IN THE CIRCUIT COURT OF FRANKLIN COUNTY, ILLINOIS

GERALD THORNHILL, an individual, on behalf of himself and all others similarly situated	)	Case No.:
Plaintiff,	)	Hon.:
v.	)	
JANE DOE a/k/a LISA DAVIS; JANE DOE a/k/a MIA REYES; JOHN DOE a/k/a BILL DAVIS; JOHN DOE a/k/a John Harrison And JOHN DOES 3-25,	)	2025LA27
Defendant.	)	

COMPLAINT

NOW COMES Plaintiff, Gerald Thornhill ("Plaintiff"), by and through his attorneys, ESBROOK P.C., and for his Complaint against Defendants Jane Doe a/k/a Lisa Davis, Jane Doe a/k/a Mia Reyes, John Doe a/k/a Bill Davis, John Doe a/k/a John Harrison, and John Does 3-25 ("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. Plaintiff was defrauded of approximately $102,327 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. This scam was perpetrated starting June 2024 and continuing until January 2025.

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 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 contacted Plaintiff via both Whatsapp and Telegram. The scammers posed as friendly and successful investors, engaging Plaintiff in regular conversation and offering to provide lessons regarding investing. Defendants called these lessons the "millionaire bootcamp." Defendants, thus, developed a rapport with Plaintiff by presenting themselves as sophisticated advisors, including one of the scammers calling himself Professor Harrison to make himself seem credible.

6. Defendants gained Plaintiff's trust and persuaded him to make an initial small deposit into what appeared to be a legitimate online cryptocurrency trading platform – CLFcoin.com ("CLFcoin"). After this first "investment" transaction, the platform showed a significant return on the initial investment.

7. At one point, Defendants persuaded Plaintiff to participate in a purported Initial Coin Offering ("ICO") and Defendants offered Plaintiff a $30,000 loan to enable his participation.

Defendants represented that the ICO was successful and that Plaintiff had to repay the loan out of his own funds rather than from the profit Plaintiff purportedly made on the ICO. Plaintiff, thus, had to send funds to Defendants.

8. These artificial profits from the ICO and other purported trades and investments, combined with ongoing encouragement from Defendants, led Plaintiff to deposit increasingly large sums of money. CLFcoin continued to simulate gains, reinforcing the illusion that Plaintiff's funds were growing, when in fact they were being siphoned off to digital wallets controlled by Defendants.

9. When Plaintiff eventually attempted to withdraw a significant portion of his investment, he was told he must first pay a withdrawal fee. This demand was yet another attempt to extract additional funds from Plaintiff.

10. Despite repeated attempts to withdraw his money, Plaintiff was unable to retrieve any of the deposits or supposed earnings. Eventually, all communication ceased and CLFcoin became inaccessible. Defendants stole approximately $102,327 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.

11. Plaintiff retained a forensic cryptocurrency expert, Inca Coalition ("Inca"), to trace the stolen funds on the blockchain. Each transaction, as explained in more detail below, 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.

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

13. 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 platforms, emotional and psychological manipulation, misrepresentation of profits, 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.

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

THE PARTIES

15. Plaintiff is an individual and a retired teacher residing in Mulkeytown, Illinois.

16. 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

17. 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.

18. 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 Franklin County, where Plaintiff resides and was primarily targeted by Defendants' scheme.

CRYPTOCURRENCY BASICS

19. 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. Bitcoin ("BTC") and Ethereum ("ETH") are the most well-known virtual currencies in use.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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

28. 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

29. "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]

30. 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. The scammers guide the victims to a fake cryptocurrency trading platform.[2]

31. The fraudulent investment 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.

---

[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.

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

33. 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]

34. 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.

35. 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

36. Pig butchering schemes are frequently orchestrated by transnational criminal organizations based in Southeast Asia, particularly Myanmar, Laos, and Cambodia. These criminal

[3] *See* Federal Bureau of Investigations ("FBI") 2024 Crime Report https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[4] *Id*.

groups operate with high degree of coordination, often using trafficked labor to target victims around the globe, including United States.[5]

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

38. 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]

39. 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

[5] *See* https://www.pbs.org/newshour/show/how-human-trafficking-victims-are-forced-to-run-pig-butchering-investment-scams
[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

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

40. 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 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.

41. 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.

42. 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.

[9] *See* https://www.wired.com/story/pig-butchering-scam-invasion/

DEFENDANTS LURE PLAINTIFF

43. Plaintiff was contacted by Defendants who represented themselves as investment advisors and encouraged him to create an account with CLFcoin which appeared to be a legitimate cryptocurrency derivatives trading platform. CLFcoin appeared professional and it included content that gave the impression of a credible operation.

44. In order to gain Plaintiff's trust, Defendants purported to provide educational support and guidance in cryptocurrency investing. They presented themselves as knowledgeable professionals, offering investment lessons and strategic advice. One of the defendants operated under an alias, styling himself as "Professor Harrison" thereby falsely implying authority and expertise in financial matters. This deceptive conduct was a calculated effort to manipulate Plaintiff into relying on Defendants' guidance and entrusting funds to CLFcoin.

45. Defendants used other aliases. Plaintiff often communicated with Defendants Lisa Davis ("Davis"), Mia Reyes ("Reyes") and Bill Davis.

46. On or around June 2024, Davis was the first person to contact Plaintiff. Davis initiated communication regarding an opportunity related to the CLFcoin platform. As Plaintiff understood it at the time, Davis was offering access to a cryptocurrency investment and trading program.

47. Believing he was signing up to receive legitimate investment advice, Plaintiff was added by the Defendants to a WhatsApp group chat. The group included other individuals who were, according to Defendants, also receiving instruction in cryptocurrency investing and participating in trading activities via the CLFcoin platform.

48. Within the group, individuals identifying themselves as Bill Davis and another using the alias "Professor" John Harrison conducted so-called investment lessons and training

sessions. These sessions were labeled the "Millionaires Bootcamp." During these sessions, the Defendants directed Plaintiff and other participants on specific trades to execute on the CLFcoin platform.

49. To further bolster the appearance of legitimacy and instill confidence in the operation, Defendants presented what they claimed was an advertisement for the CLFcoin platform displayed in New York City's Times Square. Upon information and belief, this advertisement was fabricated and used solely as a deceptive tool to create credibility.

50. Initially, Defendants credited Plaintiff with $500 on the CLFcoin platform, stating that Plaintiff could use the amount to trade and would be allowed to keep any resulting profits. The platform subsequently showed what appeared to be a successful trade, which persuaded Plaintiff to invest his own personal funds.

51. Defendants represented that CLFcoin provided the opportunity to trade options on cryptocurrency, specifically through a method known as binary options trading. In this model, participants are required to predict the directional movement of cryptocurrency's price within a set time frame — whether the price would move up or down.

52. Based on Defendant's representations and encouragement, Plaintiff invested more funds into the CLFcoin platform. In order to do so, Plaintiff withdrew money from his own savings account, from his retuirement accounts, and from his account in the Robinhood app (mobile app that allows users to trade stocks).

53. At a later stage, Defendants represented to Plaintiff that he had been issued a $30,000 loan for the purpose of investing in an ICO. Plaintiff accepted this purported loan from Defendants and invested in the ICO.

54. Defendants claimed this purported investment had generated profits totaling approximately $1,200,000.

55. Defendants informed Plaintiff that in order to access the purported profits from the ICO, he was required to first repay the loan. To do that, Plaintiff had to withdraw funds from his bank and retirement accounts and mail cash to Defendants in order to repay the purported loan.

56. Plaintiff was not allowed to repay the loan from the funds allegedly earned in the ICO.

57. Thereafter, Plaintiff attempted to withdraw his earnings. Plaintiff was informed by Defendants that he had to pay a withdrawal fee in the amount of $27,000 in order to access his earnings. Plaintiff had to withdraw funds from his retirement account in order to make this withdrawal fee payment.

58. Defendants represented that once the withdrawal fee was paid, the funds would be deposited directly into Plaintiff's personal bitcoin wallet. However, no such deposit was ever made. When Plaintiff inquired, Defendants claimed that the wallet address provided by Plaintiff was incorrect.

59. After falsely claiming the funds could not be transferred due to the alleged incorrect wallet address, Defendants, via purported customer service agents on CLFcoin, demanded an additional payment, described as a "recovery fee" of $10,000 in order to release the funds.

60. While Plaintiff was attempting to withdraw his funds, Professor Harrison contacted Plaintiff and told him that Plainitff had to pay yet another fee to withdraw his earnings because the price of BTC went up. Plaintiff paid additional $8,000 to Defendants to access his purported earnings.

61. After Plaintiff made a $8,000 payment, Defendants stopped talking with Plaintiff and disappeared. Defendants deleted the contents of their conevrsations on WhatsApp and Telegraph.

62. At that point Plaintiff realized he was scammed.

63. Between June 6, 2024 and January 2, 2025, Plaintiff transferred a total of $65,827 across 21 transactions to CLFcoin, which was a fraudulent platform controlled by Defendants. Additionally, Plaintiff sent cash to Defendants to repay the purported loan. 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.	2024-06-06 1:10:11	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x3B2f70827f561428CAd820aEe8229F40491AaB20	USDT	1,389.576674	$1,389.34
2.	2024-06-18 8:20:12	Coinbase	36ecnmVHRgTysY3vyzZX8aTeuca7jev678	bc1q6tza5ppsjnkwfuwzn6ns5786rsaer80cvg4k xp	BTC	0.00308097	$200.66
3.	2024-06-18 21:18:09	Coinbase	bc1q38mjry4c6557y4324w44zlcggqt6pfjpg0t6ts	bc1q0e63kuwfhzjwjzqgseghprq7kvks7l2szg8gc 4	BTC	0.00306905	$199.36
4.	2024-06-18 1:59:15	Coinbase	0x1985EA6E9c68E1C27 2d8209f3B478AC2Fdb25c87	0x3B2f70827f561428CAD820aEe8229F40491AaB20	USDC	490	$490.05

5.	2024-06-19 15:23:11	Coinbase	0x1985 EA6E9c 68E1C2 7 2d8209f 3B478A C2Fdb2 5c87	0xEE685 cB73E45 c5A B1d6B05 9886E67 620c D0dEd74	USDC	1,353.00	$1,353.11
6.	2024-06-20 5:36:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C AD820a Ee8229F 40491 AaB20	USDC	5	$5.00
7.	2024-06-20 23:31:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C AD820a Ee8229F 40491 AaB20	USDC	3,001.3	$3,000.08
8.	2024-06-21 23:02:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C Ad820aE e8229F4 0491 AaB20	USDC	1,502.87	$1,501.91
9.	6/27/2024 12:45:11 AM	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C AD820a Ee8229F 40491 AaB20	USDC	497.99	$497.92
10.	2024-06-28 16:18:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C Ad820aE e8229F4 0491 AaB20	USDC	45	$44.99
11.	2024-07-02 23:20:11	Coinbase	0xA9D1 e08C77 93af67e	0x3B2f7 0827f561 428C	USDC	1,243.84	$1,242.99

			9d92fe3 08d5697 FB81d3 E43	AD820a Ee8229F 40491 AaB20			
12.	2024-07-24 20:25:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C Ad820aE e8229F4 0491 AaB20	USDC	1,001.04	$1,000.04
13.	2024-07-30 12:44:07	Coinbase	bc1qmfl fugz9sm crg35t4 04trgejd l3tyd0ae j296e	1C8vAHj 3k87A22 x3B ehvy1JR FZmw6A yNu Y	BTC	0.00035165	$22.89
14.	2024-08-06 11:49:11	Coinbase	0xA9D1 e08C77 93af67e 9d92fe3 08d5697 FB81d3 E43	0x3B2f7 0827f561 428C Ad820aE e8229F4 0491 AaB20	USDC	145.46	$144.99
15.	2024-09-27 2:22:41	Crypto.co m	bc1q7cy rfmck2ff u2ud3r n5l5a8y v6f0chk p0zpemf	bc1q9ng wreza8uz 9m8jt g4wqajky laxz39kja jvfff	BTC	0.414059	$26,989.04
16.	2024-09-28 2:07:30	Crypto.co m	bc1q7cy rfmck2ff u2ud3r n5l5a8y v6f0chk p0zpemf	bc1q9ng wreza8uz 9m8jt g4wqajky laxz39kja jvfff	BTC	0.0144	$945.61
17.	2024-10-06 11:04:49	Crypto.co m	bc1q7cy rfmck2ff u2ud3r n5l5a8y v6f0chk p0zpemf	bc1qrmw c4envmw w3s admsk7e h4uewrd m2ea wxckz9q	BTC	0.18895648	$11,775.09
18.	2024-11-12 2:07:48	Crypto.co m	bc1q7cy rfmck2ff u2ud3r	33EJeZH LiQZK5 wwo7	BTC	0.00227044	$204.00

			n5l5a8yv6f0chkp0zpemf	WuoZGiF1Uw6rgGJxe			
19.	2024-12-20 2:30:53	Coinbase	bc1qvma8hpqd58wavp33p82t7k83n8ksh5tmpdv24m	33EJeZHLiQZK5wwo7WuoZGiF1Uw6rgGJxe	BTC	0.00207232	$199.63
20.	2024-12-20 1:24:24	Crypto.com	bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf	bc1qjlhtclds9u47xxpy47dvecapzlv6fq3tuvctj5	BTC	0.0686	$6,680.34
21.	2025-01-02 12:48:34	Crypto.com	bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf	bc1qjlhtclds9u47xxpy47dvecapzlv6fq3tuvctj5	BTC	0.08411799	$7,940.11

DEFENDANTS CONVERT PLAINTIFF'S ASSETS

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

65. Inca's investigation revealed that Defendants used CLFcoin to convert Plaintiff's funds and assets, and then sent those assets and funds 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 Plaintiff and Class Members' funds.

A. Inca's Methodology

66. 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").

67. 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.

68. 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.

69. 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 scheme by analyzing how widely dispersed stolen funds became before reaching their final destinations.

B. Tracing the Movement of Plaintiff's Funds

70. As discussed above, Plaintiff made 21 different transaction between June 6, 2024 and January 2, 2025. Plaintiff transferred a total of $65,827.00 to Intake Wallets – the first known scam-controlled addresses where Defendants directed Plaintiff to send assets. Plaintiff also mailed Defendants $36,500 in cash.

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

a. **Intake Wallet #1:** 0x3B2f70827f561428CAd820aEe8229F40491AaB20

b. **Intake Wallet #2:** bc1q6tza5ppsjnkwfuwzn6ns5786rsaer80cvg4kxp

c. **Intake Wallet #3:** bc1q0e63kuwfhzjwjzqgseghprq7kvks7l2szg8gc4

d. **Intake Wallet #4:** 0xEE685cB73E45c5AB1d6B059886E67620cD0dEd74

e. **Intake Wallet #5:** 1C8vAHj3k87A22x3Behvy1JRFZmw6AyNuY

f. **Intake Wallet #6:** bc1q9ngwreza8uz9m8jtg4wqajkylaxz39kjajvfff

g. **Intake Wallet #7:** bc1qrmwc4envmww3sadmsk7eh4uewrdm2eawxckz9q

h. **Intake Wallet #8:** 33EJeZHLiQZK5wwo7WuoZGiF1Uw6rgGJxe

i. **Intake Wallet #9:** bc1qjlhtclds9u47xxpy47dvecapzlv6fq3tuvctj5

72. 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.

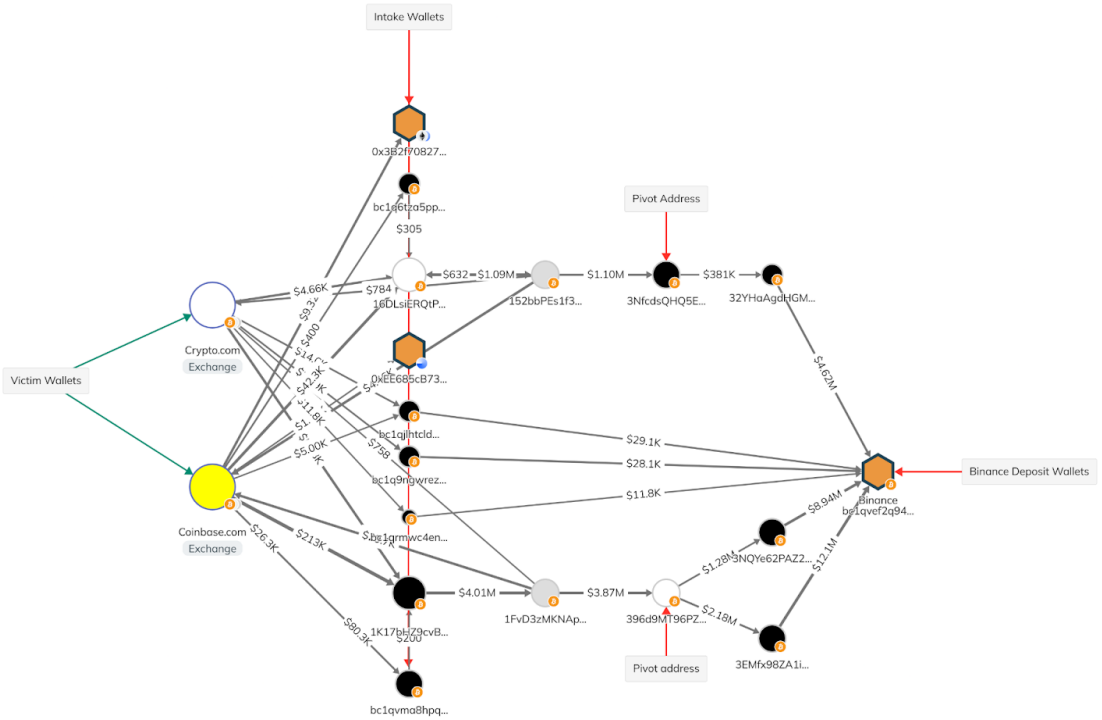
73. In this case, Inca's forensic analysis identified two Pivot Wallets where the misappropriated funds were consolidated: (1) 3NfcdsQHQ5EgszvxxwmwFkYvg2hKPXm9NX and (2) 396d9MT96PZDrGdrMQv1dM4Fc3y4BQLh8c.

74. Forensic blockchain analysis confirms that Plaintiff's funds were systematically routed through transaction pathways designed to obscure their origin.

75. Inca's forensic analysis identified two pathways that traced Plaintiff's funds.

76. Pathway 1 involves the direct transfer of funds from Pivot Wallets to Exchange Deposit Wallets without additional intermediary steps. Pathway 2 shows a more complex route in which funds moved from Pivot Wallets through one or more Intermediary Wallets before reaching Exchange Deposit Wallets.

77. The movement of Plaintiff and victim funds' can be visualized as follows:



D. Tracing the Movement of Class Members' Funds

78. 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.

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

80. 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.

81. 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.

82. By tracing inflows into known the Pivot Wallet, Inca identified several 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.

83. Estimated total class-wide losses are approximately $25,788,591 based on cumulative victim deposits into the identified Pivot Wallet. Approximately $20,425,938 in total was transferred from the identified Pivot Wallet to Deposit Wallets.

84. 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	bc1qpzkywnxpvavv4mpzeahx6u2msu8lg2w64ny78l
Binance	173h6qLV2Q9qAnuPhan5iA19NN8W9hFfkp
Binance	1a3mrzsEa9dbpFsZptbYBntv85kiw99eA
Binance	bc1qvef2q948lpcc4hrtxhsnz8e5760qhwdkqs5m2c

Binance	1J5fHhbYD2mE4DYsvvxKUCuagR4BwUbaCw
Binance	bc1qhvv6xy83e86xyaz2s5msh2kpzgquvmld0qp73v
Binance	17N4xBJ4djsP2L9FB7Yy5SMwXWTkCpT5GD
Binance	17hcwXPCoHKToVvdCX5bqWSPrasSYeynD4
Binance	1PBscVYqvVgLFZKgX3uLFEsnwx3uMrkv2e
Binance	1DnpLKszbCt84ZB9ibXmNh7yoLWyWHi7XY
Binance	1PMZyRAdf5FUoU9YcBMGsDkLTXTiBYfgLy
Binance	17QMVbiZuuXuWJbViK5p7BaXEKGBadebRi
Binance	1N52Dc6HRET1qciP5hgpUc6FW4ffRc2cFc
Binance	165az4zzkuf1p4aWW4XZTWd5YGizFS3NXa
Binance	1EL74i3GSJw3zQsWyT6Hmv2wn6m5nMJTtj
Binance	1L3NjDDG8wtdzCB34ZPsS87xgn8RkB8skV
Binance	1BbaVcW9XDCoi2mYMDDkdHjHFGg7RMrBov

CLASS ALLEGATIONS

85. 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:[10]

> 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.

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

86. 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.

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

88. 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;

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.

89. 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.

90. 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.

91. 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

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

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

94. Plaintiff retained an absolute and unconditional right to the immediate possession of these funds and assets. 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.

95. 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.

96. 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.

97. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $102,327, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $25,788,591.

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 cost, as allowable by law; and

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

COUNT II – UNJUST ENRICHMENT

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

99. Plaintiff transferred substantial funds, totaling in excess of $102,327, to what he was led to believe was a legitimate investment platform promoted and controlled by Defendants.

100. These funds were obtained by Defendants and/or entities controlled by them through misrepresentations and deceptive practices, including false claims about trade returns, withdrawal procedures, and the legitimacy of the CLFcoin platform.

101. 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.

102. Plaintiff received no actual returns on his cryptocurrency deposits into CLFcoin, 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.

103. 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.

104. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $102,327, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $25,788,591.

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 IV - REPLEVIN

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

106. Plaintiff is the rightful owner of, or lawfully entitled to the immediate possession of, certain personal property consisting of funds and assets totaling approximately $102,327, which were transferred to Defendants, via CLFcoin, under false pretenses and are now wrongfully detained by Defendants or their agents.

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

108. 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.

109. 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.

110. 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 V – DECLARATORY RELIEF

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

112. Plaintiff has a clear, legally protectable, and tangible interest in the funds and assets he transferred, totaling in excess of $102,327, which he believed were being deposited into a legitimate work platform operated and promoted by Defendants.

113. 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.

114. 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.

115. 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.

116. 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 his favor and for the following relief:

i. Declaration that Plaintiff is entitled to funds he deposited into the CLFcoin 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
Taras Garapiak
ESBROOK P.C.
321 N. Clark Street, Suite 1930
Chicago, IL 60654
(312) 319-7680
michael.kozlowski@esbrook.com
taras.garapiak@esbrook.com

Attorneys for Plaintiff

Dated: July 3, 2025

APPENDIX A

Pivot Wallets

Pivot Wallet #1: 3NfcdsQHQ5EgszvxxwmwFkYvg2hKPXm9NX

Pivot Wallet #2: 396d9MT96PZDrGdrMQv1dM4Fc3y4BQLh8c