IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

SHAWUTI MAIMAITIYUMAIER, an individual, on behalf of himself and all others similarly situated	)	Case No.: 2025CH05863
Plaintiff,	)	Hon.
v.	)	
JANE DOE a/k/a "Carrie" and JOHN DOES 1-25,	)	
Defendants.	)	

COMPLAINT

NOW COMES Plaintiff, Shawuti Maimaitiyumaier ("Plaintiff"), by and through his attorneys, ESBROOK P.C., and for his Complaint against Defendants John Does 1-25 ("Defendants"), alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of himself and all others similarly situated to recover funds stolen from them through an insidious scheme known as "pig butchering."

2. This class action arises from a sophisticated online theft scheme commonly referred to as "pig butchering," in which scammers cultivate trust with unsuspecting victims, entice them to deposit funds in fraudulent cryptocurrency platforms, and ultimately abscond with the victims' hard-earned money and life savings. The scam is methodical, psychologically manipulative, and technologically deceptive. Plaintiff brings this action on behalf of himself and all other similarly situated victims.

3. Over the course of November and December 2024, Plaintiff was defrauded of approximately $19,018.05 by unidentified Defendants who engaged in a targeted campaign of

deception and theft. The scope of the perpetrated "pig butchering" scam is vast and the harm it caused is deeply personal and financially devastating.

4. The term "pig butchering" refers to the scammers' strategy of "fattening up" the victim—coaxing increasingly large money deposits—before abruptly cutting off all communication and stealing the victims' funds. These scams often blend the cryptocurrency fraud with emotional manipulation. The scammers cultivate trust through friendships, promises of easy work and fast money, or other forms of online social relationships. The scammers prey on human vulnerability while hiding behind layers of digital anonymity.

5. Defendants, whose real identities remain unknown, executed an organized campaign to scam Plaintiff and members of the class. In Plaintiff's case, Defendants first contacted Plaintiff via WhatsApp. The scammers posed as friendly recruiters, offering Plaintiff an easy, remote part-time job. Over the course of November and December 2024, Defendants developed a rapport with Plaintiff, promising him easy work and high commissions for his part-time work.

6. Defendants gained Plaintiff's trust by promising him significant earnings. Plaintiff was to conduct work through what appeared to be a legitimate online cryptocurrency platform – digitalleaderpl.com ("Digital Leader"). Plaintiff was assigned tasks to complete on this fraudulent platform. Plaintiff also had to make Bitcoin ("BTC") deposits on Digital Leader in order to complete these tasks. Once the tasks were completed, Digital Leader showed that Plaintiff made significant commissions.

7. These artificial commissions, combined with ongoing encouragement from Defendants, led Plaintiff to deposit increasingly large sums of BTC into Digital Leader. This platform continued to simulate gains and commissions, reinforcing the illusion that Plaintiff was

indeed doing legitimate work and earning commissions, when in fact Plaintiff's BTCs were being siphoned off to digital wallets controlled by Defendants.

8. When Plaintiff eventually attempted to withdraw a siginificant portion of his purported earnings, he was told he must first pay additional fees because his account on Digital Leader was frozen. These demands were further attempts to extract additional funds from Plaintiff.

9. Despite repeated attempts to withdraw his money, Plaintiff was unable to retrieve any of the deposits or supposed earnings. Eventually, all communication ceased and the fake cryptocurrency work platform became inaccessible. Defendants stole approximately $19,018.05 from Plaintiff. The same pattern of deceit has been reported by numerous victims around the country, indicating that this is not an isolated incident but part of a widespread, coordinated scam.

10. Plaintiff retained a forensic cryptocurrency expert, Inca Coalition ("Inca"), to trace the stolen funds and BTC on the blockchain. Each transaction was tied to a unique hash and tracked across various wallets, showing a consistent laundering pattern. The forensic trail shows that the same or similar individuals, entities, and digital infrastructure have been used to commit this techonogical scam against numerous others.

11. This scheme was intentionally designed to mimic legitimacy, from the user interface of the fake work platform to the scripted responses of the scammers posing as recruiters. The result is widespread financial harm to Plaintiff and others similarly situated.

12. Plaintiff brings this class action pursuant to 735 ILCS 5/2-801 on behalf of all individuals who were similarly scammed. Plaintiff and the members of the Class, as defined further below, were subjected to the same scam tactics, suffered similar harms, and seek similar relief. The class members' claims share common issues of law and fact, including the use of fake work platforms, emotional and psychological manipulation, misrepresentation of earnings and

commissions, the inability to withdraw funds, and the laundering of assets via cryptocurrency wallets. A class action is the most efficient and fair means of adjudicating these claims.

13. This complaint seeks redress for the injuries caused and accountability for the individuals who perpetrated this scam.

THE PARTIES

14. Plaintiff is a molecular technologist working in Chicago, Cook County, Illinois.

15. Defendants are persons of unknown citizenship who perpetrated the wrongdoing alleged herein. Plaintiff will attempt to identify Defendants by name through discovery served on third parties with whom Defendants interacted.

JURISDICTION AND VENUE

16. The Court has personal jurisdiction over Defendants because the claims asserted herein arise in substantial part from Defendants' actions and scheme purposefully directed at Plaintiff in Illinois, and because the effects of Defendants' actions and scheme were felt from within Illinois by Plaintiff as a citizen and resident of Illinois. Jurisdiction, therefore, is properly laid in this Court.

17. Venue is proper in this Court under Section 2-101 of Illinois Code of Civil Procedure because a substantial part of the events giving rise to the claims occurred in Cook County, where Plaintiff works and was primarily targeted by Defendants' scheme. Additionally, certain cryptocurrency transfers described herein occurred within Cook County.

CRYPTOCURRENCY BASICS

18. Virtual currencies, also known as cryptocurrency, are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are

generated and controlled through computer software. BTC and Ethereum ("ETH") are the most well-known virtual currencies in use.

19. Virtual currency is tied to a virtual address. Virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. Like with bank accounts, one cannot send money to a virtual address without knowing the specific string of characters.

20. The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), but analysis of the blockchain can sometimes be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

21. Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address' private key can authorize a transfer of virtual currency from that address to another address. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

22. Blockchain is used by many virtual currencies to publicly record all of their transactions. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

23. Virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

24. Centralized Exchanges are digital platforms that facilitate the buying, selling, and trading of cryptocurrencies through a centralized organization that manages the platform and user funds. These exchnages operate similarly to traditional stock exchanges, acting as intermediariers between buyers and sellers. Examples of well know centralized exchanges include Binance, Coinbase, and Kraken.

25. While centralized cryptocurrency exchanges have enabled broader public access to digital asset markets, their rise has also coincided with the proliferation of fraudulent schemes that exploit consumer trust and the complexity of the blockchain-based transactions.

26. Phony exchanges promising outrageous returns have been established and continue to operate with the sole purpose of conning unsuspecting people out of their hard-earned money and life savings.

OVERVIEW OF THE PIG BUTCHERING EPIDEMIC

27. Plaintiff and the Class had their funds and cryptocurrency stolen as part of elaborate pig butchering scams. Defendants' conduct is not isolated or unique but rather a part of a vast and global network of criminal operations engaged in perpetrating these schemes.

A. How Pig Butchering Works

28. "Pig butchering" is a sophisticated and insidious scheme that involves cultivating a relationship with a targeted individual through deceptive means over time, with the ultimate goal of financial exploitation. Pig butchering victims in the United States have lost billions of dollars

and "pig butchering" schemes have been the subject of state and federal government investigations and prosecution.[1]

29. Scammers typically initiate contact with victims through social media platforms, dating apps, or messaging services like WhatsApp. They pose as friendly or romantic interests, gradually building trust over weeks or months. Once a relationship is established, the scammer introduces the victim to a fraudulent investment opportunity, often involving cryptocurrency. Sometimes scammers pose as job recruiters. The scammers guide the victims to a fake cryptocurrency trading platform.[2]

30. The fraudulent cryptocurrency platforms are designed to appear legitimate, complete with professional-looking websites that include polished interfaces and dashboards that display fictitious returns and trading data. Victims are encouraged to make small initial investments, which seemingly yield significant profits. These apparent gains entice victims to invest larger sums.

31. As the victim continues to invest, the scammer may fabricate reasons to prevent fund withdrawals, such as additional fees for account verification or taxes. These fabrications are designed to prolong the scheme and extract more money from the victim. Eventually, the victim attempts to withdraw funds independently and discovers that the platform does not allow access to their balance or that customer support is non-responsive or non-existent. In some cases, the

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

[2] In 2022, ProPublica published an in-depth investigation of pig butchering, describing how criminal syndicates operate, often by forcing human trafficking victims to perpetrate the schemes against their will. See Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One.* PROPUBLICA, Sept. 19, 2022, https://www.propublica.org/article/whats-a-pig-butchering-scam-hereshow-to-avoid-falling-victim-to-one.

purported platform becomes inactive. At that point, the victim discovers that the investment platform is a sham, resulting in substantial financial loss.

32. The scale of pig butchering scams is staggering. According to the FBI's 2024 Internet Crime Report, Americans lost $9.3 billion to cryptocurrency scams in 2024 alone, with pig butchering being a significant contributor.[3]

33. Victims of pig butchering span all demographics but often include older adults and retirees seeking financial security. The emotional manipulation involved can lead to victims taking out loans and depleting life savings to invest in the fraudulent scheme and trading platforms.

34. Law enforcement agencies, including the FBI, have recognized the severity of pig butchering scams. In response, the FBI launched "Operation Level Up" in early 2024, identifying over 4,300 victims, 76% of whom were unaware they were being scammed at the time of contact.[4]

B. International Criminal Networks Conducting Pig Butchering Scams

35. Pig butchering schemes are frequently orchestrated by transnational criminal organizations based in Southeast Asia, particularly Myanmar, Laos, and Cambodia. These criminal groups operate with high degree of coordination, often using trafficked labor to target victims around the globe, including United States.[5]

36. The international crime syndicates operating these scams include but are not limited to the Chinese 14K Triad and the Karen Border Guard Force. Wan Kuok-Koi a/k/a "Broken Tooth" is a reputed Chinese mafia boss who has been sanctioned by the U.S. Government. He is the former

[3] *See* Federal Bureau of Investigations ("FBI") 2024 Crime Report https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[4] *Id*.
[5] *See* https://www.pbs.org/newshour/show/how-human-trafficking-victims-are-forced-to-run-pig-butchering-investment-scams

head of the Chinese 14K Triad.[6] The 14K Triad is a criminal operation based in Hong Kong with ties to various scam compounds, such as KK Park, an online scam factory on Myanmar's border with Thailand.[7]

37. The Karen Border Guard Force ("KBGF") is a violent militia that controls much of Myanmar's border areas with China, Laos, and Thailand. The KBGF operates in Myanmar's Karen State and is headed by Colonel San Myint a/k/a Saw Chit Thu. The KBGF has overseen the development of numerous illegal casino operations, which are used as pig butchering scam compounds. The KGBF changed its name in 2024 to the Karen National Army ("KNA"). The KBGF/KNA is considered a "major node in a network of cyber scam centers . . . in Southeast Asia in which criminal groups are earning billions of dollars."[8]

38. Within the last year "offshoots of the Southeast Asian activity have emerged in the Middle East, Eastern Europe, Latin America, and West Africa. Many of these expanded operations … evolved in parallel to Chinese Belt and Road Initiative investments, the country's massive international infrastructure and development initiative."[9] The pig butchering epidemic, thus, is no longer contained to Southeast Asia. Rather, it is a global epidemic now.

C. Off-Ramping Stolen Cryptocurrency

39. The ultimate goal of the scammers in pig butchering schemes is to "off-ramp" the stolen cryptocurrency—i.e., to convert it from traceable blockchain assets into fiat currency that can be freely spent or hidden outside the digital ecosystem. This conversion process often involves

[6] *See* https://www.wsj.com/world/china/china-mafia-broken-tooth-wan-kuok-koi-online-fraud-scam-70c09afb
[7] *See* https://www.dw.com/en/china-repatriates-hundreds-of-scam-factory-survivors/a-68408165
[8] *See* https://www.justiceformyanmar.org/stories/the-karen-border-guard-force-karen-national-army-criminal-business-network-exposed
[9] *See* https://www.wired.com/story/pig-butchering-scam-invasion/

layering transactions through multiple wallets, mixing services, or foreign exchanges in order to obscure the origin of the funds. The end result is the placement of illicitly obtained crypto into the traditional financial system, a process functionally and legally akin to money laundering. By distancing the funds from their criminal origins through complex blockchain transactions, the perpetrators aim to make detection and recovery extremely difficult.

40. As part of the laundering process, cyber criminals deploy various techniques such as (1) exchange hopping - using multiple crypto exchanges to transfer funds across different platforms; (2) staggering –structuring transfers in a way that reduces detection risk by dispersing funds across multiple transactions, wallets, or time intervals; and (3) mixing or commingling-blending crypto from multiple sources to obscure the transaction history. Digital banks that offer banking-as-a-service (BaaS) in jurisdictions deficient in their anti-money laundering systems afford criminals the opportunity to "cloak" the stolen crypto by mixing it with legitimate funds.

41. Despite increased awareness and enforcement efforts, pig butchering scams continue to proliferate due to their sophisticated nature and the anonymity afforded by digital platforms and cryptocurrencies. The combination of emotional manipulation and financial deception makes these scams particularly devastating.

DEFENDANTS LURE PLAINTIFF IN

42. In or around November 26, 2024, Plaintiff was contacted via WhatsApp by one of the Defendants identifying herself as "Carrie" who offered Plaintiff a lucrative part-time job opportunity.

43. Carrie claimed to be a trainer and a mentor and introduced Plaintiff to a Digital Leader platform which she represented was a legitimate platform for earning commissions.

44. Relying on Carrie's representations, Plaintiff created an account on the Digital Leader platform with her assistance. Defendants explained that to earn commissions, Plaintiff would need to complete specific tasks or missions on the platform.

45. These tasks or missions involved product reviews. Plaintiff's purported job was to review a batch of products, which included anything from gaming consoles to clothes to shoes. Plaintiff would assign these products a rating between one and five and upon completion of a batch (which usually included 40 some products), Plaintiff would earn a commission. Daily commissions ranged from $60 to $150 and Plaintiff was required to complete two or three tasks per day to get the purported commission payments.

46. Defendants further explained that users were required to deposit BTC into their accounts to unlock batches of products to review, which would then be used to generate commissions upon task completion.

47. Initially, Plaintiff was able to complete tasks and received commissions, which reinforced the appearance of legitimacy of Digital Leader and the purported job opportunity.

48. Plaintiff was encouraged by Defendants to deposit increasingly large amounts of BTC into Digital Leader to unlock higher value products to review and earn more commissions.

49. Plaintiff did indeed make larger deposits. For example, on December 6, 2024, Plaintiff deposited $1,934.34 worth of BTC into the Digital Leader platform. On December 7, 2024, Plaintiff deposited $3,816.28 worth of BTC. Finally, on December 9, 2024, Plaintiff deposited $12,314.80 worth of BTC into the platform. In total, Plaintiff deposited $19,018.05 worth of BTC into the platform.

50. Subsequently, Plaintiff attempted to make a substantial withdrawal of his purported earnings and commissions. At that time, Plaintiff was informed by Defendants that his account

had been frozen. Defendants claimed that to unfreeze the account, Plaintiff needed to continue funding it with additional Bitcoin deposits.

51. Despite Plaintiff's multiple deposits, he was unable to withdraw any funds. Carrie and other Defedants provided various excuses for the delays and continued to pressure Plaintiff into making further deposits under the pretense of completing tasks and earning commissions.

52. This pattern of behavior is consistent with known pig butchering scams, where victims are lured into fraudulent cryptocurrency schemes through the guise of professional relationships, leading to significant financial losses.

53. The Digital Leader platform was a fraudulent operation designed to deceive individuals into depositing cryptocurrency under the false promise of earning commissions through task completion of product reviews.

54. Digital Leader's operators utilized deceptive tactics, including impersonating legitimate job recruiters, to exploit Plaintiff and other victims' trust and to extract funds.

55. Between November 26 and December 9, 2024, Plaintiff transferred a total of $19,018.05 across 8 transactions to Digital Leader, which was a fraudulent platform controlled by Defendants. In reality, these BTC deposits went into wallets controlled by Defendants. The table below details all transactions made by Plaintiff:

No.	Date/Time	From Exchnage	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
1.	11/26/2024 23:57	CashApp	bc1qxru 4d77r0v mv8 66ltcp65 3sl0e3cl 5vq 0nzpue	bc1q4ufq euhelstl9j ymcg3gy 3k8df904 g8cdnghp w	BTC	0.00107585	$100.07

No.	Date/Time	From Exchnage	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
2.	1/27/2024 22:26	CashApp	bc1qt9a3hs8kcl3z2m8vxlveu7l8eskvtnsuf0a80v	bc1q4ufqeuhelstl9jymcg3gy3k8df904g8cdnghpw	BTC	0.0012386	$113.83
3.	11/28/2024 21:44	CashApp	bc1qys9dye8vxxtq2u942j5u0885tq555sh5q3rtcf	bc1q4ufqeuhelstl9jymcg3gy3k8df904g8cdnghpw	BTC	0.00150417	$144.34
4.	11/28/2024 22:19	CashApp	bc1qsvd6xp6kjxxg94uug2n7yu9xfk467gp563rnxq	bc1q4ufqeuhelstl9jymcg3gy3k8df904g8cdnghpw	BTC	0.00175811	$167.13
5.	12/05/2024 22:10	Strike	bc1q72edfas0c38gxjskn4j97t9edmq86eetcxmp6w	bc1q4qh7u0m359cgwpckfpa2xzqtd5f9333jha7a2a	BTC	0.0043	$427.25
6.	12/06/2024 23:13	Strike	bc1qa7re4nq5np2jkjwmm65ly98c42z3eq04xft37n	bc1q4qh7u0m359cgwpckfpa2xzqtd5f9333jha7a2a	BTC	0.0192	$1,934.34
7.	12/07/2024 00:57	Strike	bc1qs0y5eu4e3y2j63pe6njvjqflwsm5me3nltnpcf	bc1q4qh7u0m359cgwpckfpa2xzqtd5f9333jha7a2a	BTC	0.038	$3,816.28

No.	Date/Time	From Exchnage	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
8.	12/09/2024 17:02	Strike	bc1q3x7j8lrqvf30ddrpfsvts0fs792cm8qknjnzev	bc1q4lfk9gr64cupngpsxgw85xs9jkzaxcvc4s2m5g	BTC	0.1217	$12,314.80

DEFENDANTS CONVERT PLAINTIFF AND CLASS MEMBERS' ASSETS

56. As stated, Plaintiff engaged Inca in order to conduct a forensic analysis to trace the disposition of Plaintiff's BTC deposits.

57. Inca's investigation revealed that Defendants used Digital Leader to convert Plaintiff and Class Members' assets, and then sent those assets through a web of transactions designed to hide their trail. Inca has traced and connected Defendants' transactions, found and followed a trail of transactions, and identified the cryptocurrency wallets that hold Class Members' funds. Inca's investigation found that Plaintiff and Class Members sent funds from accounts at the following sources and cryptocurrency exchanges: CashApp and Strike.

A. Inca's Methodology

58. Inca Digital's forensic tracing process follows a structured two-phase methodology to reconstruct the movement of stolen assets. This process identifies key wallet types that play distinct roles in the laundering scheme:

a. **Intake Wallet**: The first address provided to the victim for depositing funds into the scam. Intake Wallets are controlled by Defendants and serve as the entry point for misappropriated assets before further movement through laundering pathways (hereinafter referred to as "Intake Wallet").

b. **Pivot Wallet**: An address that consolidates stolen funds from multiple victims before dispersing them to final deposit addresses. These wallets obscure the original source of funds and facilitate layering to evade detection. Identifying Pivot Wallets is critical in tracing structured laundering patterns (hereinafter referred to as "Pivot Wallet").

c. **Deposit Wallet**: A cryptocurrency wallet assigned to a user account on a centralized exchange. These wallets serve as deposit points where funds are sent before potential withdrawal, liquidation, or further movement (hereinafter referred to as "Deposit Wallet").

59. The forensic tracing process consists of two phases, each of which is precise, reliable, and replicable: Forward Tracing, which follows stolen assets from their initial destination through intermediary transactions to their final locations, and Reverse Tracing, which traces back from the final deposit points to uncover additional victims and the broader extent of the scam.

60. Forward Tracing tracks stolen funds through intermediary transactions to Deposit Wallets. It identifies key laundering techniques, including Intake Wallet transfers, Pivot Wallet aggregation, partial splits, layering transactions, and rapid transfers used to disguise fund origins. Pivot Wallets act as collection points where multiple victims' funds are pooled before further redistribution. These wallets are commonly used in laundering schemes to break the direct trace between stolen assets and their final destinations.

61. Reverse Tracing involves tracing back from Deposit Wallets to confirm they received funds from multiple unrelated victim wallets, establishing the structured nature of the

laundering process. Inca traces back from Pivot Wallets to identify additional victims whose assets were commingled before further movement. This process confirms the extent of the fraud scheme by analyzing how widely dispersed stolen funds became before reaching their final destinations.

B. Tracing the Movement of Plaintiff's Funds

62. As discussed above, Plaintiff made 8 different transaction between November 26, 2024 and December 9, 2024. Plaintiff transferred a total of $19,018.05 to Intake Wallets – the first known scam-controlled addresses where Defendants directed Plaintiff to send assets.

63. From these wallets, perpetrators systematically moved funds through a series of additional transactions until they reached Deposit Wallets. In total, Plaintiff sent funds to three different Intake Wallets:

a. **Intake Wallet #1:** bc1q4ufqeuhelstl9jymcg3gy3k8df904g8cdnghpw

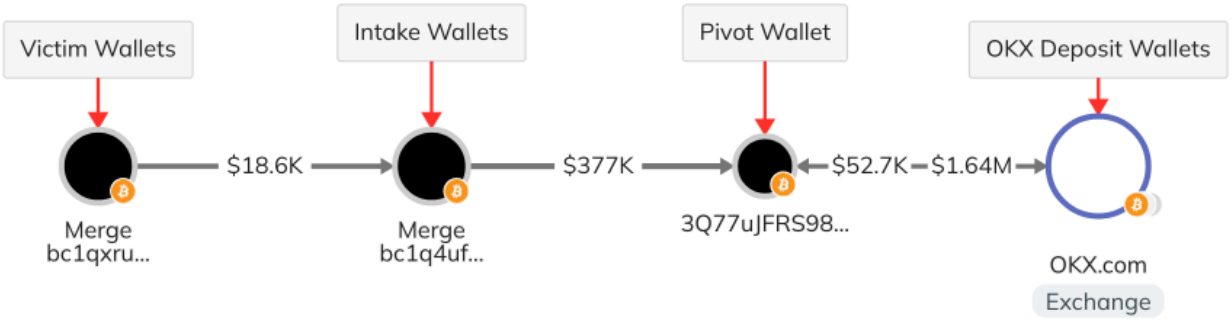
b. **Intake Wallet #2:** bc1q4qh7u0m359cgwpckfpa2xzqtd5f9333jha7a2a

c. **Intake Wallet #3:** bc1q4lfk9gr64cupngpsxgw85xs9jkzaxcvc4s2m5g

64. Plaintiff's funds were routed through intermediary wallets, including Pivot Wallets, where they were combined, split, and transferred across multiple additional addresses. These structured movements demonstrate an intent to break direct transaction links, disrupt traceability, and hinder asset recovery. The assets were ultimately deposited into Deposit Wallets.

65. In this case, Inca's forensic analysis identified one Pivot Wallet where the misappropriated funds were consolidated: 3Q77uJFRS98MndyY8d2t4eyZgjL2x1w9JX

66. Inca's forensic analysis identified one pathway that traced Plaintiff's funds. This involves a direct transfer where funds moved from Intake Wallets to the Pivot Wallet to the Deposit Wallets without additional intermediary steps. This can be visualized as follows:



67. Each of the eight transfers made by Plaintiff followed the same pattern.

D. Tracing the Movement of Class Members' Funds

68. Forensic blockchain analysis confirms that the theft of Plaintiff's assets was not an isolated incident but part of a systematic fraud scheme, structured to obscure transaction origins and facilitate large-scale misappropriation of cryptocurrency.

69. The same Pivot Wallet that received Plaintiff's funds also shows structured inflows from multiple unrelated wallets following similar transaction patterns, confirming their role as collection points in a broader fraud network.

70. Pivot Wallets are essential to identifying the affected group or class of victims because they establish that multiple victims' funds were controlled by the same bad actor or group. These wallets function as aggregation points where stolen funds from numerous victims converge, demonstrating a systematic, coordinated scheme.

71. By consolidating funds from unrelated victims into a single location, Pivot Wallets establish a centralized point of control, linking disparate victims to a unified fraudulent operation.

72. By tracing inflows into known the Pivot Wallet, Inca identified approximately 44 additional victim wallets whose transactions followed the same structured fund movement patterns as Plaintiff's transactions. These wallets exhibited identical laundering behaviors:

a. **Matching structured transaction pathways** observed across multiple victims, following the same laundering techniques;

b. **Pivot Wallet aggregation**, confirming that multiple victims' funds were pooled in the same intermediary wallets before onward movement;

c. **Consistent transaction behaviors** across victims, reinforcing the presence of a coordinated fraud operation.

73. Estimated Total Class-Wide Losses are pproximately $1,999,539 based on cumulative victim deposits into the identified Pivot Wallet. Approximately $2,121,323 in total was transferred from the identified Pivot Wallet to Deposit Wallets, including $1,640,369 USD to OKX and $480,954 USD to Binance.[10]

74. The following Deposit Wallets represent the last known locations where misappropriated assets were traced. Forensic blockchain analysis confirms that these wallets were used in structured laundering processes, and the stolen funds remain at imminent risk of further dissipation beyond recovery:

Exchange	**Wallet Address**
Binance	1GoKwxgMgK7oWKyaWsiwh9Yj5zS9WgbmDy
OKX	bc1qpalxma6vz4yexujhh7vgaxl0np69r2rpnyjftrdz77u80nl0g8vspqesmq
OKX	bc1q3cmxrnu9a4xcm4asjpqh6ry43k65ua8r2szrdk23ewf7stheuyxqclrzps

CLASS ALLEGATIONS

[10] OKX and Binance are are cryptocurrency exchanges – online platforms where users can buy, sell, and trade digital assets like BTC.

75. This action may be properly maintained as a class action under Illinois law. Plaintiff, therefore, files this as a class action on behalf of himself and the following class:[11]

> all persons and entities who, at the suggestion of the scammers or individuals acting under the scammers' instruction or control, transferred cryptocurrency into one or more of the cryptocurrency wallets identified in Appendix A and other scam wallet addresses as may be identified during discovery.

65. Excluded from the Class are the Court and its personnel and the Defendants and their officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them has a controlling interest.

66. The members of the Class are so numerous that joinder is impracticable.

67. Common questions of law and fact are apt to drive resolution of the case, exist as to all members of the Class, and predominate over any questions affecting solely individual members of the Class including, but not limited to, the following:

a. Whether the Defendants unlawfully obtained the Plaintiff's and Class Members' cryptocurrency;

b. Whether Defendants had a legal right to acquire Plaintiff's and Class Members' cryptocurrency;

c. Whether Defendants were unjustly enriched as a result of the transfer of the Plaintiff's and Class Members' cryptocurrency;

d. Whether Defendants received from Plaintiff and the Class Members money and property;

[11] Plaintiff reserves the right to modify the Class Definition at the class certification stage or as otherwise instructed by the Court.

e. Whether Defendants withheld and converted to themselves the assets and property of Plaintiff and Class Members in a manner inconsistent with their property rights in those assets;

f. Whether Plaintiff and Class Members have been deprived of the use of their assets and damaged as a result;

g. Whether Defendants knew or should have known they received money wrongfully obtained from Plaintiff and Class Members through unlawful conduct including but not limited to theft or conversion;

h. Whether Defendants unfairly benefited by keeping the Plaintiff's and Class Members' funds at issue;

i. Whether Defendants' retention of the Plaintiff's and Class Members' assets is inequitable;

j. Whether Defendants' receipt and retention of the Plaintiff's and Class Members' funds in question caused Plaintiff and the Class Members financial harm; and

k. Whether Defendants acted with oppression, fraud, and malice, and with actual and constructive knowledge that the Plaintiff's and Class Members' assets were wrongfully converted by Defendants for their own personal use and without the knowledge of or approval by Plaintiff or the Class Members.

68. Plaintiff's claims are typical of the claims of other Class Members, as all members of the Class were similarly affected by Defendants' wrongful conduct in violation of law, as complained of herein.

69. Plaintiff will fairly and adequately protect the interests of the Class Members and has retained counsel that is competent and experienced in class action litigation. Plaintiff has no interests that conflicts with, or is otherwise antagonistic to, the interests of other Class Members.

70. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Further, as the damages that individual Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for Class members to individually redress the wrongs done to them, especially given the complex and convoluted details of the scheme at issue. There will be no undue difficulty in management of this action as a class action.

COUNT I – CONVERSION

71. Plaintiff realleges and incorporates herein by reference the foregoing paragraphs as though fully set forth herein.

72. At all times relevant, Plaintiff had a lawful right to possess the funds and assets transferred to Digital Leader platform as described above. These funds and assets were Plaintiff's personal property.

73. Plaintiff retained an absolute and unconditional right to the immediate possession of these funds. At no point did Plaintiff intend to relinquish ownership of these funds permanently, nor did he authorize their conversion to another person's use outside the context of the promised cryptocurrency investment returns and withdrawals.

74. Plaintiff made multiple demands for the return and withdrawal of these funds, each of which was denied or ignored by Defendants through false representations, fabricated fees, or a complete cessation of communication.

75. Defendants wrongfully and without authorization assumed control, dominion, and ownership over Plaintiff's funds and assets by transferring them from Plaintiff's accounts into digital wallets controlled exclusively by Defendants, without any intent to return the funds and without legal justification.

76. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $19,018.05, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $1,999,539.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court enter judgment in its favor and for the following relief:

i. Compensatory and punitive damages in an amount to be determined at trial;

ii. Pre- and post- judgment interest;

iii. Attorney's fees and costs, as allowable by law; and

iv. Any additional relief that this Court deems equitable and just.

COUNT II – UNJUST ENRICHMENT

77. Plaintiff realleges and incorporates herein by reference the foregoing paragraphs as though fully set forth herein.

78. Plaintiff transferred substantial funds, totaling in excess of $19,018.05, to what he was led to believe was a legitimate work platform promoted and controlled by Defendants.

79. These funds were obtained by Defendants and/or entities controlled by them through misrepresentations and deceptive practices, including false claims about commissions, withdrawal procedures, and the legitimacy of the Digital Leader platform.

80. Defendants retained the benefit of these funds, either by personally converting the funds, transferring them to Deposit Wallets under their control, or otherwise gaining economic benefit at Plaintiff's expense.

81. Plaintiff received no actual returns on his cryptocurrency deposits into Digital Leader, nor was he permitted to withdraw the funds. The entire structure of the transaction was a scheme designed to unjustly enrich the Defendants at Plaintiff's direct financial detriment.

82. Defendants' retention of these funds violates fundamental principles of justice, equity, and good conscience. It would be inequitable to allow Defendants to retain the benefit of Plaintiff's funds under these circumstances.

83. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $19,018.05, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $1,999,539.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court enter judgment in its favor and for the following relief:

i. Compensatory and punitive damages in an amount to be determined at trial;

ii. Pre- and post- judgment interest;

iii. Attorney's fees and costs, as allowable by law; and

iv. Any additional relief that this Court deems equitable and just.

COUNT III - REPLEVIN

84. Plaintiff realleges and incorporates herein by reference the foregoing paragraphs as though fully set forth herein.

85. Plaintiff is the rightful owner of, or lawfully entitled to the immediate possession of, certain personal property consisting of funds and assets totaling approximately $19,018.05,

which were transferred to Defendants, via Digital Leader, under false pretenses and are now wrongfully detained by Defendants or their agents.

86. These funds are traceable and identifiable as cryptocurrency assets that Plaintiff deposited into what he was fraudulently led to believe was a legitimate work platform promoted, controlled, or operated by Defendants.

87. Defendants are wrongfully detaining this property without legal justification and have refused to return it to Plaintiff despite repeated demands. Plaintiff's right to the funds is superior to that of Defendants, and he seeks recovery based on the strength of his own title and entitlement to immediate possession.

88. Upon information and belief, the property in question has not been taken for any tax, assessment, or fine levied under any law of this State against Plaintiff, nor has it been seized under any lawful process against Plaintiff's goods and chattels, nor is it held by virtue of any order for replevin against Plaintiff.

89. Defendants' continued possession of the property constitutes unlawful detention and deprives Plaintiff of the use, benefit, and value of his funds.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court enter judgment in its favor and for the following relief:

i. Return of the stolen funds;

ii. Pre- and post- judgment interest;

iii. Attorney's fees and costs, as allowable by law; and

iv. Any additional relief that this Court deems equitable and just.

COUNT IV – DECLARATORY RELIEF

90. Plaintiff realleges and incorporates herein by reference the foregoing paragraphs as though fully set forth herein.

91. Plaintiff has a clear, legally protectable, and tangible interest in the funds and assets he transferred, totaling in excess of $19,018.05, which he believed were being deposited into a legitimate work platform operated and promoted by Defendants.

92. Defendants, by fraudulently inducing Plaintiff to transfer said funds and subsequently assuming control and ownership over them, assert an adverse and opposing interest in the funds, which is in direct conflict with Plaintiff's right to immediate possession and control.

93. An actual and ongoing controversy exists between the parties concerning their respective rights to the funds and assets, which are traceable to the Deposit Wallet addresses and other digital accounts associated with Defendants. Plaintiff seeks a judicial declaration to resolve this dispute and to confirm his entitlement to restitution of the full amount of funds he deposited.

94. The controversy is not moot, hypothetical, or premature. It involves a concrete dispute over the ownership of specific funds and does not seek an advisory opinion or a determination based solely on future or abstract events.

95. Declaratory relief is appropriate and necessary to clarify and affirm Plaintiff's legal rights and interests with respect to the misappropriated funds.

WHEREFORE, Plaintiff respectfully requests that this Honorable Court enter judgment in its favor and for the following relief:

i. Declaration that Plaintiff is entitled to funds he deposited into the Digital Leader platform promoted by Defendants;

ii. Attorney's fees and costs; and

iii. Any additional relief that this Court deems equitable and just.

Respectfully submitted,

/s/ Michael Kozlowski
Michael Kozlowski
ESBROOK P.C.
321 N. Clark Street, Suite 1930
Chicago, IL 60654
(312) 319-7680
michael.kozlowski@esbrook.com
Attorney No. 62618

Attorneys for Plaintiff

APPENDIX A

Pivot Wallets

1. 3Q77uJFRS98MndyY8d2t4eyZgjL2x1w9JX