

CAUSE NO. _____

NATALIA ELMOWAFI, on behalf of	§	IN THE DISTRICT COURT OF
Herself and all others similarly situated,	§	
	§	
Plaintiff,	§	
	§	
V.	§	HARRIS COUNTY, TEXAS
	§	
CHRIS YANG and JOHN DOES 1-25,	§	
	§	
Defendants.	§	___ JUDICIAL DISTRICT

**PLAINTIFF’S ORIGINAL VERIFIED CLASS ACTION PETITION,
APPLICATION FOR TEMPORARY RESTRAINING ORDER,
TEMPORARY, AND PERMANENT INJUNCTIONS**

Class Plaintiff Natalia Elmowafi (“Plaintiff”) files this, her Original Class Action Petition, Application for Temporary Restraining Order, Temporary, and Permanent Injunctions and requesting class certification as follows:

I. DISCOVERY CONTROL PLAN

1. Plaintiff intends to conduct discovery under Level 2 pursuant to Texas Rule of Civil Procedure 190.3.

II. INTRODUCTION

2. This case involves a cryptocurrency scam in which Defendants solicit investors to transfer cryptocurrency assets to a fake cryptocurrency trading platform, falsely represent that the investors have earned positive returns, and then steal their money.

3. Defendants contact potential victims using generic inquiries about cryptocurrency investments. When a person responds, Defendants engage in further correspondence, sending standardized messages about investment strategies to entice them into investing. They then provide

cryptocurrency wallet addresses and instructions for transferring funds, giving victims access to a fake cryptocurrency trading website purportedly linked to a legitimate trading platform.

4. Defendants falsely represent that the trades on the fake platform are real. Victims receive real-time reports of gains and current position valuations, leading them to believe they are trading actual cryptocurrencies on a legitimate exchange. These representations are entirely false.

5. In this case, Defendants utilized a fraudulent trading platform to lure a common class of victims (“Class Members,” or the “Class”) to transfer funds to cryptocurrency wallets under Defendants’ control. The Class is defined as all persons and entities whose funds were unlawfully taken by Defendants up to the date of this Petition, whose stolen cryptocurrency is contained in the wallets set forth in Exhibit A, or in other cryptocurrency accounts controlled by Defendants as set forth in Exhibit A.

6. Defendants followed a consistent scheme to persuade Class Members to transfer cryptocurrency to wallets controlled by Defendants. Initially, they requested small contributions to set up accounts. Defendants then claimed that Class Members had earned returns from their trading activities. When Class Members attempted to withdraw funds, Defendants persuaded them to deposit additional funds under the pretext of standard requirements such as trading fees, taxes, or "gas" fees. After securing these additional deposits, Defendants stole all the contributed money and transferred it to wallets under their control.

7. Defendants attempted to conceal their actions by transferring stolen assets through a series of online transactions designed to hide their trail. Through the substantial effort of her counsel and investigative experts, Plaintiff has identified specific cryptocurrency wallets in which the ill-gotten gains of Defendants’ scheme are *presently* held. These are set forth in Exhibit A.

8. Time is of the essence, as Defendants can transfer these cryptocurrency proceeds beyond the Class Members' knowledge and reach at any moment. Plaintiff therefore seeks immediate *ex parte* injunctive relief to freeze the identified cryptocurrency wallets identified in Exhibit A. Without such emergency relief, Plaintiff and similarly situated class members will be left without an adequate remedy at law. If the criminal enterprise of which the Defendants are a part is provided notice of hearing, they will simply transfer the Class Members' stolen assets out of the wallets identified in Exhibit A.

9. Plaintiff resides in Houston, Harris County, Texas. Like other similarly situated Class Members, Plaintiff was deceived by one or more individuals, including a person identifying himself as Chris Yang ("Yang"), as part of a common scheme to transfer funds to cryptocurrency wallets controlled by Defendants via the fraudulent trading platforms.

III. PARTIES

10. Plaintiff is a resident of Harris County, Texas. The last four digits of her Texas Drivers' License are 0991.

11. Defendants have gone to great lengths to conceal their true identities, including anonymously registering their fake website. The true identities and residences of the Defendants are currently unknown and are subject to ongoing investigation. Defendant "Yang" contacted Plaintiff using three U.S. phone numbers: 424-335-4392 and 213-569-3590, which he claimed were his personal numbers, and 917-470-7696, which he stated was his work number. Yang also represented himself as an officer of a company called Row.

12. Due to the defendants' use of fictitious identities and unknown locations, traditional service methods are unavailable. Pursuant to Rule 106, Plaintiff seeks judicial approval for alternative service methods, reasonably calculated to provide to provide actual notice, including

service via airdropping a special purpose token to the defendants' cryptocurrency wallet, as further described herein.

13. The amounts sought by Plaintiff exceed the minimum jurisdictional limits of this Court.

14. This action accrued in Harris County, Texas, Defendant is domiciled in Harris County, Texas, and the property underlying the claims brought herein is located in Harris County, Texas.

15. Jurisdiction and venue are proper in this Court.

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

IV. STATEMENT OF FACTS

A. PIG BUTCHERING BRIEFLY EXPLAINED

17. Defendants' scheme is called a "pig butchering" scam. Defendants first reach out to or otherwise make contact with victims by sending fake "wrong number" texts, sometimes including pictures, meet victims on dating apps using fake profiles, or send messages through social media. When victims respond, even to say the scammer has the wrong number, the con begins. The scammer will attempt to strike up a conversation, attempting to gain the victim's confidence or establish a personal connection. Eventually, the scammer moves the conversation to an encrypted method of communication, like WhatsApp or Telegram, and turns the conversation toward cryptocurrency investing.

18. These scams typically involve the promise of returns after perpetrators fabricate evidence of positive performance on fake websites made to look like functioning cryptocurrency trading venues, job sites, or investment companies. Victims are enticed to "invest" or send money

based on misrepresentations. After victims have transferred substantial sums, typically in cryptocurrency, the scammers disappear and cover their tracks by moving the stolen funds through a maze of subsequent transactions, causing victims severe financial loss. This scheme involves sophisticated psychological manipulation and exploits the anonymity and irreversibility of cryptocurrency transactions. Victims in the United States have collectively lost billions of dollars, and these “pig butchering” schemes have been the subject of state and federal government investigation and prosecution, including recently in Texas.¹

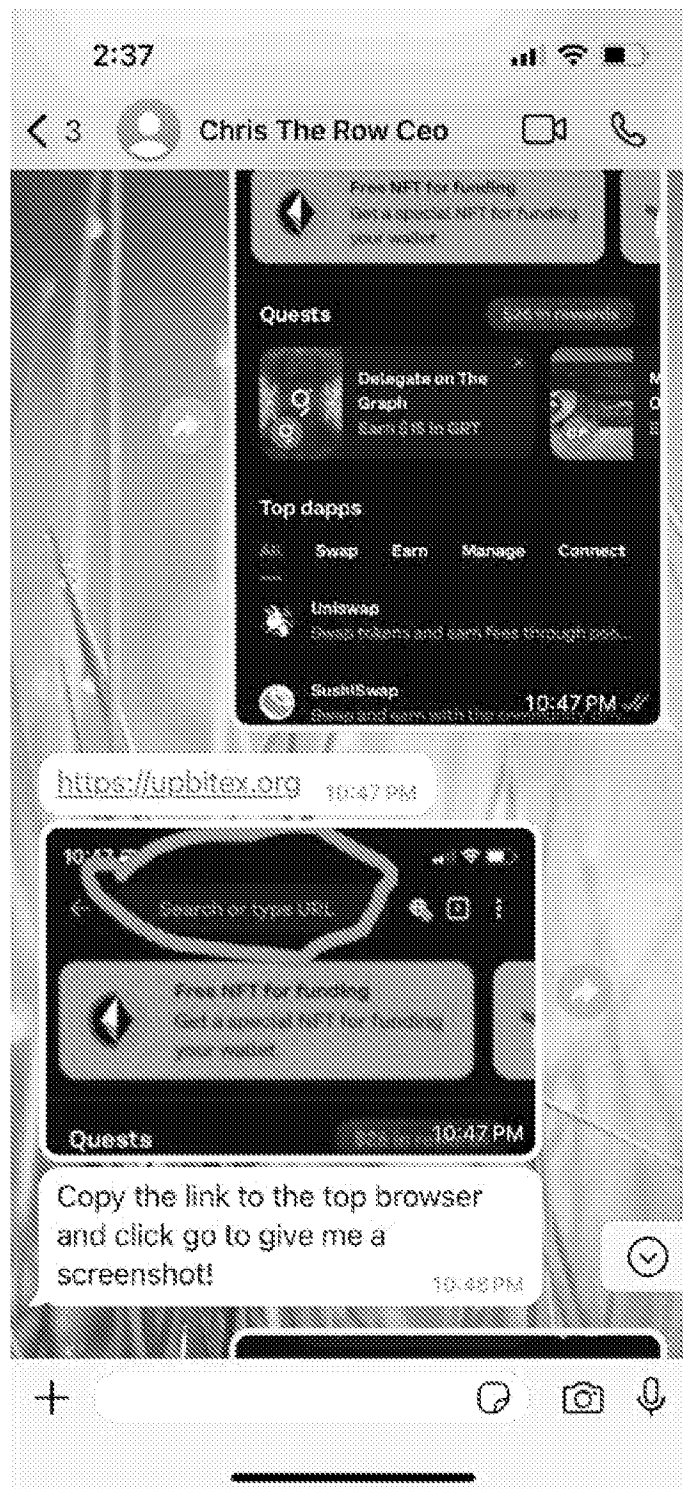
19. Defendants in this case made false promises about the legitimacy of a cryptocurrency trading platform. Class Members were enticed to invest through this platform with the expectation of such legitimacy. Defendants further promised the Class Members that they could withdraw the money they had earned, but only after making additional payments. Class Members were never able to withdraw anything.

B. PLAINTIFF IS “PIG BUTCHERED” BY DEFENDANTS

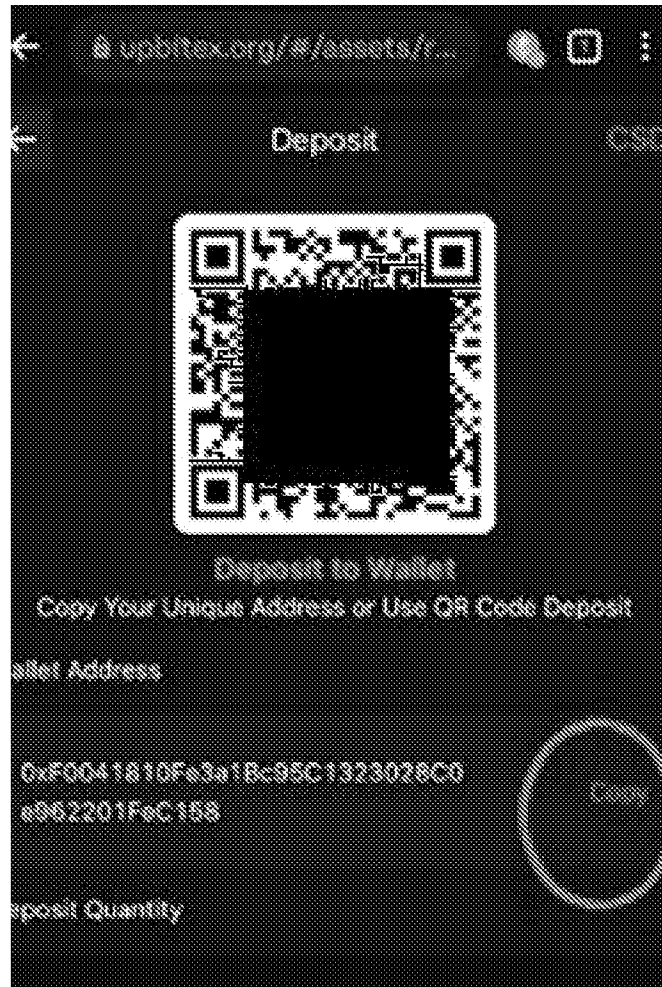
20. The scheme involving Plaintiff began on or about November 18, 2023, when Defendant Yang contacted her via text message from phone number 1-917-470-7696. Defendant Yang represented that he was a 45-year-old male with a daughter, originally from Hong Kong. He described a cryptocurrency platform called “upbitex” as legitimate and informed Plaintiff that transactions could be conducted on this platform after registering with Coinbase and transferring

¹ See U.S. Attorney’s Office, Eastern District of Texas Press Release: Chinese National Charged in “Pig Butchering” Scheme, May 21, 2024, <https://www.justice.gov/usao-edtx/pr/chinese-national-charged-pig-butchering-scheme>; 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; Teele Rebane & Ivan Watson, Killed by a Scam: A Father Took His Life after Losing His Savings to International Criminal Gangs; He’s Not the Only One, Jun. 19, 2024, Cable News Network, <https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html>.

funds from a Coinbase wallet. Below is a screenshot from Defendant Yang, who identified himself as “Chris The Row Ceo,” providing Plaintiff with instructions to access the “upbitex” platform:

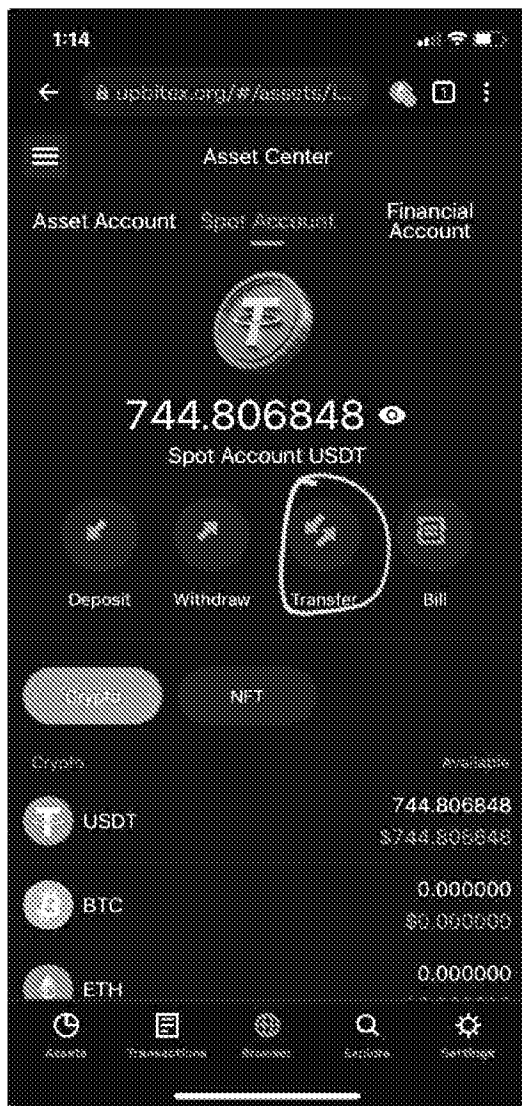


21. Defendant Yang gained Plaintiff's confidence during the following days and proposed an investment opportunity involving cryptocurrency. Plaintiff followed Defendant Yang's instructions to register her Coinbase wallet on November 23, 2024, and made an initial deposit by withdrawing cryptocurrency from her Coinbase account and using the "upbitex" platform, as indicated in the screenshot below:²



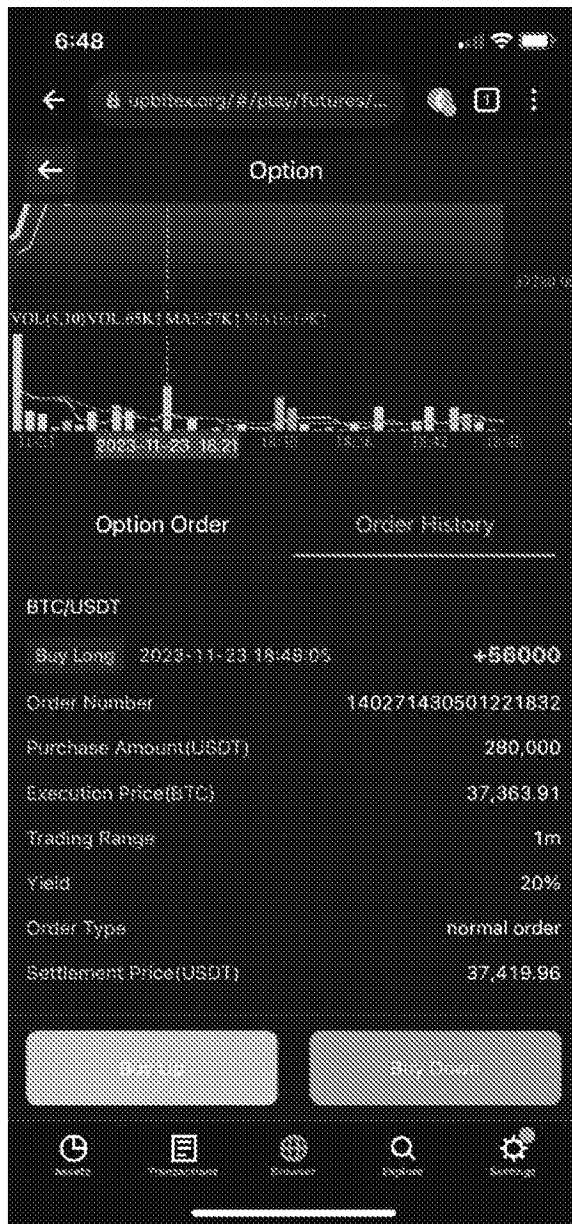
² The QR code has been obstructed.

22. On or about November 24, 2023, Plaintiff transferred funds in a series of small transactions from her account at Coinbase to a wallet address that purported to be on the “upbitex” platform. The platform showed that the funds were in her account, as indicated in the screenshot below, which shows approximately \$745 of value:

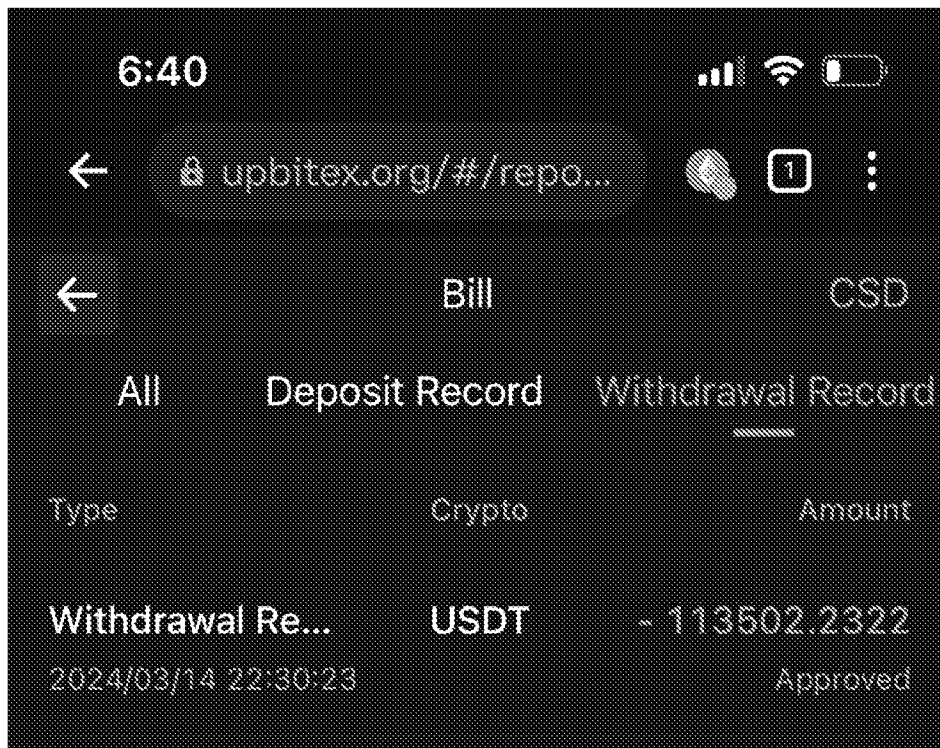


23. Defendant Yang represented that Plaintiff could use her funds on the platform to invest various Bitcoin trading strategies. According to reports from the platform, these trading strategies were profitable, and Plaintiff was able to withdraw \$756.

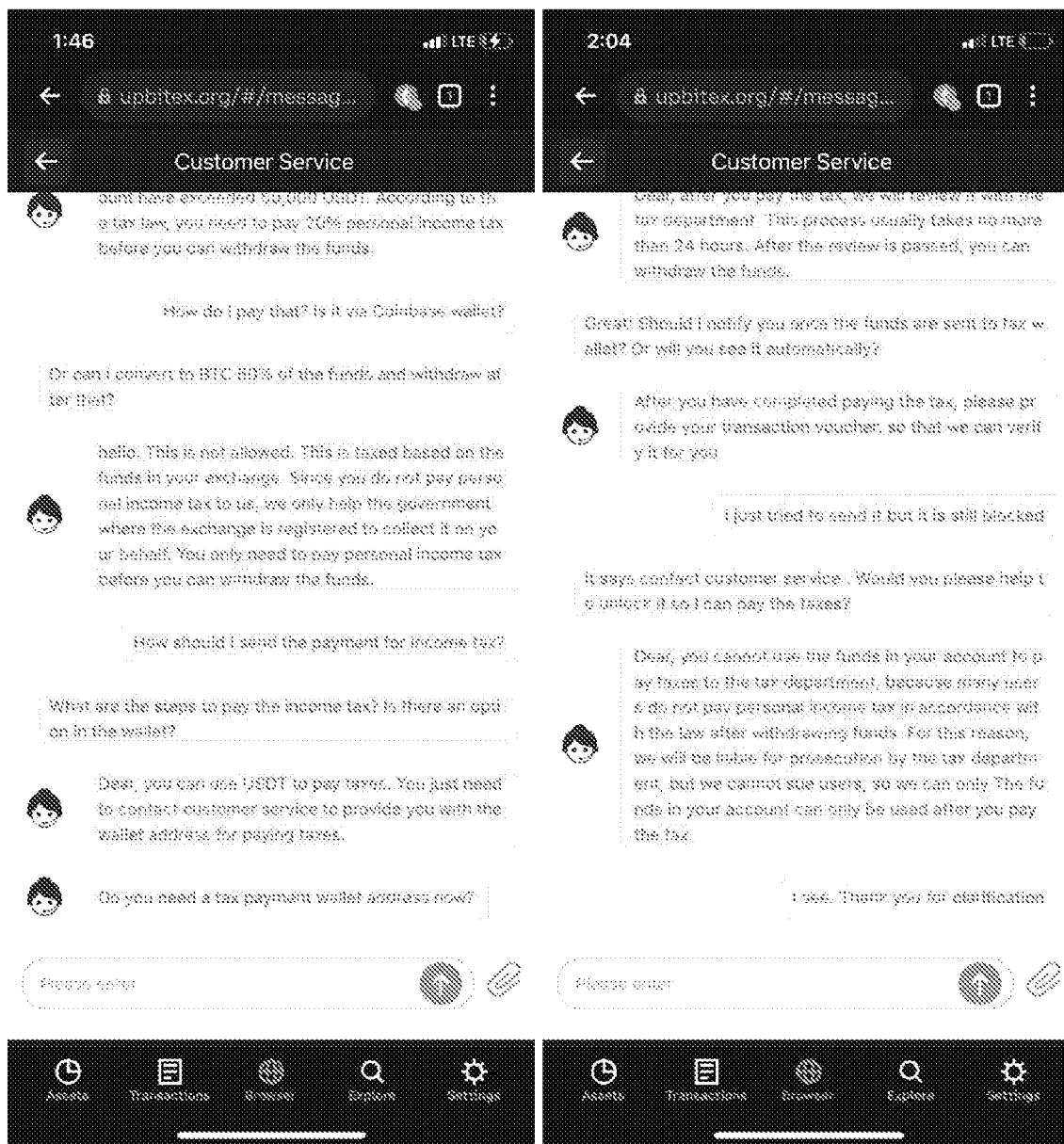
24. Based on the purported early success of these strategies, and the apparent legitimacy of the platform, Plaintiff made additional deposits on or about November 30, 2024, totaling \$30,000, and continued to invest in various trading strategies, as advised by Defendant Yang. These strategies also appeared to be profitable, as indicated by the screenshot below, showing a profit of \$56,000:



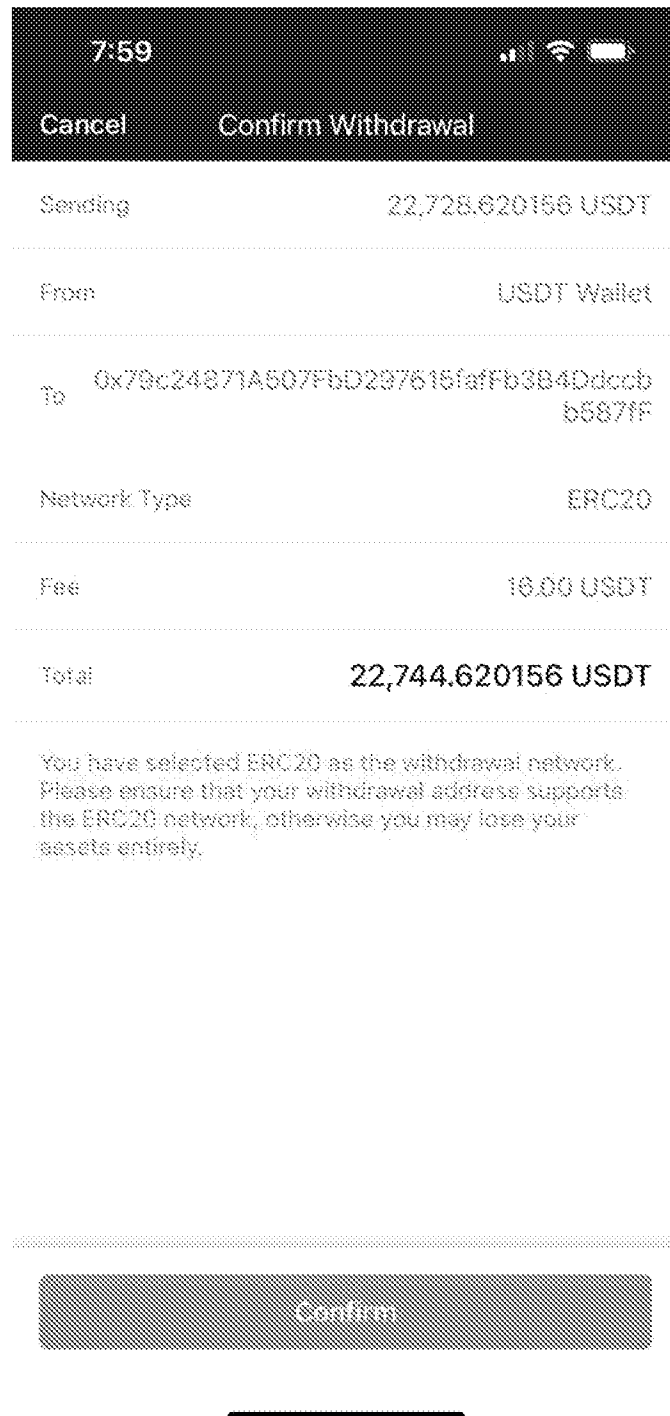
25. Plaintiff continued to use the “upbitex” platform during 2023 and early 2024, and her account appeared to reflect significant profits. On March 14, 2024, Plaintiff attempted to withdraw funds, as indicated by the screenshot below:



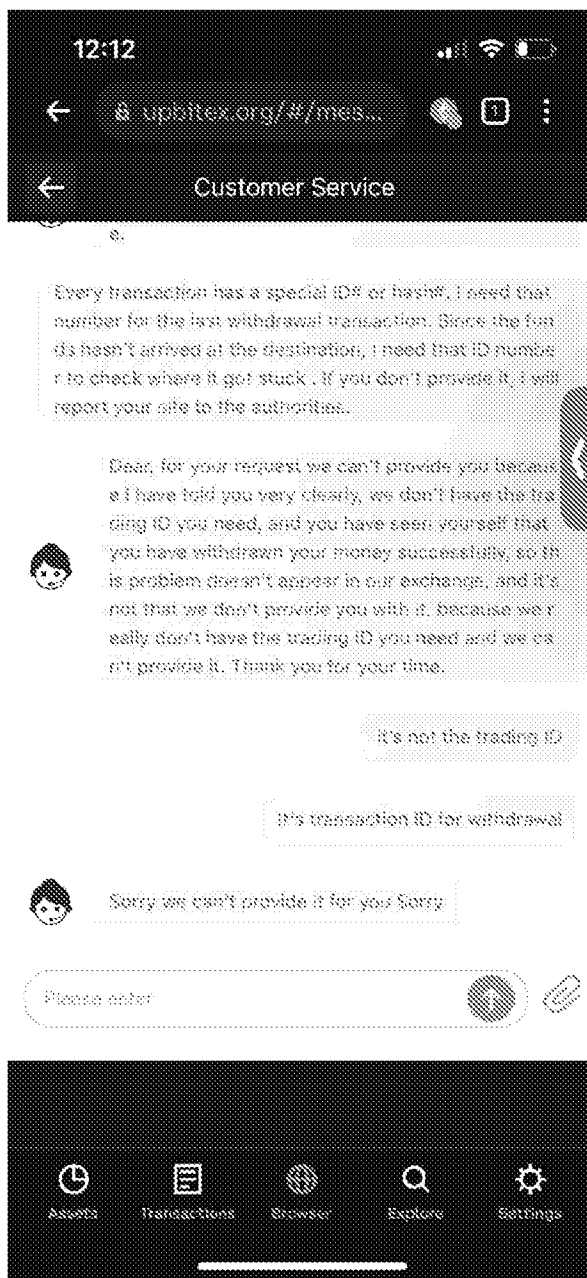
26. Representing themselves as “Customer Service” contacts at the “upbitex” platform, however, Defendants informed Plaintiff that she would be required to pay an additional “tax” in order to make withdrawals, as indicated in the screenshots below:



27. Plaintiff followed Defendants' instructions, and paid approximately \$22,745 of "tax," as indicated in the screenshot below:



28. After Plaintiff sent these additional funds, Defendants refused to permit her to withdraw any funds from the platform, giving various excuses, as indicated in the screenshot below:



29. Defendants subsequently blocked Plaintiff from accessing her accounts and transferring funds, using standardized excuses.

30. After Plaintiff could not recover her funds, she contacted Inca Digital (“Inca”), a cryptocurrency investigation firm, which traced her transactions and confirmed that Defendants were orchestrating a fake cryptocurrency trading platform scheme. As described below, Inca investigated other transactions involving the fake trading platforms and found that these transactions were part of a common scheme to steal Class Member funds.

C. INCA CAPITAL CONFIRMS THE SCHEME AND TRACES CLASS MEMBERS’ STOLEN ASSETS

31. Inca Digital is a sophisticated digital market investigation firm. It was founded in 2009 when it built open-source data analytics tools for INTERPOL, helping catch bad actors in illicit markets. Inca’s CEO, Adam Zarazinski, spent four years as an active-duty judge advocate with the US Air Force, serving at Joint Base Andrews and in Afghanistan. Others at the firm come from similar backgrounds, having worked for the US and other militaries and intelligence agencies from the US and around the world. Relying on Inca’s investigations, courts around the country have entered orders freezing wallets containing potentially hundreds of millions of dollars in stolen cryptocurrency. In 2023, the Defense Advanced Research Projects Agency (“DARPA”) contracted with Inca to study cryptocurrency markets, “exploring advanced methods for identifying and analyzing activity involving distributed ledgers, crypto and other digital assets.”³ A “beneficial side effect” of DARPA’s work with Inca is gaining “a better understanding of illicit actors’ behavior,” according to DARPA a program manager. *Id.*

32. Here, Inca’s investigation revealed that Defendants used the fake cryptocurrency platform to steal Class Members’ assets, including Plaintiff’s assets, and then sent those assets through a web of transactions designed to hide their trail.

³ See <https://www.axios.com/2023/04/11/inca-digital-darpa-crypto>, last accessed on July 23, 2024.

33. As outlined in Exhibit A, Inca identified the specific cryptocurrency wallets in which the ill-gotten gains of Defendants' scheme are *presently* held. Time is critical, as Defendants can transfer these cryptocurrency proceeds beyond Class Members' knowledge and reach at any moment.

34. 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. This tracing led to the wallets set forth in Exhibit A, each of which hold assets involved in transactions that originated from Class Member wallets.

35. After identifying the wallet addresses to which Plaintiff's funds were transferred, Inca "reverse traced" in phase two. This process allowed Inca to identify additional wallet addresses involved in the same transaction patterns, revealing more victims of the scheme.

36. Based on Inca's investigation, Defendants' conversion scheme involved transactions from November 18, 2023, through at least the date of this Petition. It affected approximately 200-250 Class Member victims and involved the conversion of at least \$8 million of Class Member funds by Defendants, with potential losses being higher.

37. In sum, Defendants employed a systematic multi-stage crypto theft scheme to target Class Members, including Plaintiff, and lured them to transferring increasing amounts of cryptocurrency through a fake cryptocurrency trading platform. The final step in this scheme, identical for Class Members, was the theft of their funds by Defendants.

38. The addresses of the wallets identified by Inca, where Class Member funds were ultimately sent, are listed in Exhibit A and categorized by the exchanges they are on. Plaintiff seeks to freeze these wallets and requests that this Court issue a Temporary Restraining Order, a Temporary Injunction, and a Permanent Injunction to freeze these wallets.

V. CLASS ALLEGATIONS

39. This action may be properly maintained as a class action pursuant to TEX. R. CIV. P. 42.

40. 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 Exhibit A, or in other cryptocurrency accounts controlled by Defendants at the exchanges set forth in Exhibit A.

41. 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.

42. 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 Exhibit A to this Complaint, as well as through discovery, including into account records at relevant institutions.

43. The same "pig butchering" scheme involving the same fake trading platform 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.

44. 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 her 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.

45. Plaintiff will fairly and adequately represent the Class and protect the interests of the class. By proving her 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.

46. 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.

47. 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.

48. The “platform” Defendants created to lure Plaintiff and Class Members – on a site which no longer exists – was fake. But the money taken by Defendants is real and so are the wallets and the assets held in them as identified in Exhibit A. Because those assets are real, they must be held on legitimate cryptocurrency platforms such as Binance, OKX, Gate.io, KuCoin, LBank, and others. By this Petition, Plaintiff and Class Members make no allegation that any of these legitimate crypto platforms had any prior knowledge of the unlawful conduct which led to the transfer of these assets onto their platforms. Plaintiff and Class Members do, however, request that

they be identified as enjoined parties in order to secure the unlawfully-obtained assets being stored in their systems.

49. 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 Exhibit A, Plaintiff and Class Members will not be able to recover their funds, and will lose their property forever.

VI. CAUSES OF ACTION

A. CONVERSION

50. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs.

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

52. The cryptocurrency assets transferred by Plaintiff and Class Members to the Defendants was (1) delivered for safekeeping, (2) intended to be kept segregated, (3) substantially in the form in which it is received or an intact fund, and (4) not the subject of a title claim by any Defendant.

53. The cryptocurrency assets of Plaintiff and all Class Members are or will be specifically identifiable, because Defendants' wrongful actions alleged herein involve cryptocurrency assets that are traceable along one or more blockchain technologies used to transfer cryptocurrency assets.

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

B. MONEY HAD AND RECEIVED / UNJUST ENRICHMENT

55. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs.

56. Defendants hold money or cryptocurrency stolen from Plaintiff and Class Members. That money or cryptocurrency was obtained unlawfully.

57. In equity and good conscience, all money or cryptocurrency held in the wallets described in Exhibit A belong to the Plaintiff and Class Members from whom they were stolen.

C. WRIT OF SEQUESTRATION / REPLEVIN

58. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs.

59. Defendants have taken possession of Plaintiff and Class Members' personal property, namely cryptocurrency. In equity and good conscience, all cryptocurrency held in the wallets described in Exhibit A belong to the Plaintiff and Class Members from whom they were stolen.

60. There is immediate danger that the Defendants in possession of that property will conceal or dispose of it through anonymous and speedy asset dissipation. It would be a simple matter for Defendants to transfer cryptocurrency to unidentified recipients outside the traditional banking system and effectively place the assets at issue in this matter beyond the reach of the Court. Here, through substantial effort, the current location of the cryptocurrency has been established. But that location can change quickly because Defendants can quickly and easily move the cryptocurrency to other digital wallets, continuing to put those assets outside the reach of victims and this Court.

61. The only way to prevent the foregoing irreparable harm is the sequestration of the wallets that currently hold the cryptocurrency, thereby preventing Defendants from transferring the cryptocurrency to parts unknown.

VII. REQUEST FOR *EX PARTE* INJUNCTIVE RELIEF

62. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs.

63. Plaintiff and Class Members request the Court enter a Temporary Restraining Order and Temporary Injunction preventing Defendants, non-parties Binance Holdings Ltd., OKX, Gate.io, KuCoin, LBank, and any of their agents, servants, employees, attorneys, partners, successors, assigns, subsidiaries, or any other person(s) through which they act, or who act in active concert with them and who receive actual notice of such order(s) from: withdrawing, transferring, selling, encumbering, or otherwise altering any of the cryptocurrency or assets held in the wallet addresses listed in Exhibit A of this Order, whether such property is located inside or outside the United States of America. Such a freeze is necessary to preserve the possibility of restitution for the Plaintiff and other victims.

64. Plaintiff and Class Members request the Court issue the temporary restraining order on an *ex parte* basis for the reasons described above and because the Defendants are a criminal enterprise who have already caused Plaintiff and Class Members to lose substantial amounts of money, repeatedly providing excuses as to why money cannot be returned to them. Defendants have transferred Plaintiff and Class Members' money between wallets repeatedly in an effort to hide it from them. It is only because of the extraordinary skill of Plaintiff and Class Members' investigators that the wallets identified in Exhibit A have been found. Should the Defendants

receive notice of this application, they will move the assets again, but this time in a way that Plaintiff and Class Members cannot trace.

65. Without the issuance of an *ex parte* temporary restraining order, Plaintiff and Class Members will suffer immediate and irreparable injury, loss, or damage because Defendants will, as they have in the past, transfer the stolen cryptocurrency, hiding it from Plaintiffs and Class Members and outside the reach of this Court. Since the Defendants almost certainly concealed their identities in furtherance of this scheme, it is impossible or impractical to provide notice to them. Providing notice to the Defendants would moot the request for injunctive relief.

66. Pursuant to Texas Rule of Civil Procedure 684, "no writ of injunction shall issue except upon the giving of a bond." However, Texas courts have "considerable discretion" in setting the amount of the bond. *See Hsin-Chi-Su v. Vantage Drilling Co.*, 474 S.W.3d 284, 304 (Tex. App.—Houston [14th Dist.] 2015, pet. denied). Here, the provisional relief sought aims to freeze the wallets where the stolen cryptocurrency was traced. Defendants have no legitimate claim to this stolen property and will sustain no damages if they are restrained from further transferring these assets. Therefore, Plaintiff requests a nominal bond to enjoin the transfer of assets stolen from her.

67. Plaintiff proposes a method of service that is the best available under the circumstances and is reasonably calculated to provide actual notice to Defendants. Traditional methods of service are unavailable due to Defendants' use of fictitious identities and unknown locations. Therefore, Plaintiff requests that the Court authorize an alternative method of service pursuant to Texas Rule of Civil Procedure 106(b), which allows for service in any manner that the court finds will be reasonably effective to give the defendant notice of the suit.

68. Therefore, the Proposed Order requires Plaintiff to serve a copy of the Order, as well as Plaintiff's Petition, within this period upon the owners of each identified wallet through a special purpose token or similar device delivered or airdropped into these wallets. Each service token will contain a hyperlink to a website maintained by Plaintiff's counsel or investigators, which will include the Order and all related papers. This method effectively notifies Defendants of the pendency of this action and informs them how they may object to the TRO and/or requested temporary injunction.

69. Additionally, the Proposed Order directs that the exchanges where these cryptocurrency wallets are held, provide separate notice of this Order to the customers of each identified cryptocurrency wallet. This comprehensive approach is reasonably calculated to lead to actual notice to the actual owners of the affected cryptocurrency wallets, who may then appear at the preliminary injunction hearing if they wish.

VIII. CONDITIONS PRECEDENT

70. All conditions precedent have been performed, occurred, or excused.

IX. MAXIMUM DAMAGES

71. Plaintiff and Class Members seek monetary relief in excess of \$1,000,000. Tex. R. Civ. P. 47(c)(4).

X. CONCLUSION AND PRAYER

Plaintiff and Class Members pray that the Court enter a temporary restraining order as described above, temporary and permanent injunctive relief, certify the class described above, and, upon final trial of this case, they have and recover judgment against Defendants as follows:

- a. Actual damages;

- b. Disgorgement of all funds currently held in the cryptocurrency wallets described in Exhibit A;
- c. Distribution of all funds held in the cryptocurrency wallets described in Exhibit A;
- d. Replevin;
- e. Exemplary damages;
- f. Prejudgment interest on all amounts unlawfully retained by Defendants;
- g. Postjudgment interest at the highest amount permitted by law on all amounts awarded until paid;
- h. Costs of Court; and
- i. All other and further relief to which they may show themselves to be justly entitled.

Respectfully submitted,

BERG PLUMMER & JOHNSON, LLP

By: /s/ Geoffrey Berg (by permission)
Geoffrey Berg (gberg@bergplummer.com)
Texas Bar No. 00793330
3700 Buffalo Speedway, Suite 1150
Houston, Texas 77098
713-526-0200 (tel)
832-615-2665 (fax)

DOW GOLUB REMELS & GILBREATH, PLLC

By: /s/ Andrew S. Golub
Andrew S. Golub
Texas Bar No. 08114950
asgolub@dowgolub.com
2700 Post Oak Blvd., Suite 1750
Houston, Texas 77056
Telephone: (713) 526-3700
Facsimile: (713) 526-3750

ATTORNEYS FOR PLAINTIFF

Exhibit A

Binance

0x6E031365EBa4A48E47015aF708c943c2F119C52b
0xe4CAC07aaba8e667Ef8413aFDE82cdA897a80804
0x270Cb3c9869A2A09C23b8E0B838501724DAE5C9B
0xc70b18eAaa79f87E79deB79a9f6e2886CA7aEDbC
0xA66d89F035756F98FF9aC4a3b48e1E5fdE086E26
0x28E6d72063A5B9B26173F81609D07aF899682f7F
0x1F7C1deaDfB8FA8f5CD9A42cf34C70327c19C420
0xEeF5E766036AF94C5599C1025774706706F5B7ea
0x3Bf212B83c37A33fC4F2aF3f8fBDeBE25D4118F6
0x723a01d4344d97b0Cf937eEc599AFF717028108d
0x48ca7E8A3D62c546cD57BdDCE6354cfA72C3f478
0xd31734Cdeb17aE29Dfe161b1EF729e4611047E19
0x7db44943441A61Fe5359bea8c7b344f4Cc663Ca1
0x6Ba52c611A6fdAb14c77B5b12b53C9B85d0A4465
0x8851b21d296942e804b3Eaa47049BD62c7C419A8
0x33D591c68bfb5bAA6753dB30aa937756c6b3fA30
15Q1cvrFiG4rDPQa4CPT28v6v142KDtfYM

OKX

0xd49cd43230860f7A244D52FCD78a43CbE068e8Ff
0xa4A76eC9697Be8fcF1fDb907d9e2F64378c83762
0x0eC4E0303897a8E8b477Fdce43e577B3981b5617
0xdA22870E0Bd87133250fbC319476E278D7af93c2
0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6

ByBit

0x64fA177058113A5D668A4a33809514740AB20a57
0xf614c8dA40D87B16a04150ec36fBC23e8f303aAf

KuCoin

0xCB63262C60aa7CBCe8E128F746D75DEf6B59dDA3

BloFin

0xE385be9087900D61db242d6776A1468Bc3EfebC5

HTX

1MspmVHmVLA2y841xapZcCEoFHiwGlyeap

CAUSE NO. _____

NATALIA ELMOWAFI, on behalf of
Herself and all others similarly situated,

Plaintiff,

V.

CHRIS YANG and JOHN DOES 1-25,

Defendants.

§
§
§
§
§
§
§
§
§

IN THE DISTRICT COURT OF

HARRIS COUNTY, TEXAS

JUDICIAL DISTRICT

VERIFICATION

STATE OF _____ §
§
COUNTY OF §

My name is Natalia Elmowafi. I am over 18 years of age, have never been convicted of a felony or a crime of moral turpitude, and am otherwise competent to execute this declaration. I am the named plaintiff in the above-captioned matter, which I have filed as a class action on behalf of myself and all others similarly situated.

The facts stated in Paragraphs 17-30 of Plaintiff's Verified Original Class Action Petition, Application for Temporary Restraining Order, Temporary, and Permanent Injunctions ("Petition") are within my personal knowledge and are true and correct. Moreover, the screenshots included in the Petition were taken by me on my phone. They are true and accurate representations of what they purport to be. I have not altered them in any way, except as indicated above to protect personally identifiable information.

My name is Natalia Elmowafi, my date of birth is July 12, 1977, and my address is 7100 Alameda Rd., Apt. 2230, Houston, Tx 77054. I declare under penalty of perjury the foregoing is true and correct.

Executed in Houston, Harris County, Texas on July 23, 2024.



Natalia Elmowafi

CAUSE NO. _____

NATALIA ELMOWAFI, on behalf of	§	IN THE DISTRICT COURT OF
Herself and all others similarly situated,	§	
	§	
Plaintiff,	§	
	§	
V.	§	HARRIS COUNTY, TEXAS
	§	
CHRIS YANG and JOHN DOES 1-25,	§	
	§	
Defendants.	§	<u>JUDICIAL DISTRICT</u>

VERIFICATION

STATE OF _____ §
§
COUNTY OF §

My name is Charles Zach. I am over 18 years of age, have never been convicted of a felony or a crime of moral turpitude, and am otherwise competent to execute this declaration. Attached hereto is a true and correct copy of my curriculum vitae.

I am employed as a Lead Illicit Finance Investigator by Inca Digital, a company that investigates cryptocurrency schemes, including “pig butchering.” As part of my employment at Inca Digital, I have investigated matters related to the above-captioned action. The facts stated in Paragraphs 31-38 of Plaintiff’s Verified Original Class Action Petition, Application for Temporary Restraining Order, Temporary, and Permanent Injunctions (“Petition”) are within my personal knowledge and are true and correct. Moreover, I declare the following is true and correct:

1. I hold a Master of Arts in Global Risk from Johns Hopkins University, School of Advanced International Studies (SAIS), where I specialized in Strategic Foresight for Political Risk Analysis, Risk in International Politics and Economics, and Conflict and Risk in Cyberspace. Additionally, I earned a Bachelor of Arts in International Relations with a concentration in European Studies from the University of Arkansas.

2. I am a Certified Cryptocurrency Tracing Examiner (CTCE) and possess foundational certifications in Anti-Money Laundering and Transaction Monitoring. I am also a member of the Association of Certified Anti-Money Laundering Specialists (ACAMS).

3. As part of my employment at Inca Digital, I conduct digital asset investigations and generate actionable intelligence insights. Prior to my role at Inca Digital, I served as a Cleared American Guard with NVE Inc. and the United States Department of State, managing access control, secure material storage, and classified documents control. Additionally, I have experience as a Marine Embassy Security Guard with the United States Marine Corps, where I controlled daily security operations for embassy compounds and supervised local national guard forces.

4. Based upon my expertise in blockchain forensics and my substantial experience investigating “pig butchering” schemes similar to this one, if Plaintiff is required to wait until after the Defendants receive notice of this action, it is highly likely that Defendants will transfer cryptocurrency at issue beyond the reach of discovery or recovery.

5. I am familiar with the process of providing notice via the deposit of airdropped or similar service tokens to cryptocurrency accounts, and in my experience, the method of notice proposed in the Proposed Order is reasonably calculated to and would likely result in actual notice of those documents to the individuals or entities that control those wallets, and the existence and contents of those service tokens would be readily apparent to the owners.

My name is Charles Zach, my date of birth is July 11, 1989, and my address is Brnaze 239C, Sinj, Croatia. I declare under penalty of perjury the foregoing is true and correct.

Executed in Sinj, Splitsko Dalmatinska, Croatia on July 23, 2024.



Charles Zach

Engaging and detail-oriented professional with a big picture mindset, exceptional time management skills, and the capacity to energize a team of professionals by creating a dynamic and innovative team culture.

Qualifications Summary

- ♦ Innovative professional specializing in Open Source Intelligence (OSINT) and Blockchain Forensics, with a global operational background. Demonstrates exceptional analytical skills and a keen eye for detail in high-stakes environments. Experienced in leveraging open-source data and blockchain technology to conduct in-depth analyses and investigations across diverse geographical regions.
- ♦ **OSINT Expertise:** Skilled in the strategic collection and analysis of open-source data to support intelligence and investigative efforts. Proficient in utilizing advanced OSINT tools and methodologies to uncover critical insights and inform decision-making processes.
- ♦ **Blockchain Forensics:** Deep understanding of blockchain technology and its applications in forensics. Experienced in tracing and analyzing cryptocurrency transactions to detect fraud, money laundering, and other illicit activities. Proficient in using blockchain analytics platforms to conduct comprehensive investigations.
- ♦ **Global Intelligence Operations:** Led multinational teams in gathering and analyzing intelligence from open sources, contributing to the security and strategic planning of operations across Europe, Africa, the Middle East, and the Americas.
- ♦ **Interagency Collaboration:** Established effective partnerships with international law enforcement and intelligence agencies, sharing insights and collaborating on OSINT and blockchain forensic investigations.
- ♦ **Risk Assessment & Security Strategy:** Leveraged OSINT and blockchain forensics to enhance security management and risk assessment frameworks. Developed and implemented strategies to mitigate potential threats identified through intelligence analysis.

Career Experience

Inca Digital | Remote: Split, Croatia

Lead Illicit Finance Investigator – National Security and Law Enforcement Team | June 2021 to Present

Exercise sound judgment and discretion while conducting investigations in the digital asset space. Demonstrate strong leadership and foresight while working with large financial and blockchain data sets to investigate alerts and generate reports and visualizations for publication.

- ♦ Refined investigative methodologies and established precise goals by integrating expert knowledge in blockchain forensics. This strategy enhanced the collection and analysis of data, providing actionable intelligence insights for clients navigating the complexities of blockchain adoption and its implications.
- ♦ Showcased analytical acumen and detail-oriented scrutiny by examining anomalies within blockchain data. This approach facilitated the uncovering of critical intelligence related to blockchain dynamics and the digital asset ecosystem, aiding national security and law enforcement agencies through sophisticated data collection techniques and forensic tools.
- ♦ Enhanced intelligence gathering capabilities by focusing on blockchain forensic analysis, enabling the extraction of pivotal insights from blockchain transactions and activities. This dedicated approach

informed strategic decisions for clients grappling with the security and regulatory implications of digital currencies, through advanced data collection and analytical methodologies.

NVE Inc. / United States Department of State | Dhahran, Saudi Arabia and Montevideo, Uruguay
Cleared American Guard | January 2018 to May 2020

Maximized productivity and provided vital structure by managing access control, secure material storage, and classified documents control in accordance with federal guidelines.

- ◆ Supervised access control and perimeter security of State Department overseas buildings for a total of 6,250 hours with zero security incidents; actions enabled several multimillion-dollar construction contracts to proceed ahead of schedule.
- ◆ Demonstrated insightful leadership and enhanced clarity of mission through supervision of daily security operations including multinational guard force, technical surveillance systems, and physical security.

United States Marine Corps / Embassy of the United States to Croatia | Zagreb, Croatia
Marine Embassy Security Guard | September 2016 to September 2017

Captured substantial gains in efficiency and productivity while controlling daily security operations for the embassy compound including access control, local national guard force supervision, emergency responses, and monitoring of technical surveillance systems.

- ◆ Embraced responsibility for fulfilling secondary responsibilities as Operations Manager, dedicating time outside of work to develop solutions to key security concerns facing the Embassy.
- ◆ Defined direction that catalyzed coordination of the Embassy's security risk mitigation strategies by developing six tactical frameworks and emergency response plans.

United States Marine Corps / Marine Security Augmentation Unit | Quantico, Virginia
Team Leader | September 2015 to September 2016

Leveraged experience and skill to perform comprehensive security assessments, produce tactical employment plans, and provide risk mitigation solutions for the United States Embassies in Madrid, Spain and Tallinn, Estonia.

- ◆ Ensured flawless execution while conducting security operations in support of United States government overseas diplomatic visits for President Barack Obama (Riyadh, Saudi Arabia), Vice President Joe Biden (Istanbul, Turkey and Belgrade, Serbia), and Secretary of State John Kerry (Oslo, Norway and Tbilisi, Georgia).
- ◆ Demonstrated balanced, disciplined leadership while leading team on a security augmentation mission to the US consulate in Rio de Janeiro during the 2016 summer Olympics.
- ◆ Employed refined relationship-building skills and collaborative mindset as liaison with local law enforcement and security forces during overseas missions.

United States Marine Corps / Embassy of the United States to Zambia | Lusaka, Zambia
Marine Embassy Security Guard | September 2014 to September 2015

Established strong foundation for success by controlling the embassy compound's daily security operations including access control, local national guard force supervision, emergency responses, and technical surveillance systems monitoring.

- ◆ Demonstrated exceptional planning, logistics, and communication skills by coordinating the annual Marine Corps Ball.
- ◆ Exercised detailed analysis and judgment while managing Marine detachment financial accounts, with a 100% pass rate during each monthly audit.

United States Marine Corps / National Security Agency | San Antonio, Texas

Signals Intelligence Analyst | June 2011 to July 2014

Provided insightful vision and guidance while preparing written and oral briefings for high-level leadership on potential solutions regarding time sensitive intelligence requirements. Exhibited exceptional critical thinking and creative ability to deliver intelligence solutions by performing Target Discovery and Target Development analysis in response to customer requests for essential information.

Education

Master of Arts in Global Risk (3.56 GPA), May 2021

Selected Coursework: Strategic Foresight for Political Risk Analysis, Risk in International Politics and Economics, Conflict and Risk in Cyberspace

Johns Hopkins University, School of Advanced International Studies (SAIS), Bologna, Italy

Bachelor of Arts, International Relations | European Studies Concentration (3.10 GPA), May 2011

Chancellor's Scholarship

University of Arkansas, Fayetteville, AR

Professional Proficiencies and Coursework

Microsoft Office Suite | Geographic Information Systems (GIS) | Python | Splunk | Introduction to Country Risk and Political Analysis | How to Write Country Risk Reports for Corporate and Institutional Clients | Country Risk Modeling and Writing

Professional Certifications

Cryptocurrency Tracing Certified Examiner (CTCE)

Anti-Money Laundering Foundations

Transaction Monitoring Foundations

Professional Community Memberships

Association of Certified Anti-Money Laundering Specialists (ACAMS)

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Brenda Castillo on behalf of Andrew Golub

Bar No. 8114950

bcastillo@dowgolub.com

Envelope ID: 90140545

Filing Code Description: Petition

Filing Description: Plaintiff's Original Verified Class Action Petition, Application for Temporary Restraining Order, Temporary, and Permanent Injunctions

Status as of 7/24/2024 3:26 PM CST

Associated Case Party: Natalia Elmowafi

Name	BarNumber	Email	TimestampSubmitted	Status
Andrew SGolub		asgolub@dowgolub.com	7/24/2024 2:40:50 PM	SENT
Geoffrey Berg		gberg@bergplummer.com	7/24/2024 2:40:50 PM	SENT

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Brenda Castillo		bcastillo@dowgolub.com	7/24/2024 2:40:50 PM	SENT
Tracy Moebes		tmoebes@bergplummer.com	7/24/2024 2:40:50 PM	SENT



I, Marilyn Burgess, District Clerk of Harris County, Texas certify that this is a true and correct copy of the original record filed and or recorded in my office, electronically or hard copy, as it appears on this date.

Witness my official hand and seal of office this November 19, 2024

Certified Document Number: 115552402 Total Pages: 32

Marilyn Burgess, DISTRICT CLERK
HARRIS COUNTY, TEXAS

In accordance with Texas Government Code 51.301 and 406.013 electronically transmitted authenticated documents are valid. If there is a question regarding the validity of this document and or seal please e-mail support@hcdistrictclerk.com