDANT "A", being the true and correct identity of the individual identified herein as Defendant Olivia Ava; FICTITIOUS DEFENDANT "B", being the true and correct identity of the individual identified herein as Defendant Emma Miller; FICTITIOUS DEFENDANT "C", being the true and correct identity of the individual identified

herein as Defendant F.B. Lee; FICTITIOUS DEFENDANTS "D" – "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. Plaintiff avers that the identities of Defendants "A"- "Z" are currently unknown to Plaintiff but will be added when Plaintiff ascertains their true identities through discovery.

14. 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, and otherwise committed tortious acts herein.

15. 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.

16. 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.

STATEMENT OF FACTS

17. As detailed below, Defendants 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.[1]

18. 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.

19. 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 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

20. 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.

[1] 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.

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.

21. 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.

22. 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.

23. On April 6, 2024, Defendant 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 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.

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

25. 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.

26. For example, Plaintiff was first solicited by Defendant 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 Defendant Lee (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.

27. Plaintiff was later solicited by Defendant Miller, also over WhatsApp, 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 Defendant Miller (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 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.

28. The company Grayphite referenced by Defendant Lee and the company Resy referenced by Defendant Miller are legitimate businesses, consistent with the typical pattern in online crypto theft schemes of the type perpetrated by the Defendants against the Class. 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 site Defendants have created, which uses the name of the same legitimate business to deceive the target further.

29. 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. Defendants Lee and Miller both followed this pattern in their communications with Plaintiff.

30. From there, the Defendants "train" the target on how to use the online platform to complete the necessary tasks to earn revenue. Defendants 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.

31. 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.

32. After Defendants 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. Defendants 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.

33. 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 Lee and Miller 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.

34. 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 Defendant Lee on WhatsApp. Defendant Lee told Plaintiff his "credit score" on the platform had dropped to 80%, and he needed to restore his score to access his cryptocurrency. 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%. Defendant 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

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

36. 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. Defendant Lee once again offered to assist Plaintiff, this time by supposedly transferring cryptocurrency into Plaintiff's account.

37. Finally, Defendants' crypto theft scheme involved threats related to alleged law enforcement involvement. For example, Defendant 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 Defendant Lee had borrowed from a friend, only to find out Defendant Lee used stolen funds in Plaintiff's account.

38. Plaintiff asked Defendant Lee for a copy of the police report, which Lee failed to provide. WhatsApp conversations between Plaintiff and Defendant Lee continued until April 27, 2024, when Plaintiff concluded that there were "[t]oo many bad people and liars stealing money that they don't deserve." Plaintiff also ceased interacting with Defendant Miller, informing her, "I'm done with all the optimization programs. Lost too much money."

39. 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

40. 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.

41. 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 Exhibit A, each of which were involved in transactions originating with Class Member wallets.

42. 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 be frozen. Those wallets are set forth in Appendix A, categorized by exchange.

43. 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 seeks to freeze.

CLASS ALLEGATIONS

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

45. The proposed Class is defined as follows: all persons and entities whose funds were unlawfully taken by Defendants through the date of this Complaint, and whose stolen cryptocurrency is contained in the wallets set forth in Appendix A, or in other cryptocurrency accounts controlled by Defendants at the exchanges set forth in Appendix A.

46. 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.

47. 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.

48. The same "pig butchering" scheme, involving the same fake work platforms, 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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

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

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

56. 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.

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

SECOND CAUSE OF ACTION
REQUEST FOR INJUNCTIVE RELIEF

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

59. Plaintiff requests a freeze of all accounts that have transacted through the fake work platforms, 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.

Wherefore, Plaintiff respectfully requests that this Court enter a temporary restraining order and freeze the cryptocurrency addresses set forth in Appendix A, and 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.

Dated: June 3, 2024

Respectfully submitted,

/s/ Robert R. Riley, Jr.
Robert R. Riley, Jr. (ASB-8310-Y75R)

/s/ Keith Jackson
Keith Jackson (ASB-7519-J66B)

/s/ James E. Murrill
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
TXMA8WaXdWa5EYkBhAMuCwjHjSdHGvyV2y
TCzHEWKCgo17CVwbkPFmZorDi9kWkpMbnd
TKJ77SjyQGAX4u711tneGXpgZLTVwRZ8Uk
TFsZ9UvNYS4tLPWLUzKsGviHsPsWFuKsH8
TPJV9ayW6YqPK9yddvaMzKwm424ySeJriK
TNRzzzCZ5x1HPS6LSca2MCamDLoJNQLTdW
TDuJLcreNwBzDp3RHrpsoTbhnw9s3QmPb9
TBJh9brKQp8ZvTq6vi5BvU9epdwEP63ysj
TWUeDMvPrY88cpX2EmFxHdd2xtWfm9cPDK
TLvFAMp7qZ7iF8fqqewM7AMjJtzZwjSWve
TGqjuFc8jxfjZBpUuFGnRLAXqzbHzYB4Wm
TLN6ayhvQqzFK1KweyNDfMiqMfgrZ2rMg3
TUjGaqLmBnYythnN5hPNELyJPBBmEcjXdW
TTv4AqmaKwMt2SagrSyRyqE7XB6dpLUHyd
THEJ47jWuKmwssvvo7hrmw1wyjFbxDR54p
TP9uatVfbAcZe4qAqANZ6Hjc7JrzGGYhro
TJphKU7t3aW1WoJ3ur9YW4zxNwE9cc6e2H

OKX
TSLj5S3KAfvK8mDtDBisZvWDGUbKUDR16v
TCeLkTvsCb6Tz2ik7xng1YoT9BYdcVxHnr
TJGebBJfUAgs4NUManaRFGQRpoLEwYPj2o
TLXtzgg2Axd7ThhhZRq5LoBLgsUYnx8TpZ
THGTenLmvqWycGLGtgRvX4wURiHQeDvNps
TFwi8cW7CUZ3mVY92hYaQiEoAYr5z1E2Kh
TUxrJsf1ZcRgXpfX9L2VLUCEJ5DUs2mWC7
TKuKfiyMCV65AK4A5YGLP3sgDnzkMc6fdp
TA8C3BnEyVvyPGTTEhcsNZz9jNNm6j8tbi

Gate.io
TXV4pAhJSk9BxetRLh2BvTEnyC8xc7VZM8

KuCoin
TDGGk3yNwo9uEmL69zmdwJwUYaCozZMQuD
TUijurbvTKwCpYzEi3TnC62gRLGCxn7q6T

LBank
TUNN5XDrQg6fkfUEdWcYDHgvPwXyxS1k2C
TGUSM4zJ6XrJ5xaD9pnB5eLrKy2GqjG3pC
TVXe59tPrQmFVrP4no59t1Vp3aDSfs8m2t