CAUSE NO. 25-BC11B-0067

RISPBA MCCRAY-GARRISON, STACEY BROWN, WEN CAO, JESSECA DICKERSON, NARESH GORANTLA, MATTHEW HIZON, JORDAN PARTIER, GREG RICHARDS, REITTA SEIDEL, MARIA SISSON, SAMANTHA KAUK VINCENT, ALEXANDRA MURRIETTA, PRASHANT KATYAL, STANISLAV TSOY, NEHA MALHOTRA, KYLE ADAMS, HILARIO FLORES, LANE GARNER, CHETAN JOSHI, BALAKRISHNA KONDURU, ABHISHEK SINGH, JOSE VASQUEZ, and BILL YOUNG, **Plaintiffs,**	§	IN THE BUSINESS COURT OF TEXAS
V.	§	ELEVENTH DIVISION
"TOM SHELDON HALEY" [WhatsApp: +1-470-697-1565], "JINGYI LI" [WhatsApp user], "JINGQIU NING" [WhatsApp: +1-973-282-8222], "KSENIA" [WhatsApp: +1-213-661-3580], "NINA/ANNIE" [WhatsApp: +1-917-420-3859], "ZOE" [WhatsApp: +1-332-272-4264, +1-626-630-9256, +1-646-294-9168], "GRACE LIN" [Facebook Messenger user], "SAM BENNETT" [Telegram user], "CAROLINE MARTIN" [WhatsApp: +1-458-250-9980], "MARK/PROFESSOR" [WhatsApp: +1-740-491-1166, Telegram: @Mark44777], "ASSISTANT ERIN" [WhatsApp: +1-234-301-8088], "EMILY TRENT" [WhatsApp user], "DAVID" [WhatsApp user], "SHELBY PETTY" (IMPERSONATOR) [WhatsApp: +44-7449-0075], "DIANNE HOLLISTER" [Email: diannehollister0@gmail.com], "MARCO ROSSI" [WhatsApp user], "EMILY" [WhatsApp: +1-646-296-7124], "DAVID" [WhatsApp: +1-778-595-0741], "LAUREN CHRISTIE" [WhatsApp: +1-503-421-5594, +1-503-752-7094, +1-404-493-5667, +1-	§	COURT 11B

503-490-6297, Telegram: @ASO1268], § "PROFESSOR WILBUR CLARK" § [WhatsApp: +1-404-441-9801, +1-503-998- § 5264, +1-503-449-5634], ZHIDE CO § LIMITED [Standard Chartered Bank Hong § Kong, Account: 40711487154, UNIT § 1406B, 14/F, THE BELGIAN BANK § BUILDING, NOS.721-725 NATHAN § ROAD, KL], HS TRADE HONG KONG § CO., LTD [Bank of Communications Hong § Kong, Account: 382561107723101, 2-14 § Tai Fung Street, Yuen Long District, Hong § Kong), "JOAN ANDREWS" (WhatsApp: § +1 774 703 5065), RCBEHIND SCREEN § INC., LIGHTWEIGHT HIFIER INC., § COMMERCE BLAZE INC., "JENNY § KOWALSKA" (WhatsApp: +1-332-248- § 3624), "ALBEE JIANG" (Line § Messenger),"MARTINA" (WhatsApp § Contact), "LISA DAVIS" (WhatsApp), § "PROFESSOR JOHN" (IPA Community), § "ELLA" / "LI XIN YUE" (Instagram: § glamgoddesscara, WhatsApp: +1-312-536- § 3950, +1-415-795-7328), "RODNEY" § (app.bmcc88.vip), "KAYLA" § (app.bmcc88.vip), "LUNA LEE" § (WhatsApp+1-628-629-5774),"HENRY § ROGAN" (WhatsApp+1-973-809-3948), § "SILVERLAKEVIRTUAL" § (silverlakevirtual.com),"AI MINING" (defi- § mining.tech), "RICHARD BILL" § [WhatsApp: +1-404-319-9709],"JAMES § WILSON" [WhatsApp: +1-404-449-5999], § "MALCOIN008" [Telegram: § @Malcoin008], "CRYPTO MERCHANT" § [Telegram: @CryptoMerchant009], § "POINTS REDEEMER" [Telegram: § @ZMQ112233], FB Financial Institute § [operating through website: fortune- § build.com], MalCoin Trading Platform § [operating through websites: § globalmalcoin.com, h5.malcoin.top, and § h5.globalmalcoin.com], JOHN DOES 1-10, § and JANE DOES 1-, **Defendants.** §

PLAINTIFFS' FIRST AMENDED ORIGINAL VERIFIED PETITION, FIRST AMENDED APPLICATION FOR TEMPORARY RESTRAINING ORDER, TEMPORARY AND PERMANENT INJUNCTIONS

TO THE HONORABLE JUDGE OF SAID COURT:

PLAINTIFFS file this First Amended Verified Petition, First Amended Application for Temporary Restraining Order, Temporary and Permanent Injunctions, and respectfully show the Court the following:

I. DISCOVERY CONTROL PLAN

1. Plaintiffs intend to conduct discovery under Level 2 of Texas Rule of Civil Procedure 190.3. Due to the technical complexity of this cryptocurrency fraud case involving multiple international defendants and sophisticated blockchain transactions, Plaintiffs anticipate the need for extended discovery time frames and specialized technical discovery methods.

2. This case involves technically sophisticated cryptocurrency fraud operations conducted through multiple digital platforms, international cryptocurrency exchanges, and numerous blockchain wallet addresses. The nature of these transactions requires specialized discovery procedures to properly trace, document, and preserve digital evidence.

3. Plaintiffs will require access to blockchain forensic analysis, exchange transaction records, international wire transfer documentation, and digital communication records. Due to the cross-border nature of the fraud and the technical complexity involved, Plaintiffs request the Court's assistance in facilitating appropriate discovery from cryptocurrency exchanges and international financial institutions.

4. The technical nature of this case necessitates discovery of electronic information in native formats to preserve critical metadata and technical transaction details. Plaintiffs will seek

discovery of wallet address control mechanisms, exchange account ownership records, and fund flow documentation that may require specialized electronic discovery protocols.

5. The documented evidence in the McCray-Garrison case reveals technical complexities requiring specialized discovery approaches, including blockchain forensic analysis of fund movements across 59 cryptocurrency addresses and more than 1,000 exchange transfers, technical examination of the multiple interconnected platforms used in the scheme, and preservation of encrypted communications within hierarchical group channels. This evidence demonstrates the need for expert testimony regarding sophisticated fund movement patterns across multiple international cryptocurrency exchanges and specialized protocols for data authentication and admission.

6. Plaintiffs request the Court establish appropriate protocols for the preservation, collection, and authentication of blockchain evidence, digital platform records, and cryptocurrency transaction data to ensure the integrity of evidence in this technically complex case.

II. INTRODUCTION

7. This case involves a sophisticated, international cryptocurrency fraud scheme in which Defendants employed elaborate social engineering tactics and fraudulent investment platforms to induce victims to transfer cryptocurrency assets worth millions of dollars.

8. Between January 2023 and February 2025, Defendants systematically targeted Plaintiffs through multiple coordinated channels including social media platforms, messaging applications, dating sites, and compromised accounts of known associates.

9. Through technically sophisticated deception, Defendants provided Plaintiffs access to professional-looking but entirely fraudulent trading platforms that displayed artificial profits while implementing systematic withdrawal prevention mechanisms.

10. In this case, Defendants utilized more than fifteen fraudulent trading platforms to lure Plaintiffs into transferring approximately $5,870,983 in cryptocurrency assets through hundreds of blockchain transactions.

11. Blockchain forensic analysis shows systematic dispersion of funds across multiple major cryptocurrency exchanges through complex patterns of transfers designed to obscure the source of funds.

12. The operations conducted by Defendants bear all the hallmarks of what law enforcement agencies have identified as "pig butchering" scams, a sophisticated form of financial fraud that combines social engineering, technical deception, and psychological manipulation to extract maximum funds from victims.

13. Defendants employed a multi-phase approach that began with trust-building through legitimate investments or social connections, followed by platform migration, progressive investment escalation, and ultimately the implementation of technical mechanisms designed to prevent fund withdrawal.

14. Defendants employed documented psychological manipulation tactics including exclusivity through 'VIP' programs, artificial time constraints, manufactured emergencies, and strategic success demonstrations.

15. The perpetrators of this scheme demonstrate significant technical capabilities in cryptocurrency operations, including wallet address management, cross-chain transactions, exchange integration, and sophisticated fund movement patterns consistent with professional money laundering operations.

16. Each Plaintiff's experience demonstrates a methodical pattern of manipulation designed to build trust, maximize financial extraction, and ultimately prevent fund recovery through technical barriers, psychological pressure, and systematic withdrawal obstacles.

17. Defendants operate what appears to be a transnational criminal enterprise with sophisticated technical infrastructure, coordinated social engineering tactics, and complex financial operations spanning multiple blockchain networks, cryptocurrency exchanges, and international banking systems.

18. Due to the irreversible nature of cryptocurrency transactions and the immediate risk of further fund dissipation, temporary ex parte injunctive relief is required to preserve identifiable cryptocurrency assets in wallets and exchanges where they can be traced and potentially recovered.

19. The technical nature of cryptocurrency operations, combined with the international scope of this scheme, necessitates specialized approaches to asset preservation, fund tracing, and recovery efforts that traditional financial fraud remedies cannot adequately address.

20. This petition seeks emergency injunctive relief to freeze identifiable cryptocurrency assets, preserve electronic evidence, and prevent further dissipation of funds while the Court examines the substantial evidence of fraud documented through blockchain analysis, exchange records, and communication logs.

21. Plaintiffs bring this action seeking all available legal remedies, including without limitation actual damages, exemplary damages, declaratory judgment, asset preservation, disgorgement of ill-gotten gains, and such other relief as the Court deems just and proper. Some of the Plaintiffs had previously filed in Harris County but dismissed the case without prejudice.

III. JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to Texas Government Code § 24.007 because the amount in controversy exceeds the minimum jurisdictional limits of the district courts of the State of Texas.

23. This Court has personal jurisdiction over Defendants because they purposefully directed their activities toward the State of Texas and purposefully availed themselves of the privilege of conducting activities within Texas, thus invoking the benefits and protections of its laws. Defendants systematically targeted multiple Texas residents, including lead Plaintiff Dr. Rispba McCray-Garrison, a resident of League City, Galveston County, Texas, as well as Plaintiffs Naresh Gorantla (Plano, Collin County), Greg Richards (Kerrville, Kerr County), Reitta Seidel (Cibolo, Guadalupe County), Samantha Kauk Vincent (Rosharon, Brazoria County), and Prashant Katyal (Austin, Travis County).

24. Personal jurisdiction over Defendants is proper because they intentionally reached into Texas through electronic communications directed at Texas residents, established continuing relationships with Texas residents, and engaged in systematic and continuous contacts with Texas through regular and sustained communication with the Texas-resident Plaintiffs.

25. Defendants' contacts with Texas include, but are not limited to:

- Initiating and maintaining regular WhatsApp and Telegram communications with Texas-resident Plaintiffs;
- Directing Texas-resident Plaintiffs to transmit funds through cryptocurrency exchanges operating in Texas;
- Creating and maintaining online accounts for Texas-resident Plaintiffs on fraudulent trading platforms;
- Accessing and manipulating account information of Texas-resident Plaintiffs;

- Soliciting and accepting cryptocurrency transfers from Texas-resident Plaintiffs; and
- Causing financial and emotional harm to Texas-resident Plaintiffs while knowing they resided in Texas.

26. Venue is proper in Galveston County pursuant to Texas Civil Practice & Remedies Code § 15.002(a)(1) and (2) because a substantial part of the events or omissions giving rise to the claims occurred in Galveston County, and because lead Plaintiff Dr. Rispba McCray-Garrison resides in Galveston County, Texas.

27. Specifically, Defendants "Lauren Christie," "Professor Wilbur Clark," and related entities directed their fraudulent communications and solicitations to lead Plaintiff Dr. Rispba McCray-Garrison while she was located in League City, Galveston County, Texas. These communications resulted in Rispba McCray-Garrison transferring $310,133.22 in cryptocurrency and fiat currency while she was located in Galveston County.

28. The torts committed by Defendants occurred in substantial part in Galveston County, as the fraudulent misrepresentations were received by Plaintiff McCray-Garrison in Galveston County, the cryptocurrency transactions were initiated from Galveston County, and the financial and psychological injuries were suffered in Galveston County.

29. Each of the Defendants is subject to the jurisdiction of this Court pursuant to the Texas long-arm statute, Texas Civil Practice & Remedies Code § 17.042, because each Defendant has committed torts in whole or in part in Texas and/or has established minimum contacts with Texas such that maintenance of this lawsuit does not offend traditional notions of fair play and substantial justice.

30. The exercise of jurisdiction over each Defendant is reasonable in light of their contacts with the State of Texas and the interests of Texas in providing a forum for its residents to seek redress for harms caused by out-of-state actors, particularly in cases involving technological fraud where geographical boundaries are intentionally obscured by the perpetrators.

31. This Court has jurisdiction over the subject matter of this action pursuant to principles of equity, the Texas Uniform Foreign Country Money Judgments Recognition Act, the Texas Business and Commerce Code, and other applicable laws of the State of Texas.

IV. PARTIES

A. PLAINTIFFS

32. Plaintiff Dr. Rispba McCray-Garrison is a resident of League City, Galveston County, Texas. The fraudulent investment scheme targeting her operated through the MalCoin trading platform (h5.globalmalcoin.com) and FB Financial Institute, resulting in losses of $310,133.22 through documented cryptocurrency transactions between July 9, 2024, and October 8, 2024. The perpetrators initially contacted Dr. McCray-Garrison through an Instagram advertisement for a purported investment educational course, systematically building trust through a sophisticated 'AI 4.0' investment system, VIP group membership, and artificial profit displays. Blockchain forensic analysis has traced these stolen funds through 59 related cryptocurrency addresses to multiple cryptocurrency exchanges including Binance (42%), OKX (23%), Huobi (15%), Gate.io (8%), Bybit (5%), and other exchanges (7%), with 1,105 documented instances of fund transfers to these centralized exchanges. The scheme involved transfers of Bitcoin (BTC) through wallet addresses39ugYdrSAZgiTYASntVqcTkkVkcrSmZszw, 3JvwosoWJUaCQH5M7YiJzAwn93BtRs6QNZ, and

1M8QjVDyhHzrVXonTQzg75gyu4ycnMmYj2, as well as transfers of Ethereum (ETH) through wallet address 0xd715d26bd4eeeb449dc738eab2f4e460ef380ee1.

33. Plaintiff Stacey Brown is a resident of Schuylkill Haven, Schuylkill County, Pennsylvania. The fraudulent investment scheme targeting her operated through the tradepropel.com platform, resulting in losses of $698,919 through documented cryptocurrency transactions between March 30, 2024, and June 6, 2024. The scheme involved transfers of 10.77975 BTC through wallet addresses 1QCPughtAraSkNdseEBvv6wbjFiU5j9Agg, 14QhT2sgAF7bRS944Ap2JuuvtRyMkvvXNa,bc1qv3382swzls05cemkxjh3djfmzgsxmd6nne8y4c ,and bc1qranxtfenl06rwmjh0zggr30aqn4pnlnyqkarzh.

34. Plaintiff Wen Cao is a resident of Gainesville, Alachua County, Florida. The fraudulent investment scheme targeting him operated through multiple platforms including Decode Global and GroveXCO, resulting in losses of $126,951.27 through documented cryptocurrency transactions between June 21, 2024, and September 27, 2024. The scheme involved transfers of 48.188 ETH and 300 USDT through wallet addresses 0xA84e06AFa8a7792365927d632f7CE5161d0CaA26,0x069B6C43AF503777E5ae7Fca07F65dD7426296C1,0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89, and 0x90027E195b77C7d4EF2f6DB7cD85E3E9107716aA.

35. Plaintiff Jesseca Dickerson is a resident of Louisville, Jefferson County, Kentucky. The fraudulent investment scheme targeting her operated through the Chartranks.com platform, resulting in losses of $59,000 through documented cryptocurrency transactions between July 29, 2024, and October 11, 2024. The scheme involved transfers of 5,754.3489 USDT, 2.33327 ETH, and 0.11811376 BTC through wallet addresses 0xf7473f6a31d750b8edb171091cda747e0b4f5b3d,0x7bE7E8992501549Ded06fAd4cb697C758

2548831,0x5e3035cd4ce7f5bf892a639831dca6bf3bd7a95f,and TFjwz6rUKa2aVAATPTtB5aAUSG4uPP9x1eV.

36. Plaintiff Naresh Gorantla is a resident of Plano, Collin County, Texas. The fraudulent investment scheme targeting him operated through the unions.top platform, resulting in losses of approximately $350,000 through documented cryptocurrency transactions between July 2, 2024, and November 21, 2024. The scheme involved transfers of 56.963512 ETH through wallet addresses 0x36753759cc50a0a62cefe8dc17b7fdc2a791b8f5, 0x99576adba07f66961e4788448b0ce4ad77ed1f6d, and 0x04fd6aa4eb8a03c019e5d4e7d5a1fdbcb750052f.

37. Plaintiff Matthew Hizon is a resident of Milpitas, Santa Clara County, California. The fraudulent investment scheme targeting him operated through the Nexus Nebula Exchange (nebulairs.net) platform, resulting in losses of $712,492.93 through documented cryptocurrency transactions between May 17, 2024, and October 11, 2024. The scheme involved transfers of 663,600 USDT and 15.46 ETH primarily through wallet address 0x8EDA58986D1CC51cc77119f9ad6095c2c15539Ca.

38. Plaintiff Jordan Partier is a resident of Lancaster, Lancaster County, Pennsylvania. The fraudulent investment scheme targeting him operated through the globalcryptofield.com platform, resulting in losses of $83,362.00 through documented cryptocurrency transactions between May 7, 2024, and October 8, 2024. The scheme involved transfers of 1.21439 BTC through wallet addresses: bc1q0tx9pmhxdytw5dkcy9d7tc5sv82z4twg74hsvu, bc1qexavxlt2weweuq0scwdu5mdpfxdls8frz7heqv, and bc1qvsxkwhh8wz6c0l82y9jptgj8q4mlxn7rvn9nu3.

39. Plaintiff Greg Richards is a resident of Kerrville, Kerr County, Texas. The fraudulent investment scheme targeting him operated through the defistart.top platform, resulting in losses of $98,238.00 through documented cryptocurrency transactions between September 4, 2024, and October 11, 2024. The scheme involved transfers of 39.52354 ETH through wallet address 0x3Ab11B37773A9d76277024C909B7c124fCCd4371.

40. Plaintiff Reitta "Dee" Seidel is a resident of Cibolo, Guadalupe County, Texas. The fraudulent investment scheme targeting her operated through the Vebson Trading Platform (m.vebson.trade), resulting in losses of $204,186.70 through documented cryptocurrency transactions between August 8, 2024, and October 17, 2024. The scheme involved transfers of 4.19195816 BTC and 2.88848355 ETH through wallet addresses 1CyUJzpgFztJzMPmZqNwyeRzC8WDjok3i, 388TgpKxQxr7HPrAGGcyuGAv7UhkKfunzk, and 0xbc09a9dacc301c7b4ba6620e87916bb69017dfba.

41. Plaintiff Maria Sisson is a resident of Phoenix, Maricopa County, Arizona. The fraudulent investment scheme targeting her operated through the millioneurolistings.agency platform, resulting in losses of $250,000 through documented cryptocurrency transactions between July 21, 2024, and October 2, 2024. The scheme involved transfers of 81.53626 ETH and 0.73926902 BTC through more than thirty wallet addresses, including 0x9879Fb41c9E0C9eF8adB878a9fE655C5207ABC34,0x550768A64addcF30761611273de50F158027B89B, and bc1q0awcrngushpfjxvrn8aapdjv9vf0pgglxevzay.

42. Plaintiff Samantha Kauk Vincent is a resident of Rosharon, Brazoria County, Texas. The fraudulent investment scheme targeting her operated through a compromised Facebook account, resulting in losses of $40,150.00 through documented cryptocurrency transactions between January 4, 2024, and October 29, 2024. The scheme involved transfers of 0.6104352 BTC

through wallet addresses bc1qn3z28krc53dzdhvg2e70eh7sssfrtklyx5n2st, bc1qnn7ne7788r44e00rug9tlzq2crdz0surmy8zgq, bc1qc9nhvwddh8qfmreygfr3j39ejgqw8g7nkpxjg3, and bc1qrapjfrsp3nw5215wjyq4vczvnm9gcfs7xv4s63.

43. Plaintiff Alexandra Murrietta is a resident of Fresno, Fresno County, California. The fraudulent investment scheme targeting her operated through the defiei.com platform, resulting in losses of $126,707.48 through documented cryptocurrency transactions between October 16, 2024, and November 7, 2024. The scheme involved transfers of 45.91642795 ETH through wallet addresses 0xc1576C6d19e7dab65D1be4E2bB75772AAC82d6f5 and 0x420EF2A405A21Ac4605328244E43a1a45f79576.

44. Plaintiff Prashant "Shawn" Katyal is a resident of Austin, Travis County, Texas. The fraudulent investment scheme targeting him operated through the travelvrbo-chn.com and travelvrbo-lxu.com platforms, resulting in losses of $254,159.73 through documented cryptocurrency transactions between February 22, 2024, and April 17, 2024. The scheme involved transfers of 82.21957286 ETH and 967.54 USDT through multiple wallet addresses, including0x1fea2B30967563a3457e2c8c8532a3989d08C611, 0x58501D01d30333d65a2Ec57D2a396524ff3240aF, and 0x07EC9f1edCd26675993510889Bd64ba62Ce41426.

45. Plaintiff Stanislav Tsoy is a resident of Magnolia, Montgomery County, Texas. The fraudulent investment scheme targeting him operated through the Magic Compass platform (magiccompassltd.cc), resulting in losses of $291,157.76 through documented cryptocurrency transactions between September 24, 2024, and October 25, 2024. The scheme involved transfers of 291,156.32 USDT through wallet address 0x5011ab99100b9bf94dd89a3f708cd2b3fe05e295.

46. Plaintiff Neha Malhotra is a resident of Houston, Harris County, Texas. The fraudulent investment scheme targeting her operated through the SilverLakeVirtual platform and subsequent defi-mining.tech interface, resulting in losses of $26,736.00 through systematic cryptocurrency transfers between July 12, 2024, and October 9, 2024. The scheme involved transfers of 9.789718 ETH through multiple wallet addresses including 0xf305e5310b83b2a46229c85fbc5c33ee4c7db97e.

47. Plaintiff Kyle Adams is a resident of Portsmouth, Virginia. The fraudulent investment scheme targeting him operated through the BTCC-US platform, resulting in losses of $286,600.80 through documented cryptocurrency transactions between September 11, 2024, and October 24, 2024. The scheme involved transfers of 3.89457488 BTC and 11.23 ETH through multiple wallet addresses including bc1q0ld93nxptq7rnrhytn7ljlnyzzzyerytga8je0.

48. Plaintiff Hilario Flores is a resident of Honolulu, Hawaii. The fraudulent investment scheme targeting him operated through the "Trust" application connected to Crypto.com and a fraudulent platform identified as "Ledger X", resulting in losses of $1,374,571.32 through documented cryptocurrency transactions between December 15, 2022, and March 4, 2023. The scheme involved transfers of 1,375,114.08 USDT through multiple wallet addresses including 0xdAC17F958D2ee523a2206206994597C13D831ec7.

49. Plaintiff Lane Garner is a resident of Levelland, Hockley County, Texas. The fraudulent investment schemes targeting him operated through the CXM Direct trading platform and subsequent Jenkins Tech Recovery scam, resulting in combined losses of $479,465.80. Between July 22, 2024, and October 10, 2024, the scheme involved transfers of 182.79 ETH through wallet address 0xF6EaE3f4ACC0754724D6A5b799a4DD84Cede5580 and 1.45 ETH through wallet address 0x68e580046e9030874ED8de952d9EdBa9D30Ab169.

50. Plaintiff Chetan Joshi is a resident of Tempe, Arizona. The fraudulent investment scheme targeting him operated through the app.bmcc88.vip platform, resulting in losses of $41,100.76 through documented cryptocurrency transactions. The scheme involved transfers of approximately 0.43357725 BTC ($40,000.00) and 1,100.44 USDT ($1,100.76) between July 2024 and August 2024 through wallet address 1PW6iD48oVsw8gUxses7u2psefaYeN6YuU.

51. Plaintiff Balakrishna Konduru is a resident of Leander, Williamson County, Texas. The fraudulent investment scheme targeting him operated through a cryptocurrency trading platform after initial contact from Defendant Joan Andrews, resulting in losses of $98,734.08 through documented cryptocurrency transfers between July 7, 2024, and August 13, 2024. The scheme involved transfers of 0.393 BTC through wallet address 3JGgRZNcVbmUkVPtsvMkQCJZNHx41GUbs4.

52. Plaintiff Abhishek Singh is a resident of Odessa, Florida. The fraudulent investment scheme targeting him operated through the CLFCOIN platform, resulting in losses of $117,631.75 through documented cryptocurrency transactions between July 2024 and September 2024. The scheme involved transfers of 1.64 BTC ($95,890) and 21,786 USDT ($21,741.75) through multiple wallet addresses including 16RRqJSvt3JE5U4arUJQsV26H7X49nPC6c.

53. Plaintiff Jose Vasquez is a resident of Laguna Vista, Cameron County, Texas. The fraudulent investment schemes targeting him operated through multiple cryptocurrency platforms including Jenkins Tech Recovery, resulting in losses of $35,777.85 through documented cryptocurrency transactions between June 2024 and October 2024. The scheme involved transfers of 9.789718 ETH through multiple wallet addresses including 0x68e580046e9030874ed8de952d9edba9d30ab169.

54. Plaintiff Bill Young is a resident of Houston, Harris County, Texas. The fraudulent investment scheme targeting him operated through the BitMart.space platform, resulting in verified losses of $180,403.11 through systematic cryptocurrency transfers between September 11, 2024 and October 7, 2024. The scheme involved transfers of 1.09550738 BTC ($68,948) and 33.64802896 ETH plus 21,802.556059 USDC ($111,455.11) sent to wallet bc1qam5g4xqy7yymm7cm4cunkzpp3g67ze3ajujk6c, 33.64802896 ETH sent to wallet 0xa355b5aB3d6B08f197a7bbeC5f168901F2912EcA, and 21,802.556059 USDC sent to wallet 0xF7De5b78F70bfafEfF8C27C192AD5299A39dFCBF.

B. DEFENDANTS

55. Defendant "Lauren Christie" communicates through WhatsApp (+1-503-421-5594, +1-503-752-7094, +1-404-493-5667, +1-503-490-6297) and Telegram (@ASO1268) and operates through the MalCoin trading platform and FB Financial Institute. She controls wallet addresses39ugYdrSAZgiTYASntVqcTkkVkcrSmZszw, 3JvwosoWJUaCQH5M7YiJzAwn93BtRs6QNZ, and 1M8QjVDyhHzrVXonTQzg75gyu4ycnMmYj2, which received cryptocurrency valued at $310,133.22 from Plaintiff Dr. Rispba McCray-Garrison between July 9, 2024, and October 8, 2024.

56. Defendant "Professor Wilbur Clark" communicates through WhatsApp (+1-404-441-9801, +1-503-998-5264, +1-503-449-5634) and operates through the FB Financial Institute. He controls wallet addresses associated with the MalCoin trading platform, which received cryptocurrency from Plaintiff Dr. Rispba McCray-Garrison through coordination with "Lauren Christie.

57. Defendant "Tom Sheldon Haley" communicates through WhatsApp (+1-470-697-1565) and operates through the tradepropel.com platform. He controls wallet addresses 1QCPughtAraSkNdseEBvv6wbjFiU5j9Agg,14QhT2sgAF7bRS944Ap2JuuvtRyMkvvXNa, bc1qv3382swzls05cemkxjh3djfmzgsxmd6nne8y4c, and bc1qranxtfenl06rwmjh0zggr30aqn4pnlnyqkarzh, which received 10.77975 BTC ($698,919) from Plaintiff Stacey Brown between March 30, 2024, and June 6, 2024.

58. Defendant "Jingyi Li" communicates through WhatsApp and operates through the Decode Global platform. He controls wallet addresses 0xA84e06AFa8a7792365927d632f7CE5161d0CaA26,0x069B6C43AF503777E5ae7Fca07F65dD7426296C1, and 0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89, which received cryptocurrency valued at $73,845.49 from Plaintiff Wen Cao between June 21, 2024, and September 9, 2024.

59. Defendant "Jingqiu Ning" communicates through WhatsApp (+1-973-282-8222) and operates through the GroveXCO platform (grovexcos.com). She controls wallet address 0x90027E195b77C7d4EF2f6DB7cD85E3E9107716aA, which received cryptocurrency valued at $53,105.78 from Plaintiff Wen Cao between September 18, 2024, and September 27, 2024

60. Defendant "Ksenia" communicates through WhatsApp (+1-213-661-3580) and operates through the Chartranks.com platform (Customer Service ID: Chaptr-cs07). She controls wallet addresses 0xf7473f6a31d750b8edb171091cda747e0b4f5b3d, 0x7bE7E8992501549Ded06fAd4cb697C7582548831,0x5e3035cd4ce7f5bf892a639831dca6bf3bd7a95f, and TFjwz6rUKa2aVAATPTtB5aAUSG4uPP9x1eV, which received cryptocurrency valued at $59,000 from Plaintiff Jesseca Dickerson between July 29, 2024, and October 11, 2024.

61. Defendant "Nina/Annie" communicates through WhatsApp (+1-917-420-3859) and operates through the unions.top platform. She controls wallet addresses 0x36753759cc50a0a62cefe8dc17b7fdc2a791b8f5,0x99576adba07f66961e4788448b0ce4ad77ed1f6d,and 0x04fd6aa4eb8a03c019e5d4e7d5a1fdbcb750052f, which received 56.963512 ETH ($152,481.00) from Plaintiff Naresh Gorantla between July 2, 2024, and November 21, 2024.

62. Defendant "Zoe" communicates through WhatsApp (+1-332-272-4264, +1-626-630-9256) and operates through the unions.top platform. She controls wallet addresses associated with the unions.top platform, which received cryptocurrency valued at $197,432.67 from Plaintiff Naresh Gorantla between July 11, 2024, and July 24, 2024.

63. Defendant "Grace Lin" communicates through Facebook Messenger and operates through the Nexus Nebula Exchange (nebulairs.net) platform. She controls wallet address 0x8EDA58986D1CC51cc77119f9ad6095c2c15539Ca, which received 663,600 USDT and 15.46 ETH ($712,492.93) from Plaintiff Matthew Hizon between May 17, 2024, and October 11, 2024.

64. Defendant "Unknown Impersonator" (using the name of Don Landrus) communicates through Facebook Messenger and operates through the globalcryptofield.com platform. The impersonator controls wallet addresses bc1q0tx9pmhxdytw5dkcy9d7tc5sv82z4twg74hsvu,bc1qexavxlt2weweuq0scwdu5mdpfxdls8frz7heqv, and bc1qvsxkwhh8wz6c0l82y9jptgj8q4mlxn7rvn9nu3, which received 1.21439 BTC ($83,362.00) from Plaintiff Jordan Partier between May 7, 2024, and October 8, 2024.

65. Defendant "Sam Bennett" communicates through Telegram and operates through the globalcryptofield.com platform. He controls wallet addresses associated with the globalcryptofield.com platform, which received cryptocurrency from Plaintiff Jordan Partier through coordination with "Don Landrus."

66. Defendant "Caroline Martin" communicates through WhatsApp (+1-458-250-9980) and operates through the defistart.top platform. She controls wallet address 0x3Ab11B37773A9d76277024C909B7c124fCCd4371, which received 39.52354 ETH ($98,238.00) from Plaintiff Greg Richards between September 4, 2024, and October 11, 2024.

67. Defendant "Mark/Professor" communicates through WhatsApp (+1-740-491-1166) and Telegram (@Mark44777) and operates through the Vebson Trading Platform (m.vebson.trade). He controls wallet addresses 1CyUJzpgFztJzMPmZqNwyeRzC8WDjok3i, 388TgpKxQxr7HPrAGGcyuGAv7UhkKfunzk, and 0xbc09a9dacc301c7b4ba6620e87916bb69017dfba, which received 4.19195816 BTC and 2.88848355 ETH ($204,186.70) from Plaintiff Reitta Seidel between August 8, 2024, and October 17, 2024.

68. Defendant "Assistant Erin" communicates through WhatsApp (+1-234-301-8088) and operates through the Vebson Trading Platform (m.vebson.trade). She controls wallet addresses associated with the Vebson Trading Platform, which received cryptocurrency from Plaintiff Reitta Seidel through coordination with "Mark/Professor."

69. Defendant "Emily Trent" communicates through WhatsApp and operates through the millioneurolistings.agency platform. She controls wallet addresses 0x9879Fb41c9E0C9eF8adB878a9fE655C5207ABC34,0x550768A64addcF30761611273de50F158027B89B,bc1q0awcrngushpfjxvrn8aapdjv9vf0pgglxevzay, and additional associated addresses, which received 81.53626 ETH and 0.73926902 BTC ($250,000) from Plaintiff Maria Sisson between July 21, 2024, and October 2, 2024.

70. Defendant "David" communicates through WhatsApp and operates through the millioneurolistings.agency platform. He controls wallet addresses associated with the

millioneurolistings.agency platform, which received cryptocurrency from Plaintiff Maria Sisson through coordination with "Emily Trent."

71. Defendant "Shelby Petty" (impersonator) communicates through WhatsApp (+44-7449-0075) and operates through a compromised Facebook account. She controls wallet addressesbc1qn3z28krc53dzdhvg2e70eh7sssfrtklyx5n2st, bc1qnn7ne7788r44e00rug9tlzq2crdz0surmy8zgq,bc1qc9nhvwddh8qfmreygfr3j39ejgqw8g7nkpxjg3,and bc1qrapjfrsp3nw5215wjyq4vczvnm9gcfs7xv4s63, which received 0.6104352 BTC ($40,150.00) from Plaintiff Samantha Kauk Vincent between January 4, 2024, and October 29, 2024.

72. Defendant "Dianne Hollister" communicates through email (dianneholliste r0@gmail.com) and operates as a claimed CEO of an unnamed investment company. She controls wallet addresses associated with wallet addresses used by "Shelby Petty" impersonator, which received cryptocurrency from Plaintiff Samantha Kauk Vincent through coordination with the "Shelby Petty" impersonator.

73. Defendant "Marco Rossi" communicates through WhatsApp and operates through the defiei.com platform. He controls wallet addresses 0xc1576C6d19e7dab65D1be4E2bB75772AAC82d6f5 and 0x420EF2A405A21Ac4605328244E43a1a45f79576, which received 45.91642795 ETH ($119,184.22) from Plaintiff Alexandra Murrietta between October 16, 2024, and November 7, 2024.

74. Defendant "Emily" communicates through WhatsApp (+1-646-296-7124) and operates through the travelvrbo-chn.com and travelvrbo-lxu.com platforms. She controls wallet addresses0x1fea2B30967563a3457e2c8c8532a3989d08C611,

0x58501D01d30333d65a2Ec57D2a396524ff3240aF,

0x8F1C4F3198D26B34e62570Fa082DF13D33447309,

0x6da48556fFD546358Aa4A9f00255c2aB062fDc20,

0x2143B109675191cD39BcA2F1e6F41Ca9b1F77808,

0xb43ad532C25f0974FB7D905cad8a1D4dB1eB98d5,

0x07EC9f1edCd26675993510889Bd64ba62Ce41426,and

0x42199dDb2a0B25ceC955324033db2032456C3957, which received 82.21957286 ETH and 967.54 USDT ($254,159.73) from Plaintiff Prashant Katyal between February 22, 2024, and April 17, 2024.

75. Defendant "David" communicates through WhatsApp (+1-778-595-0741) and operates through the travelvrbo-chn.com and travelvrbo-lxu.com platforms. He controls wallet addresses associated with the travelvrbo-chn.com and travelvrbo-lxu.com platforms, which received cryptocurrency from Plaintiff Prashant Katyal through coordination with "Emily."

76. Defendant ZHIDE CO LIMITED accepts wire transfers through Standard Chartered Bank Hong Kong (Account: 40711487154) and is located at UNIT 1406B, 14/F, THE BELGIAN BANK BUILDING, NOS.721-725 NATHAN ROAD, KL. This company received $152,432.67 in wire transfers from Plaintiff Naresh Gorantla between July 11, 2024, and July 18, 2024.

77. Defendant HS TRADE HONG KONG CO., LTD accepts wire transfers through Bank of Communications Hong Kong (Account: 382561107723101) and is located at 2-14 Tai Fung Street, Yuen Long District, Hong Kong. This company received $45,000 in wire transfers from Plaintiff Naresh Gorantla on July 24, 2024.

78. Defendants "SilverLakeVirtual" and "AI Mining" operate fraudulent cryptocurrency trading platforms at silverlakevirtual.com and defi-mining.tech respectively. Through these platforms, they orchestrated the systematic theft of cryptocurrency assets from Plaintiff Malhotra between July 12, 2024, and October 9, 2024. SilverLakeVirtual initially presented itself as a legitimate cryptocurrency trading platform, displaying artificial profits before freezing funds and demanding access fees. After payment of these fees, funds were transferred to AI Mining's defi-mining.tech platform, where they were falsely shown as "pledged" and subject to additional fee requirements. Through these deceptive practices and technical manipulation, these defendants extracted a total of 9.789718 ETH ($26,736.00) from Plaintiff Malhotra through multiple wallet addresses including 0xf305e5310b83b2a46229c85fbc5c33ee4c7db97e.

79. Defendant 'Joan Andrews' communicates through WhatsApp number +1 774 703 5065 and initially contacted Plaintiff Konduru on July 7, 2024. She built trust through seemingly legitimate stock recommendations before directing Plaintiff Konduru to a fraudulent cryptocurrency trading platform. Through systematic manipulation and social engineering tactics, she orchestrated the theft of $98,734.08 through a combination of wire transfers and cryptocurrency transactions, including a $75,000.00 wire transfer to Rcbehind Screen Inc (Account #202431530635 at Choice Financial Group) and cryptocurrency transfers totaling 0.393 BTC ($23,734.08) through wallet address 3JGgRZNcVbmUkVPtsvMkQCJZNHx41GUbs4.

80. Defendant Rcbehind Screen Inc. maintains bank account #202431530635 at Choice Financial Group (routing #091311229) and operates from a listed address at 1100W Slauson Ave, Los Angeles, CA 90044. It processes fraudulent wire transfers and cryptocurrency transactions on behalf of Gold Miner Finance Ltd.

81. Defendant Lightweight Hifier Inc. operates from a listed address at 523 West 6th Street, Los Angeles, CA 90013 and processes fraudulent wire transfers through bank account #202401304259 at Choice Financial Group. It acts as a secondary fund collection entity for the fraudulent scheme.

82. Defendant Commerce Blaze Inc. operates from a listed address at 815 Cheyenne Meadows Rd, Colorado Springs, CO 80906 and processes fraudulent wire transfers through bank account #202413620308 at Choice Financial Group. It acts as an additional fund collection entity for the fraudulent scheme.

83. Defendant "Jenny Kowalska" communicates through WhatsApp number +1-332-248-3624 and operates through the BTCC-US platform (btcc-us.com). She controls multiple cryptocurrency wallets including:

bc1q0ld93nxptq7rnrhytn7ljlnyzzzyerytga8je0 (1.47915488 BTC)

1BsVriDePL12XDNTFQ2sfDkngEECb6eoBw (0.96166975 BTC)

1J777EfJsrHeunP4hZUSHH3CoTS79gKsSs (0.85129864 BTC)

1QBhNXirisSYhV6LV1hnyzbu3RZ13Pj75S (0.60246044 BTC)

0x3B18360Fc97AEA4F6D0B45fb4d367beF96ddc8F4 (2.01579524 ETH)

0x7Abaa432f60132A615404DBDD18501C13DcdD1BA (9.20646893 ETH) Through these wallets and the BTCC-US platform, she defrauded Plaintiff Adams of $286,600.80.

84. Defendant "Albee Jiang" communicates through the Line messaging application and operates through the "Ledger X" platform. She controls multiple cryptocurrency wallets receiving transfers of 1,375,114.08 USDT from Plaintiff Flores, including:

0xdAC17F958D2ee523a2206206994597C13D831ec7

0x7510Ba3A0CaB2d07b8563Be13cEd76ceF1dE71e0

0x6D51B8579ED72ef991c2CaCF886dc635693351bE

85. Defendant "Martina" communicates through WhatsApp and operates through the CXM Direct platform (cxmdiolkj.com). She controls wallet address 0xF6EaE3f4ACC0754724D6A5b799a4DD84Cede5580, which received 182.79 ETH from Plaintiff Garner, and directs victims to the fraudulent Jenkins Tech Recovery platform.

86. Defendant "Lisa Davis" communicates through WhatsApp and operates as an administrator of the "IPA Community" through the CLFCOIN platform. Along with "Professor John," she orchestrated the fraud scheme targeting Plaintiff Singh.

87. Defendant "Professor John" operates as the claimed leader of the "IPA Community" through the CLFCOIN platform. He controls multiple wallet addresses including:

16RRqJSvt3JE5U4arUJQsV26H7X49nPC6c

17p98H9RgqEJDayBU2xFw6gcvf1sKmVB8P

1FnCpyv8jgCaEhtLkZe7eemHuFd17JT64e Through these wallets and the CLFCOIN platform, he defrauded Plaintiff Singh of $125,287.00.

88. Defendant "Ella" / "LI XIN YUE" communicates through Instagram (username: glamgoddesscara) and WhatsApp numbers +1-312-536-3950 and +1-415-795-7328. She operates through the Magic Compass platform (magiccompassltd.cc) and controls wallet address 0x5011ab99100b9bf94dd89a3f708cd2b3fe05e295, which received 291,156.32 USDT from Plaintiff Tsoy.

89. Defendants "Rodney" and "Kayla" operate through the app.bmcc88.vip platform and control wallet address 1PW6iD48oVsw8gUxses7u2psefaYeN6YuU, through which they received 0.43 BTC and 2.41 ETH from Plaintiff Joshi.

90. Defendant "Mark" communicates through WhatsApp number +1-740-491-1166 and operates through the Vebson Trading Platform. He controls multiple wallet addresses including: 1CyUJzpgFztJzMPmZqNwyeRzC8WDjok3i (2.42891511 BTC),

388TgpKxQxr7HPrAGGcyuGAv7UhkKfunzk (0.72581884 BTC). Through these wallets and the Vebson Trading Platform, he defrauded Plaintiff Young.

91. Defendant "Erin" communicates through WhatsApp number +1-234-301-8088 and operates in conjunction with "Mark" through the Vebson Trading Platform to defraud Plaintiff Young. She assists in operating the platform interface and coordinating withdrawal prevention.

92. Defendants John Does 1-10 and Jane Does 1-10 represent additional perpetrators whose identities remain unknown but who participated in the fraudulent schemes targeting Plaintiffs through the identified trading platforms and cryptocurrency wallets. These defendants controlled additional wallet addresses, operated platform infrastructure, and coordinated the systematic theft of Plaintiffs' cryptocurrency assets.

93. Due to the defendants' use of fictitious identities, encrypted messaging platforms, and fraudulent business entities, traditional service methods are unavailable or would be ineffective. Pursuant to Rule 106, Plaintiffs seek judicial approval for alternative service methods reasonably calculated to provide actual notice, including: (a) Airdropping a special purpose token to the defendants' cryptocurrency wallets; (b) Notification through the cryptocurrency exchanges where defendants' wallets are held; (c) Messages to defendants' known WhatsApp numbers, social media accounts, and platform profiles; and (d) Blockchain transaction metadata containing service information.

94. This comprehensive approach to service is reasonably calculated to provide actual notice to Defendants while preserving Plaintiffs' ability to recover their stolen assets through the requested emergency relief.

95. Defendant "Richard Bill" communicates through WhatsApp (+1-404-319-9709) and operates as a supporting operator within the FB Financial Institute and MalCoin platform scheme. He participated in group communications and reinforced investment advice provided by "Lauren Christie" and "Professor Wilbur Clark," contributing to the coordinated deception of Plaintiff Dr. McCray-Garrison.

96. Defendant "James Wilson" communicates through WhatsApp (+1-404-449-5999) and operates as a supporting operator within the FB Financial Institute and MalCoin platform scheme. He participated in group communications and reinforced investment advice provided by other defendants, contributing to the coordinated deception of Plaintiff Dr. McCray-Garrison.

97. Defendant "Malcoin008" communicates through Telegram (@Malcoin008) and operates as a platform representative for the MalCoin trading platform. This defendant provided technical support and assisted in facilitating cryptocurrency transfers, contributing to the fraudulent scheme targeting Plaintiff Dr. McCray-Garrison.

98. Defendant "Crypto Merchant" communicates through Telegram (@CryptoMerchant009) and operates as the DEM C2C Customer Service representative for the MalCoin platform. This defendant managed the fraudulent "loan" system that was used to extract additional funds from Plaintiff Dr. McCray-Garrison.

99. Defendant "Points Redeemer" communicates through Telegram (@ZMQ112233) and operates as part of the MalCoin platform scheme. This defendant managed the fraudulent

points and rewards system designed to create an illusion of legitimacy and financial returns within the platform targeting Plaintiff Dr. McCray-Garrison.

100. Defendant FB Financial Institute operates through the website fortune-build.com and maintains WhatsApp Groups including "FB Finance Institute B5" and "AI4.0 pre-sale group 1." This entity functions as a purported investment education organization providing training and access to investment opportunities, but in fact serves as a front for cryptocurrency fraud operations targeting Plaintiff Dr. McCray-Garrison and potentially other victims.

101. Defendant MalCoin Trading Platform operates through the websites globalmalcoin.com, h5.malcoin.top, and h5.globalmalcoin.com, and maintains the Telegram Channel https://t.me/+zDaTbxf7hXwwZmY8. This entity functions as a fraudulent trading platform displaying artificial profits and implementing systematic barriers to fund withdrawal, serving as the primary technical infrastructure for the scheme targeting Plaintiff Dr. McCray-Garrison.

102. Defendant "Luna Lee" communicates through WhatsApp +1-628-629-5774 and operates through multiple cryptocurrency platforms including Jenkins Tech Recovery. She coordinates with other defendants to target victims seeking to recover funds lost in previous scams, including Plaintiff Vasquez.

103. Defendant "Henry Rogan" communicates through WhatsApp +1-973-809-3948 and operates through multiple cryptocurrency platforms including Jenkins Tech Recovery. He coordinates with other defendants to defraud victims, including processing recovery transactions for Plaintiff Vasquez.

V. CAUSES OF ACTION

A. FRAUD

104. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

105. Defendants made material false representations to Plaintiffs by: a. Presenting themselves as legitimate investment advisors, trading coaches, or platform representatives with specialized expertise in cryptocurrency and financial markets; b. Claiming to operate legitimate cryptocurrency trading platforms that would generate substantial returns; c. Presenting artificial profits on sophisticated but entirely fraudulent trading platforms; d. Misrepresenting the nature, risks, and liquidity of cryptocurrency investments on their platforms; and e. Falsely guaranteeing the ability to withdraw funds upon request.

106. When making these representations, Defendants knew they were false or made them recklessly as positive assertions without knowledge of their truth.

107. Defendants made these representations with the intent that Plaintiffs would act upon them by transferring cryptocurrency assets to wallet addresses controlled by Defendants.

108. Plaintiffs justifiably relied on Defendants' false representations by transferring cryptocurrency assets worth approximately $5,870,983 to wallet addresses controlled by Defendants.

109. Through their fraudulent schemes, Defendants have wrongfully converted the following assets for each individual client in the amount of:

Risba McCray-Garrison: 11.92995 ETH ($27,557.83); 4.14721114 BTC ($263,790.53)	**Total: $291,348.36**
Steacey Brown: 10.78086 BTC	**Total: $698,919**

Wen Cao: 48.188 ETH; 300 USDT	**Total: $73,845.49**
Jesseca Dickerson: 5,754.3489 USDT; 2.33327 ETH; 0.11811376 BTC	**Total: $20,462.54**
Naresh Gorantla: 56.963512 ETH	**Total: $152,481.00**
Matthew Hizon: 663,600 USDT ($663,600); 15.46 ETH ($48,892.93)	**Total: $712,492.93**
Jordan Partier: 1.21439 BTC ($83,362.00); 160.72 USDT ($158.24)	**Total: $83,520.24**
Greg Richards: 39.52354 ETH ($98,238.00)	**Net Loss: $97,451.00 (Successful partial recovery)**
Reitta Seidel: 4.19195816 BTC (198,236.70); 2.88848355 ETH ($5,950.00)	**Total: $204,186.70**
Maria Sisson: 81.53626 ETH ($221,263.15); 0.73926902 BTC ($44,340.00)	**Total: $265,603.15**
Samantha Kauk Vincent: 0.6104352 BTC ($40,150.00)	**Total: $40,150.00**
Alexandra Murrietta: 45.91642795 ETH ($119,184.22)	**Total: $119,184.22**
Prashan Katyal: 82.21957286 ETH ($253,192.19); 967.54 USDT ($967.54)	**Total: $254,159.73**
Stanislav Tsoy: 291,156.32 USDT ($291,157.76)	**Total: $291,157.76**
Neha Malhotra: 9.789718 ETH ($26,736.00)	**Total: $26,736.00**
Kyle Adams: 3.89457488 BTC ($258,350.00); 11.23 ETH ($28,250.80)	**Total: $286,600.80**
Hilario Flores: 1,375,114.08 USDT	**Total: $1,374,571.32**
Lane Garner (CXM Direct): 182.79 ETH ($474,723.09) Lane Garner (Jenkins Tech Recovery): 1.45 ETH ($4,980.15)	**Total: $184.24 ETH ($479,465.80)**

Chetan Joshi: 0.43357725 BTC ($40,000.00) and 1,100.44 USDT ($41,100.76)	**Total: $41,100.76**
Balakrishna Konduru: 0.393 BTC ($23,734.08)	**Total: $23,734.08**
Abhishek Singh: 1.64 BTC ($95,890**)** and 21,786 USDT ($21,741.75)	**Total: $117,631.75**
Jose Vasquez: 10.35968 ETH ($25,777.85); 0.64700748 BTC ($10,000)	**Total: $35,777.85**
Bill Young: 33.64802896 ETH + 21,802.556059 USDC ($111,455.11); 1.09550738 BTC ($68,948)	**Total: $180,403.11**
Grand Total Amount:	**$5,870,983.00**

This conduct constitutes wrongful conversion of the Plaintiffs' specifically identifiable assets.

B. CONVERSION

110. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

111. Plaintiffs owned or had legal possession of cryptocurrency assets including Bitcoin (BTC), Ethereum (ETH), Tether (USDT), and other digital assets with a total value of approximately $5,870,983.59.

112. Defendants wrongfully exercised dominion and control over Plaintiffs' cryptocurrency assets in a manner inconsistent with Plaintiffs' ownership rights when they: a. Induced Plaintiffs to transfer cryptocurrency to wallet addresses controlled by Defendants; b. Prevented Plaintiffs from withdrawing funds from fraudulent trading platforms; c. Implemented artificial technical barriers to fund withdrawal; d. Demanded additional payments as a condition for withdrawal; and e. Retained control over Plaintiffs' assets without authorization.

113. Defendants' exercise of dominion and control over Plaintiffs' cryptocurrency assets constituted a clear repudiation of Plaintiffs' rights to those assets.

114. As a direct and proximate result of Defendants' conversion, Plaintiffs have suffered actual damages in an amount to be determined at trial, but not less than $5,870,983.

114. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

115. Defendants have received money belonging to Plaintiffs in the form of cryptocurrency assets valued at approximately $5,870,983.

116. Defendants hold these funds in identifiable cryptocurrency wallets and exchange accounts that can be traced through blockchain analysis.

117. Defendants in equity and good conscience should not be permitted to retain these funds as they were obtained through fraud and deception.

118. Plaintiffs seek restitution of all cryptocurrency assets or their equivalent value that Defendants received from Plaintiffs.

C. VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

119. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

120. The Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Texas Business & Commerce Code § 17.41 et seq., prohibits false, misleading, and deceptive business practices.

121. Plaintiffs are "consumers" as defined by the DTPA because they sought to acquire goods or services by purchase or lease.

122. Defendants engaged in false, misleading, and deceptive acts or practices in violation of the DTPA by: a. Representing that their investment platforms and services had characteristics, benefits, or qualities that they did not have; b. Representing that their investment platforms and services were of a particular standard or quality when they were of another; c. Advertising their investment platforms and services with the intent not to sell them as advertised; d. Representing that an agreement conferred rights, remedies, or obligations that it did not have; and e. Failing to disclose information about their investment platforms and services that was known at the time of the transaction with the intent to induce Plaintiffs into transactions they would not have entered had the information been disclosed.

123. Defendants' actions were committed knowingly and intentionally, as evidenced by the systematic nature of their scheme and the sophisticated technical infrastructure deployed to execute it.

124. As a direct and proximate cause of Defendants' violations of the DTPA, Plaintiffs have suffered economic damages for which they seek recovery.

125. Pursuant to Texas Business & Commerce Code § 17.50(b), Plaintiffs seek economic damages, treble damages for Defendants' knowing violations, court costs, and reasonable attorney's fees.

D. CIVIL CONSPIRACY & TEXAS ORGANIZED CRIME STATUTE (TEXAS RICO)

130. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

131. Defendants were members of a combination of two or more persons.

132. The object of the combination was to accomplish an unlawful purpose or a lawful purpose by unlawful means, specifically to defraud Plaintiffs of their cryptocurrency assets through coordinated deception.

133. The members had a meeting of the minds on the object or course of action, as evidenced by:

- Defendants used common wallet addresses across multiple Plaintiffs, reinforcing their collective involvement in the scheme.
- The same fraudulent narratives were repeatedly used to deceive different Plaintiffs, indicating coordination and premeditation and psychological manipulation.
- Multiple transactions executed within minutes of each other, funneling funds into centralized exchange accounts controlled by Defendants.
- Defendants demonstrated a shared strategy for preventing withdrawals and misleading victims about their financial status.
- The similarity in operational methods across multiple fraudulent platforms.
- The consistent pattern of social engineering, trust building, investment escalation. and withdrawal prevention.
- The sophisticated technical infrastructure spanning multiple platforms.
- The coordinated fund movement patterns across wallet addresses and cryptocurrency exchanges.

134. One or more unlawful, overt acts were committed to further the object or course of action, including fraudulent misrepresentations, conversion of cryptocurrency assets, and technical manipulation of withdrawal mechanisms. These constitute civil conspiracy and violation of the Texas Organized Crime Statute under Chapter 71.02 of the Texas Penal Code.

135. Plaintiffs suffered injury as a proximate result of Defendants' wrongful acts, specifically the loss of cryptocurrency assets valued at approximately $5,870,983.

E. REQUEST FOR INJUNCTIVE RELIEF [1]

140. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

141. Plaintiffs have a probable right to recovery based on the substantial evidence of Defendants' fraud and unauthorized control over Plaintiffs' cryptocurrency assets.

142. Plaintiffs face probable, imminent, and irreparable injury in the absence of temporary injunctive relief because: a. Cryptocurrency transactions are, by their technical nature, irreversible once executed; b. Defendants have demonstrated sophisticated technical capabilities that would allow them to transfer assets to unidentifiable wallets or exchanges beyond the Court's jurisdiction; c. Defendants continue to operate their fraudulent schemes and may dissipate assets at any time; and d. Without preservation of the status quo, Plaintiffs may permanently lose any opportunity for recovery.

143. Plaintiffs lack an adequate remedy at law because monetary damages after the fact would be ineffective if Defendants have already dissipated, transferred, or concealed the cryptocurrency assets at issue.

[1] Plaintiffs were granted the requested injunctive relief on April 4, 2025 (temporary injunction), and September 23, 2025 (permanent injunction). All injunctive relief currently in place should remain in place.

144. The balance of equities favors Plaintiffs because: (a) Freezing identifiable wallet addresses and exchange accounts pending resolution preserves Plaintiffs' ability to recover their rightful property; (b) Defendants have no legitimate interest in retaining fraudulently obtained assets; and (c) Temporary preservation of assets does not prejudice any legitimate defense Defendants may have.

145. Therefore, Plaintiffs seek for the temporary injunction issued on April 4, 2025 or the permanent injunctive relief: (a) Freezing all cryptocurrency wallet addresses identified in Exhibit A; (b) Prohibiting any cryptocurrency exchanges from processing transactions from the wallet addresses identified in Exhibit A; (c) Requiring the preservation of all records relating to the wallet addresses identified in Exhibit A; (d) Requiring the disclosure of any additional wallet addresses or exchange accounts controlled by Defendants; and (e) Prohibiting Defendants from transferring, dissipating, or otherwise disposing of any cryptocurrency assets derived from Plaintiffs.

F. EXEMPLARY DAMAGES

146. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

147. Defendants' conduct, as described above, was fraudulent and malicious as those terms are defined by Texas Civil Practice & Remedies Code § 41.001(7) and § 41.001(11).

148. The fraud perpetrated by Defendants was actual fraud involving dishonesty of purpose, intent to deceive, and a breach of a duty to act in good faith.

149. Defendants acted with actual awareness that their conduct would result in substantial harm to Plaintiffs, as evidenced by their systematic approach to building trust, escalating investments, and implementing technical barriers to withdrawal.

150. Defendants' conduct involved a high degree of culpability, specifically an entire business model built around defrauding victims through sophisticated technological means and psychological manipulation.

151. Due to the fraudulent and malicious nature of Defendants' conduct, Plaintiffs seek exemplary damages as allowed by Texas Civil Practice & Remedies Code § 41.003(a).

G. REQUEST FOR EX PARTE INJUNCTIVE RELIEF[2]

152. Plaintiffs request immediate ex parte injunctive relief to preserve cryptocurrency assets that have been traced to identified wallet addresses and exchanges. The irreversible nature of blockchain transactions creates an urgent need for immediate intervention without notice to Defendants.

153. Cryptocurrency transactions are immutable and pseudonymous by design. Once executed, these transactions cannot be reversed, canceled, or recalled by any party, bank, government, or regulatory authority. Unlike traditional financial systems where fraudulent transfers may be frozen or reversed, blockchain technology makes unauthorized transactions permanent. This technological reality necessitates emergency injunctive relief to prevent further dissipation of assets.

154. Blockchain analysis has confirmed that Defendants' fraudulently obtained cryptocurrency assets currently reside in identifiable wallet addresses and on major cryptocurrency exchanges that may be subject to this Court's jurisdiction. As documented in the Dr. McCray-Garrison case, forensic blockchain analysis has successfully traced stolen funds to specific exchanges including Binance (42%), OKX (23%), Huobi (15%), Gate.io (8%), Bybit (5%), and other exchanges (7%) through 59 related cryptocurrency addresses with 1,105 documented

[2] Plaintiffs were granted the requested ex parte injunctive relief. Plaintiffs pray that all injunctive relief currently in place remain in place.

transfers to cryptocurrency exchanges. Without immediate ex parte relief freezing these assets, Defendants can instantaneously transfer these assets to new unidentified wallets, overseas exchanges, privacy-enhancing protocols, or convert them to other forms of cryptocurrency, effectively placing them beyond the reach of this Court.

155. Defendants have demonstrated sophisticated technical capabilities in cryptocurrency operations, including:

- Defendants have demonstrated sophisticated technical capabilities in cryptocurrency operations
- Utilization of multiple cryptocurrency exchanges
- Cross-chain transactions between different blockchain networks
- Implementation of layering techniques to obscure transaction sources

The Dr. McCray-Garrison case provides specific evidence of these sophisticated capabilities, documenting how perpetrators moved stolen assets through 59 related cryptocurrency addresses with 1,105 documented transfers to cryptocurrency exchanges

156. These technical capabilities, combined with the instant and irreversible nature of cryptocurrency transactions, create an exceptional circumstance justifying ex parte relief. Providing notice to Defendants before freezing the identified assets would effectively enable the complete dissipation of these assets, rendering any subsequent judgment unenforceable.

157. The traced cryptocurrency has been positively identified through blockchain forensic analysis as directly connected to the fraudulent schemes perpetrated against Plaintiffs. Each transaction from Plaintiffs to Defendants has been verified through exchange records, blockchain analysis, and transaction hash identification. This technical verification provides substantial evidence supporting Plaintiffs' ownership claims to these assets.

158. Due to the technical nature of cryptocurrency operations, the Court's intervention must include specific technical directives to cryptocurrency exchanges and wallet service providers to ensure proper execution of asset preservation. These directives must address the unique technical requirements of blockchain-based asset freezing to prevent asset dissipation through technological means.

159. The overwhelming evidence of fraud combined with the technical capability for immediate, irreversible asset dissipation constitutes an emergency situation requiring immediate ex parte relief to preserve the status quo until a full hearing can be conducted.

160. Plaintiffs therefore request immediate ex parte temporary restraining order freezing all cryptocurrency assets in the wallet addresses identified in Exhibit A, as well as any assets traceable to these addresses now held at cryptocurrency exchanges or other financial institutions, to preserve these assets pending further proceedings.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that:

a. All injunctive relief currently in place shall remain in place;

b. The Court award actual damages to the Plaintiffs according to the proof presented at trial or default judgment hearing;

c. The Court award exemplary damages to the Plaintiffs pursuant to Tex. Civ. Prac. & Rem. Code § 41.003 due to Defendants' fraud and malice according to proof presented at trial or default judgment hearing;

d. The Court award pre-judgment and post-judgment interest to the Plaintiffs at the maximum rate allowed by law;[3]

[3] All pre-judgment and post-judgment interest at the maximum rate allowed by law which has previously been granted, if any, shall remain.

e. The Court award Plaintiffs their reasonable and necessary attorneys' fees and costs of court[4]; and

f. The Court grant Plaintiffs such other and further relief to which they may be justly entitled.

Respectfully submitted,

Johnson & Associates
Attorneys at Law, PLLC

By: /s/ *Christopher L. Johnson*

Christopher L. Johnson
Texas State Bar No. 24069999
chris@Johnson-Attorneys.com
Richard L. Gorman
Texas State Bar No. 00784155
richard@johnson-attorneys.com
303 East Main Street, Suite 100
League City, Texas 77573
Main: (281) 895-2410
Fax: (409) 263-1020
Counsel for Plaintiffs

[4] All reasonable and necessary attorneys' fees and costs of court which have previously been granted, if any, shall remain.

Danziger & De Llano, LLP

By: */s/ Paul Danziger*
Paul Danziger
Texas State Bar No. 00788880
paul@dandell.com
Rod De Llano
rod@dandell.com
440 Louisiana Street, Suite 1212
Houston, Texas 77002
Main: (713) 222-9998
Fax: (713) 222-886

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I certify that on this 8th day of December, 2025, a true and correct copy of the foregoing motion was served on the Plaintiff ***via Notice of Electronic Service***.

/s/ Richard L. Gorman