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

GEORGE ZAMBRANA, an individual, on behalf of himself and all others similarly situated	)	Case No.:2025CH11647
Plaintiff,	)	Hon.
v.	)	
JANE DOE a/k/a "JESSICA" and JOHN DOES 1-25,	)	
Defendants.	)	

COMPLAINT

NOW COMES Plaintiff, George Zambrana ("Plaintiff"), by and through his attorneys, ESBROOK P.C., and for his Complaint against Defendants Jane Doe a/k/a "Jessica" and 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 August through November 2024, Plaintiff was defrauded of approximately $213,500.00 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, Defendant identifying herself as Jessica ("Jessica") contacted Plaintiff via a text message. Jessica posed as a friend to Plaintiff, often conversing with Plaintiff about their children and family backgrounds. Over the course of several months from June 2024 until November 2024, Defendants, through Jessica, developed a rapport with Plaintiff, eventually convincing Plaintiff to make cryprocurrency related investments.

6. Defendants gained Plaintiff's trust by promising him significant earnings from the purported cryptocurrency investments. Defendants introduced Plaintiff to what appeared to be a legitimate online cryptocurrency platform – jys.sgxps.net ("SGX"). Defendants then convinced Plaintiff to make Ethereum ("ETH") deposits into the platform. SGX purported to show significant growth on Plaintiff's investments and trades.

7. These artificial earnings, combined with ongoing encouragement from Defendants, led Plaintiff to deposit large sums of ETH into SGX. This platform continued to simulate gains

and commissions, reinforcing the illusion that Plaintiff was making legitimate trades, when in fact Plaintiff's ETHs were being siphoned off to digital wallets controlled by Defendants.

8. Eventually, Jessica encouraged Plaintiff to try and withdraw $100,000 of his purported earnings. At that point, Plaintiff was told that he had to pay a "VIP Fee" and a "Cross-Border Fee." Additionally, Plaintiff was told that he had to pay another fee to prevent money laundering. These fees were calculated as a percentage of Plaintiff's purported earnings and these fees were a further attempt to extract additional funds from Plaintiff as they could not be deducted from Plaintiff's purported earnings on SGX.

9. Plaintiff was unable to pay the various fees and therefore was unable to retrieve any of the deposits or supposed earnings. Eventually, all communication with Jessica ceased. Defendants stole approximately $213,500.00 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 ETH 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 technological scam against numerous others.

11. This scheme was intentionally designed to mimic legitimacy, from the user interface of the fake platform to the scripted responses of the scammers posing as Plaintiff's friends. 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 platforms, emotional and psychological manipulation, misrepresentation of earnings, 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 teacher working in Cook County, Illinois at the time the events described in this Complaint occurred.

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 lives and was primarily targeted by Defendants' scheme. Additionally, 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.

---

[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.

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 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

[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]

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 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

[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

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 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.

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

DEFENDANTS LURE PLAINTIFF IN

42. On or about June 30, 2024, Plaintiff received an unsolicited text message from an individual identifying herself as "Jessica." In the initial message, Jessica inquired whether Plaintiff wanted to get coffee. Because the phone number from which the message originated was not saved in Plaintiff's contacts, and out of courtesy in case the sender was someone known to Plaintiff, he responded affirmatively and asked the sender to identify himself or herself.

43. Jessica replied, indicating that she had mistakenly messaged the wrong number. However, rather than ending the conversation, Jessica initiated further communications and engaged Plaintiff in friendly dialogue. She soon suggested they continue the conversation on Telegram, an encrypted messaging platform, and Plaintiff agreed.

44. In the course of their communications, Jessica represented herself as a fashion designer residing in Los Angeles, California. She claimed to be a member of an exclusive country club in Los Angeles and stated that she was originally from Singapore.

45. During the course of conversations between Plaintiff and Jessica, she stated that she had a child residing in Singapore under the care of her parents. Jessica also revealed to Plaintiff that her husband had abandoned her without financial support, but that she had become financially independent and prosperous through cryptocurrency investments.

46. Over time, Plaintiff developed a friendship with Jessica. Plaintiff, who has children of his own, was in a vulnerable emotional state during this period due to the recent passing of his father. Exploiting Plaintiff's trust and vulnerable state, Jessica gradually introduced discussions about cryptocurrency investment, recommending books and materials on the subject.

47. Initially, Plaintiff expressed disinterest in cryptocurrency related trading and investments. However, Jessica enticed Plaintiff with promises of easy profits, financial freedom, and the ability to acquire luxury goods, including expensive cars.

48. Jessica directed Plaintiff to use a trading platform she identified as SGX for executing trades.

49. Under Jessica's guidance, on or around July 29, 2024, Plaintiff made an initial small trade on the SGX platform. This initial trade showed a profitable result.

50. Encouraged by the appearance of profitable results on the platform, Plaintiff proceeded to make larger deposits and trades. Plaintiff transferred funds from his Chase bank account and his retirement accounts to Crypto.com, where he purchased ETH and subsequently transferred it to the SGX platform to execute trades as directed by Jessica.

51. On several occasions, when Plaintiff's financial institutions raised concerns or delayed transfers, Plaintiff withdrew cash directly. Individuals and Defendants associated with Jessica came to Plaintiff's residence to collect the cash and deposit it into the SGX platform on his behalf. The individuals who came to Plaintiff's residence did not reveal their names.

52. The trades, as reflected on the SGX platform, appeared to be highly successful. The platform showed a steadily increasing balance, and on or about August 7, 2024, Plaintiff successfully withdrew $300 into his CashApp account, further bolstering his confidence in the legitimacy of the SGX platform.

53. By November 2024, the purported balance in Plaintiff's SGX account exceeded $2,000,000.

54. On or around November 20, 2024, Defendants informed Plaintiff that he had to pay a fee of 2% of his balance account. The fee was approximately $41,000. Plaintiff could not pay the fee out of his purported account balance on SGX. He had to make a new transfer to the platform.

55. Thereafter Jessica instructed Plaintiff to withdraw $100,000 from SGX. When Plaintiff attempted to do so, he was informed that additional fees—a "VIP Fee" and "Cross Border Fee" totaling approximately 10% of the account balance—had to be paid separately and could not be deducted from his account balance.

56. Plaintiff was further informed by Defendants that yet another 10% fee was required to prevent money laundering. At that point, Plaintiff became suspicious. Although Jessica claimed she would assist Plaintiff with one of the fees, SGX advised Plaintiff that its rules required the fee payment to originate from the same account, rendering Jessica's purported assistance futile.

57. It was at this point that Plaintiff recognized the scheme as fraudulent and understood that he had fallen victim to a scam designed to defraud him of substantial sums of money under the guise of legitimate investment activity.

58. In total, Plaintiff made seven cryptocurrency transfers into wallets controlled by Defendants:

No.	Date/Time	From Exchange	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
1.	2024-08-07 2:58:11	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	0.379	$947.96

No.	Date/Time	From Exchange	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
2.	2024-08-19 22:16:11	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	5.19	$13,580.54
3.	2024-09-24 5:17:47	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	0.210153946	$552.13
4.	2024-11-15 21:52:23	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	7.56	$23,376.26
5.	2024-11-18 22:23:11	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	4.470065702	$14,084.96

No.	Date/Time	From Exchange	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
6.	2024-11-22 20:45:35	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	6.458453649	$21,211.62
7.	2024-11-29 19:7:11	Crypto.com	0x0CfAA1866CD1C1Add85BC58c83324ddd8d5cf688	0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809	ETH	4.573468921	$16,355.12

DEFENDANTS CONVERT PLAINTIFF AND CLASS MEMBERS' ASSETS

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

60. Inca's investigation revealed that Defendants used SGX 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.

A. Inca's Methodology

61. 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").

62. 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.

63. 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.

64. 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

65. As discussed above, Plaintiff made 7 different transactions between August 7, 2024 and November 29, 2024. Plaintiff transferred a total of $ $90,108.59 to Intake Wallets – the first known scam-controlled addresses where Defendants directed Plaintiff to send assets. Additionally, Plaintiff invested $123,500 in cash for the purpose of making trades on SGX.

66. From the Intake Wallets, perpetrators systematically moved funds through a series of additional transactions until they reached Deposit Wallets. In total, Plaintiff sent funds to one Intake Wallet:

a. **Intake Wallet #1:** 0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809.

67. 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.

68. In this case, Inca's forensic analysis identified three Pivot Wallets where the misappropriated funds were consolidated: (1) 0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809, (2) 0x867BDF428D50457bAa3B8D23ebbC371352839E2D, and (3) 0xf17E04068dd253C172e3Ada593DB379d1Bc36947.

69. Inca's forensic analysis identified two pathways that traced Plaintiff's funds. Pathway 1 involves the transfer of funds from Pivot Wallets through one or more Intermediary

Wallets before reaching MEXC.com Deposit Wallets. In a subset of Pathway 1, funds are sent from Pivot Wallet #1 to an intermediary wallet only to be fully returned back to Pivot Wallet #1 and continuing on the same pathway.

70. Pathway 2 shows a route in which funds moved through two Pivot Wallets and an Intermediary Wallet before deposit into a Binance Deposit Wallet. Some funds branched off to additional Intermediary Wallets or an alternative Binance Deposit Wallet.

D. Tracing the Movement of Class Members' Funds

71. 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.

72. The same Pivot Wallets 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.

73. 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.

74. 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.

75. By tracing inflows into known the Pivot Wallets, Inca identified approximately 100 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.

76. Estimated Total Class-Wide Losses are pproximately $23,386,908.00 based on cumulative victim deposits into the identified Pivot Wallet. Approximately $13,906,615.00 in total was transferred from the identified Pivot Wallets to Deposit Wallets.

77. 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	0xA3cF57f1FAe61b39909F96c31453690187e4E339
Binance	0xAb04f223f819033e0357cEE192639dE276fAF53b
Binance	0xb1c3c86D002a5e7222CF26133d554C838298ACD6
Binance	0x2Caa548d466EBAa121173D10E0755791bCbF1f9b
Binance	0x5368Faf6b4C0E01f04672DdCa30FF679CC9F4D69
Binance	0xf7E4365FBA99F02191503B5b4Fa7E7C831fC69a4
Binance	0x8E5D9D1599877028840f88cac602392e441ED3eF
Binance	0x7d4d8056871FDA21E39C8bd6aF4247F19De2042b
Binance	0x9B92DB434F48480d8ebdbE42046D5a2AcEd0eF62

Binance	0x61b7e18BA8bA0413a9ae61CBb263507aFb53B7Cc
Binance	0x1e1D870D6781793EbA4F5818E67d5D443a2d58F9
Binance	0x664A4D0931E79F789Fd15AFa8be8B1cd33F0B4C1
Binance	0x63062CE80c9606DdfaB65868fD4d514240A4DA75
Binance	0x4b5D7A509A67255f92FB9fE2f1B1eE395f02bfA6
Binance	0x2a19A8a2Ab65881A342981B192824fDF6ceF3665
Binance	0x4D4d0A06a33c82A3EBa004B67Bd717DB6b243489
Binance	0xBf5C76FcBBC7D5595dBf746eEb89a99bb6b258D0
Binance	0xAA578136a26b0bd7C7554cB954E976Db2c5c2EA4
Binance	0x3F4b069B8b473F09BE7fC75aca643fF72cb18fE7
Binance	0x790d180ffC15fD7e334255c2DB3b590c22659053
Coinbase	0x36a27D8C800508e97e3182F905922F92098c3808
Coinbase	0x00EF27C0921fB6a5CA5d55AAc977f21f1B05d054
Coinbase	0xA97cF97e6a7567ceA0fe69DF5F59268636733fe8
Coinbase	0x6e7496804654d47D1Ffd3ABBe1C731276fe09c37
Coinbase	0xf9E8677236BaD06A8cF00D715c0A52Ab60a61fd7
Coinbase	0xb3B6F9A495bc265C9cb19C4318B8858B84547De7
Coinbase	0xeED120C0110a8C6B7becB36cc282824A4022AAB7
Coinbase	0xf1E639574dfFE745b93817452d64c25c9788dc77
Coinbase	0x32957A3c71C1dC5E8B286FF306d643D1C4814645
Coinbase	0xd74F8Dbf44f5aF98608476cf17D1814B0c2ee8eb
Crypto.com	0x1fcB5c16B7A1AB3DE79b1e3Cd920DED8f037EBa9
Crypto.com	0x8144A415a61B8A192f9955707DD4Fd31C871E8AE

Crypto.com	0x613e426654a8706cda55b0A6689cF816D03a6BfD
Kraken	0x3320beBf3c5E9868b4BA3ccc0fc40e737da030a7
Kraken	0x530860F71Ed2333a309574ed4fEfE5edfd59982A
KuKoin	0x6320EA8DA6315F971dBE9c923Dbc739e1eAa8c10
KuKoin	0x7dd672a29b71026925f9b1d4BE42370111B1b957
OKX	0xED8C7136B7643f3dc26966fD68ce5f373724fBbB
OKX	0x7A8578D8D97882F9e149745183cabC451F58c000
OKX	0xa3C1D72080d22ba79532262391c844549beC4989
OKX	0x0DEbbF4221856638dce98EFA43b10938084d80F3
OKX	0xE45787ef14dc7F295365154df72C41e79f12407d
OKX	0xf5fFe32272031aB2fBe850d1A22C18057467AF49
MEXC	0x75e89d5979E4f6Fba9F97c104c2F0AFB3F1dcB88

CLASS ALLEGATIONS

78. 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.

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.

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

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;

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 SGX 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 and assets. At no point did Plaintiff intend to relinquish ownership of these funds and assets 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 assets and without legal justification.

76. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $213,500.00, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $23,386,908.00.

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 and assets, totaling in excess of $213,500.00, to what he was led to believe was a legitimate platform promoted and controlled by Defendants.

79. These funds and assets were obtained by Defendants and/or entities controlled by them through misrepresentations and deceptive practices, including false claims about investing, withdrawal procedures, and the legitimacy of the SGX 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 SGX, nor was he permitted to withdraw his funds and assets. 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 and assets under these circumstances.

83. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff has suffered financial losses in excess of $213,500.00, exclusive of interest, attorneys' fees, and costs and total classwise losses are estimated at $23,386,908.00.

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 $213,500.00, which were transferred to Defendants, via SGX, under false pretenses and are now wrongfully detained by Defendants or their agents.

86. These funds and assets are traceable and identifiable as cryptocurrency assets that Plaintiff deposited into what he was fraudulently led to believe was a legitimate 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 and assets 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 and assets.

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 $213,500.00, 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 and assets, 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 assets 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 and assets.

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 SGX platform promoted by Defendants;

ii. Attorney's fees and costs; and

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

Respectfully submitted,

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
Attorney No. 62618

Attorneys for Plaintiff

APPENDIX A

Pivot Wallets

1. **0x4D7EAfcF2cF63b75523daFAF7bC51C5Db666D809**
2. **0x867BDF428D50457bAa3B8D23ebbC371352839E2D**
3 **0xf17E04068dd253C172e3Ada593DB379d1Bc36947**