

IN THE CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT
IN AND FOR PALM BEACH COUNTY, FLORIDA

ERIC LIEBERMAN,
Plaintiff,

v.

Case No.: _____

JANE DOE (a/k/a “Anais Durran”),
DIGITAL ERA GLOBAL LIMITED
(d/b/a “TOKENLON”)
BINANCE HOLDINGS LTD.,
Defendants.

EQUITABLE RELIEF REQUESTED

JURY TRIAL DEMANDED

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Plaintiff Eric Lieberman (“Plaintiff”), by and through undersigned counsel, alleges as follows:

PRELIMINARY STATEMENT

1. Plaintiff Eric Lieberman brings this action to preserve and recover specific, traceable cryptocurrency assets that were wrongfully diverted from his control and can now be followed, through publicly verifiable blockchain transactions, to accounts and transaction pathways associated with Defendants, including Binance and Tokenlon.

2. This is not a speculative claim. It is a case about identifiable property. Plaintiff’s cryptocurrency—consisting of 196.1874 Ethereum and 3.03723 Bitcoin, valued at approximately \$919,336 at the time of transfer—was transferred through a series of intermediary wallets and ultimately routed to addresses and infrastructure associated with Defendants. Those transfers are recorded on immutable public ledgers and can be independently verified through wallet addresses and transaction histories.

3. Blockchain tracing demonstrates a clear and continuous flow of Plaintiff's assets from his originating wallets to exchange-linked endpoints. In particular, Ethereum assets were transferred through intermediary addresses and routed to wallets associated with Binance, including 0x4b92cC0b53E3C3F70EcF190a35E2f86a80Fc9A78, as well as through transaction pathways involving Tokenlon, including 0x7F4B435A3366Fab16627c2d0E0aB1AA55BFCAb55. Plaintiff's Bitcoin assets followed a similar laundering pattern, ultimately reaching a Binance-associated deposit address, including 1Dwv6NFLD41XGQAJLpu9QYm5TJf3PuhBsQ.

4. These assets are therefore specific, identifiable, and recoverable—if preserved.

5. The relief sought in this action is narrow, practical, and urgent. Plaintiff seeks a preliminary injunction directing Defendants to freeze all assets traceable to Plaintiff's transfers and preserve all associated accounts and records pending adjudication of his claims. Plaintiff does not ask this Court to resolve ultimate liability at this stage. Rather, he seeks to maintain the status quo and prevent the irreversible dissipation of traceable property while this case proceeds.

6. The need for immediate judicial intervention is acute. Cryptocurrency assets can be transferred across wallets and jurisdictions in minutes. The blockchain records in this case already reflect a multi-hop laundering pattern, demonstrating that dissipation is ongoing—not hypothetical. Absent prompt relief, the remaining traceable assets are likely to be further transferred, converted, or commingled beyond recovery.

7. Defendant Binance, as a centralized exchange, maintains custody and control over accounts receiving cryptocurrency deposits and has the technical ability to freeze funds, restrict withdrawals, and preserve assets. Tokenlon, through its routing, execution, and liquidity infrastructure, facilitated the movement and potential conversion of Plaintiff's assets and, upon

information and belief, may provide access to or be associated with wallets, smart contracts, or liquidity pools containing traceable proceeds.

8. This action therefore presents a straightforward and urgent question: whether identifiable property, traceable to Plaintiff and currently within or accessible through Defendants' platforms, should be preserved before it is lost.

9. Equity—and the integrity of the judicial process—require that the answer be yes.

PARTIES

10. Plaintiff Eric Lieberman is an individual residing in Palm Beach County, Florida. At all relevant times, Plaintiff owned and controlled cryptocurrency assets that are the subject of this action and suffered injury in Florida.

11. Defendant Jane Doe, also known as “Anais Durran,” is an individual whose true identity is presently unknown. Upon information and belief, Doe resides outside the United States and conducted the fraudulent scheme alleged herein through electronic communications and cryptocurrency infrastructure directed at Plaintiff. Doe may be served pursuant to applicable rules governing service on unknown and foreign defendants.

12. Defendant Digital Era Global Limited is a company organized under the laws of Singapore, with its principal place of business in Singapore. Digital Era Global Limited operates and controls the cryptocurrency platform known as “Tokenlon,” which facilitates digital asset routing, execution, and liquidity services, including transactions involving Ethereum-based assets. Upon information and belief, Digital Era Global Limited conducts business globally, provides services accessible to users in Florida, facilitates transactions involving Florida residents, and played a role in routing and/or executing transactions involving Plaintiff's cryptocurrency assets.

13. Defendant Binance Holdings Limited is a company organized under the laws of the Cayman Islands. Upon information and belief, Binance Holdings Limited operates, controls, and/or oversees the global cryptocurrency exchange commonly known as “Binance,” which provides custodial, trading, and asset transfer services for digital assets. Binance Holdings Limited conducts substantial business affecting Florida residents, facilitates transactions involving Florida-based users, and maintains infrastructure through which cryptocurrency assets—including those traceable to Plaintiff’s transfers—are received, held, transferred, and/or liquidated. Binance Holdings Limited possesses the ability to identify, restrict, and preserve assets within its control.

14. Upon information and belief, Binance Holdings Limited operates through a network of affiliated entities, platforms, and infrastructure collectively referred to as “Binance,” and is responsible for the policies, operations, and custody functions relevant to the transactions at issue in this action.

15. As used herein, “Binance” refers to Binance Holdings Limited and its affiliated entities, platforms, and infrastructure through which cryptocurrency assets are received, held, transferred, or otherwise processed.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to Article V, § 5 of the Florida Constitution and Fla. Stat. § 26.012 because this action seeks damages and equitable relief exceeding the jurisdictional minimum of this Court.

17. This Court has personal jurisdiction over all Defendants pursuant to Florida’s long-arm statute, Fla. Stat. § 48.193, and consistent with due process.

18. Personal jurisdiction exists under Fla. Stat. § 48.193(1)(a)(2) because Defendants committed tortious acts within Florida, including acts giving rise to claims for fraud, conversion, and related misconduct directed at Plaintiff while he was located in Florida.

19. Personal jurisdiction further exists under Fla. Stat. § 48.193(1)(a)(6) because Defendants caused injury to a person within Florida arising out of acts or omissions outside the state, including the misappropriation of Plaintiff's cryptocurrency assets from accounts accessed and controlled by Plaintiff in Florida.

20. Defendants purposefully directed their conduct toward Florida by, inter alia:

- a. Engaging in transactions involving cryptocurrency assets originating from a Florida resident;
- b. Operating platforms and infrastructure accessible to and used by Florida residents, including Plaintiff;
- c. Facilitating, processing, or routing transactions involving Plaintiff's assets while Plaintiff was located in Florida; and
- d. Participating in conduct that they knew or should have known would cause injury to a Florida resident.

21. Upon information and belief, Defendant Binance conducts substantial and continuous business in the United States and Florida, including providing custodial and trading services to Florida residents, facilitating cryptocurrency transactions involving Florida users, and maintaining infrastructure through which assets traceable to Plaintiff were received, held, or transferred.

22. Binance's contacts with Florida are directly related to the claims asserted herein, including its role in receiving and maintaining cryptocurrency assets traceable to Plaintiff's transfers, and exercising control over accounts capable of preserving those assets.

23. Binance Holdings Limited, directly or through its affiliated entities, purposefully availed itself of the privilege of conducting business in Florida by providing cryptocurrency

exchange and custodial services to Florida residents, including services through which Plaintiff's assets were transmitted, received, and/or maintained.

24. Upon information and belief, Defendant Tokenlon operates a cryptocurrency routing and execution platform accessible to users in Florida and facilitates transactions involving Florida residents, including Plaintiff.

25. Tokenlon's infrastructure was used to route and/or execute transactions involving Plaintiff's cryptocurrency assets, thereby establishing a direct connection between Tokenlon's activities and the injuries suffered in Florida.

26. Digital Era Global Limited, through its operation of the Tokenlon platform, purposefully directed its services toward users in Florida, including Plaintiff, by facilitating transactions involving cryptocurrency assets originating from Florida and routing those assets through infrastructure accessible within this State.

27. Defendants have sufficient minimum contacts with Florida such that the exercise of jurisdiction comports with traditional notions of fair play and substantial justice. Defendants purposefully availed themselves of the privilege of conducting activities within Florida and could reasonably anticipate being haled into court in this State.

28. Venue is proper in Palm Beach County, Florida, pursuant to Fla. Stat. § 47.011 because Plaintiff resides in this County and the injuries giving rise to this action were suffered in this County.

FACTUAL BACKGROUND

A. Social Engineering Scheme

29. Beginning in or around September 2025, Plaintiff was contacted by an individual identifying herself as "Anais Durran."

30. Upon information and belief, Doe's communications with Plaintiff were not incidental, but rather part of a coordinated effort to identify, target, and exploit individuals with cryptocurrency holdings for the purpose of inducing large-value transfers.

31. Over a period of months, Doe cultivated a personal and emotional relationship with Plaintiff through frequent communications, including daily messaging and expressions of affection.

32. Doe's communications with Plaintiff were persistent and structured, often occurring multiple times per day, and included discussions of personal matters, future plans, and financial goals, all designed to cultivate a sense of trust, familiarity, and reliance.

33. Doe leveraged this relationship to establish trust and reduce Plaintiff's skepticism, including through frequent personal communication, expressions of affection, and assurances of shared financial success.

34. Doe intentionally built Plaintiff's trust and confidence as part of a coordinated social engineering scheme designed to induce Plaintiff to invest in fraudulent cryptocurrency trading.

35. This scheme follows a well-documented "pig butchering" model, in which perpetrators cultivate trust over time, create the illusion of profitability, and gradually induce victims to transfer increasing amounts of cryptocurrency under false pretenses.

36. Upon information and belief, this scheme is consistent with widely documented cryptocurrency fraud typologies in which perpetrators use scripted communications, staged trading interfaces, and coordinated infrastructure to induce victims to transfer digital assets to controlled wallets.

37. After establishing trust, Doe introduced Plaintiff to a purported cryptocurrency trading platform referred to as "Rutormax."

38. The Rutormax domains and interfaces were not independent platforms, but rather constituted a unified fraudulent scheme operated through interchangeable front-end websites designed to evade detection, frustrate enforcement efforts, and continue soliciting victim deposits after prior domains were flagged or disabled.

39. The Rutormax platform did not execute legitimate trades, but instead functioned as a controlled interface that displayed fabricated account balances, fictitious trading activity, and artificial profit metrics designed to induce continued deposits.

40. Doe represented that:

- a. She had successfully used the platform for an extended period;
- b. She regularly generated substantial profits; and
- c. She had successfully withdrawn large sums without issue.

41. These representations were false.

42. The individual identifying herself as “Anais Durran” acted as an agent, promoter, and active participant in the fraudulent scheme, directing Plaintiff’s investment decisions, encouraging additional deposits, and providing false assurances regarding the legitimacy of the platform and the safety of Plaintiff’s funds.

43. Doe provided Plaintiff with specific instructions regarding when and how to transfer cryptocurrency assets, including directing Plaintiff to designated wallet addresses and guiding him through the transfer process, thereby actively facilitating the movement of Plaintiff’s assets into the fraudulent scheme.

44. In particular, Doe represented that she had successfully withdrawn substantial funds from the Rutormax platform on multiple occasions, a statement that was false and made for the purpose of inducing Plaintiff to continue transferring assets.

45. These representations were material to Plaintiff's decision-making and were specifically intended to overcome Plaintiff's hesitation and induce continued participation in the scheme.

46. As a direct result of Doe's representations and instructions, Plaintiff transferred substantial cryptocurrency assets in multiple transactions, ultimately resulting in the loss of approximately \$919,336.

B. Fake Exchange Mechanics

47. The Rutormax platform was not a legitimate trading platform but instead a fraudulent interface designed to:

- a. Induce deposits of cryptocurrency;
- b. Display fabricated account balances and trading profits; and
- c. Prevent withdrawals through pretextual "verification" requirements.

48. The Rutormax interface was designed to mimic legitimate cryptocurrency trading platforms, including the use of real-time price charts, order books, account dashboards, and transaction histories, all of which were fabricated to create the appearance of genuine trading activity.

49. At no point did Rutormax conduct legitimate cryptocurrency trading on behalf of Plaintiff. Instead, the platform functioned solely as a simulated interface designed to display fabricated balances and fictitious trading activity while directing deposited assets to wallets controlled by the perpetrators.

50. Rather than being held in a custodial account associated with a legitimate exchange, Plaintiff's deposited assets were transmitted to external blockchain wallet addresses controlled by the perpetrators, and were not retained within any verifiable trading platform.

51. The platform's displayed balances and purported profits bore no relationship to actual market activity and were entirely fabricated to induce additional deposits.

52. After Plaintiff deposited funds, the platform displayed increasing balances to create the illusion of successful trading activity.

53. The display of increasing account balances and purported profits was used to induce Plaintiff to make additional deposits, reinforcing the false belief that legitimate trading activity was occurring and that further investment would yield additional returns.

54. When Plaintiff attempted to withdraw funds, the platform demanded a \$533,000 “verification deposit” as a condition of withdrawal.

55. The demand for a \$533,000 “verification deposit” was not a legitimate compliance or regulatory requirement, but rather a pretext designed to extract additional funds from Plaintiff and prevent withdrawal of previously transferred assets.

56. Such a demand is a hallmark of cryptocurrency fraud schemes and is inconsistent with legitimate exchange or custodial practices, where withdrawals do not require substantial additional deposits.

57. At all relevant times, Doe reassured Plaintiff that:

- a. The verification requirement was legitimate;
- b. Plaintiff should follow “customer service instructions”; and
- c. Withdrawal would proceed once additional funds were deposited.

58. Even after Plaintiff expressed concern regarding the legitimacy of the platform, Doe continued to provide reassurances and instructions designed to maintain Plaintiff’s participation and prevent withdrawal of funds.

59. The communications from Doe and the responses from the purported “customer service” representatives were coordinated and mutually reinforcing, reflecting a unified scheme designed to maintain Plaintiff’s participation and prevent withdrawal of funds.

60. These statements were knowingly false and intended to induce further transfers.

C. Transfer of Funds

61. In reliance on Defendants' representations, Plaintiff transferred cryptocurrency assets with a total value of approximately \$919,336, consisting of 196.1874 Ethereum transferred through sixteen transactions and 3.03723 Bitcoin transferred through five transactions.

62. Each of these transfers was made in direct response to instructions, guidance, or inducements provided by Doe, including directions regarding when to transfer funds, the amounts to transfer, and the wallet addresses to which such transfers should be sent.

63. Each of these transactions is recorded on a public blockchain ledger and can be independently verified through transaction hashes and wallet address analysis, confirming both the amount and destination of Plaintiff's assets.

64. The blockchain records associated with these transactions identify the originating wallet addresses, destination wallet addresses, transaction timestamps, and amounts transferred, allowing for precise reconstruction of the movement of Plaintiff's assets.

65. The total value of Plaintiff's transferred assets was approximately \$919,336 at the time of transfer, representing a substantial portion of Plaintiff's available capital.

66. Plaintiff reasonably relied on Doe's representations and assurances, including her claimed personal success using the platform and her repeated encouragement to continue investing, in deciding to transfer substantial cryptocurrency assets.

67. The transfers were not isolated transactions, but rather part of an escalating pattern in which Plaintiff was encouraged to deposit increasing amounts over time, consistent with the structure of coordinated cryptocurrency investment fraud schemes.

68. The amounts transferred by Plaintiff increased over time as Doe continued to provide assurances of profitability and successful withdrawals, reflecting a deliberate escalation strategy designed to maximize the total value of assets transferred.

69. These transfers were made through blockchain transactions directed to wallet addresses associated with the fraudulent scheme.

70. Upon execution of each transaction, Plaintiff's cryptocurrency assets were irreversibly transferred to addresses outside of his control, and Plaintiff retained no ability to reverse, cancel, or recover those transfers through ordinary means.

71. These transactions are permanently recorded on public blockchain ledgers and are capable of being traced through wallet addresses and transaction hashes.

72. Plaintiff no longer has access to these funds.

73. The assets transferred by Plaintiff were specific, identifiable cryptocurrency units capable of precise tracing and recovery if preserved prior to further dissipation.

74. Because these assets remain traceable through blockchain analysis, they are capable of recovery if preserved; however, absent immediate intervention, such assets may be further transferred, converted, or dissipated beyond recovery.

D. Tracing and Location of Stolen Assets

75. Blockchain analysis demonstrates that Plaintiff's assets were transferred through a series of intermediary wallets and routed through decentralized and centralized platforms, including Tokenlon.

76. The blockchain analysis reflects a continuous and traceable flow of Plaintiff's assets from his originating wallets through intermediary addresses and into exchange-linked and platform-associated endpoints, without any break in the chain of custody.

77. The movement of Plaintiff's assets reflects a classic laundering pattern involving rapid transfers through multiple intermediary wallets prior to consolidation at exchange-linked addresses.

78. In particular, Plaintiff's Ethereum assets were transferred through intermediary wallets, including from 0x8E2a33cCCBdd8c9fCd627a75Acd1A6D283cdfF1c to 0x261299677F399D398137c7d022438D75b1c83ceF, and thereafter routed to addresses associated with Binance, including 0x4b92cC0b53E3C3F70EcF190a35E2f86a80Fc9A78, as well as through transaction pathways involving Tokenlon, including 0x7F4B435A3366Fab16627c2d0E0aB1AA55BFCAb55.

79. Upon information and belief, a portion of Plaintiff's assets were subsequently transferred to and/or laundered through accounts and wallets associated with Binance.

80. Plaintiff's Bitcoin assets followed a similar pattern, moving through intermediary wallets and ultimately being deposited into a Binance-associated address, including 1Dwv6NFLD41XGQAJLpu9QYm5TJf3PuhBsQ, further confirming the consolidation of Plaintiff's assets at exchange-linked endpoints.

81. Upon information and belief, Binance maintains custody and control over user accounts receiving Plaintiff's assets and has the ability to restrict withdrawals, freeze funds, and preserve assets pending judicial direction.

82. Binance, as a centralized exchange, maintains internal account records, user identification data, and custodial control over deposited assets, and therefore has the ability to identify the account holders associated with the relevant addresses and to freeze and preserve assets pending judicial direction.

83. Binance routinely exercises the ability to freeze accounts, restrict withdrawals, and preserve assets in response to suspected fraud or legal process, demonstrating that the requested relief is both practical and technically feasible.

84. These platforms:

- a. Facilitated the movement of stolen assets;
- b. Provided liquidity and conversion services; and
- c. Enabled the dissipation and concealment of Plaintiff's property.

85. At all relevant times, the transaction patterns exhibited clear indicia of fraud, including:

- a. Rapid movement of large sums;
- b. Multi-hop wallet transfers; and
- c. Structuring designed to evade detection.

86. Plaintiff's cryptocurrency assets are uniquely susceptible to rapid dissipation, transfer across jurisdictions, and laundering through decentralized and centralized platforms. Absent immediate judicial intervention, there is a substantial risk that the remaining traceable assets will be permanently lost.

87. The speed, anonymity, and cross-border nature of cryptocurrency transactions make post hoc recovery exceedingly difficult, if not impossible, once assets are further transferred or converted.

88. Blockchain tracing further demonstrates that Plaintiff's assets were routed through intermediary wallets and ultimately transferred, in part, to accounts and addresses associated with cryptocurrency platforms including Binance and Tokenlon, which provided the infrastructure necessary to facilitate the movement, conversion, and potential dissipation of Plaintiff's stolen assets.

89. Because Plaintiff's assets remain traceable through blockchain analysis to identifiable wallets, accounts, and transaction pathways associated with Defendants, they are capable of recovery if preserved prior to further dissipation.

CAUSES OF ACTION

I. COUNT I – CONVERSION (ALL DEFENDANTS)

90. Plaintiff repeats and realleges paragraphs 1–89.

91. Plaintiff owned and had an immediate right to possess specific, identifiable cryptocurrency assets, including 196.1874 Ethereum and 3.03723 Bitcoin, each of which is uniquely identifiable and traceable through public blockchain records, wallet addresses, and transaction hashes.

92. These assets constitute specific, segregated property, not general funds, and are capable of precise identification and recovery through blockchain analysis.

93. Defendants, directly and/or through intermediaries, wrongfully exercised dominion and control over Plaintiff's assets by receiving, routing, transferring, facilitating, converting, and/or retaining those assets without authorization and in a manner inconsistent with Plaintiff's ownership rights.

94. The movement of Plaintiff's assets through intermediary wallets and into accounts and infrastructure associated with Binance and Tokenlon constitutes the exercise of control over those assets and their disposition.

95. Upon information and belief, Defendants, including Binance, maintain custody or control over accounts and/or assets derived from Plaintiff's cryptocurrency and have the ability to restrict access to, freeze, or otherwise preserve those assets.

96. Plaintiff has been deprived of possession, use, and control of his cryptocurrency assets and has been unable to recover them.

97. Defendants' conduct was unauthorized and wrongful and has resulted in the misappropriation and continued retention of Plaintiff's property.

98. As a direct and proximate result of Defendants' conversion, Plaintiff has suffered damages in the amount of approximately \$919,336, representing the value of the converted cryptocurrency at the time of transfer.

99. The converted assets remain traceable, in whole or in part, to wallets and accounts associated with Defendants, and equity requires their preservation and return.

100. Plaintiff is entitled to all remedies available under Florida law, including damages, disgorgement, and the imposition of a constructive trust over all traceable proceeds, as well as equitable relief necessary to prevent further dissipation of the converted assets.

II. COUNT II – FRAUD (JANE DOE)

101. Plaintiff repeats and realleges paragraphs 1–89.

102. Beginning in or around September 2025 and continuing through November 2025, Defendant Jane Doe, using the name “Anais Durran,” communicated with Plaintiff via electronic messaging, including WhatsApp, and made multiple false statements of material fact.

103. Specifically, Doe represented, among other things, that:

- a. The cryptocurrency trading platform known as “Rutormax” was legitimate and engaged in real trading activity;
- b. Plaintiff's deposited assets were secure and could be withdrawn upon request;
- c. Doe herself had successfully used the platform for an extended period and had withdrawn substantial funds without issue; and
- d. Any withdrawal restrictions, including the demand for a \$533,000 “verification deposit,” were legitimate requirements necessary to access Plaintiff's funds.

104. These statements were false when made. Rutormax was not a legitimate trading platform, did not conduct real trading activity, and did not permit genuine withdrawals of customer funds.

105. Doe knew these statements were false or made them with reckless disregard for their truth, including by continuing to make such representations after Plaintiff encountered withdrawal restrictions and expressed concerns regarding the legitimacy of the platform.

106. Doe made these misrepresentations with the intent to induce Plaintiff to transfer cryptocurrency assets and to continue making additional deposits into the fraudulent scheme.

107. Plaintiff reasonably and justifiably relied on Doe's representations, including her claimed personal success with the platform and her repeated assurances regarding withdrawals, in deciding to transfer substantial cryptocurrency assets.

108. Plaintiff's reliance was reasonable under the circumstances, including in light of Doe's sustained communications, relationship-building efforts, and repeated reassurances designed to overcome Plaintiff's skepticism.

109. In reliance on these misrepresentations, Plaintiff transferred cryptocurrency assets totaling approximately \$919,336, consisting of 196.1874 Ethereum transferred through sixteen transactions and 3.03723 Bitcoin transferred through five transactions.

110. As a direct and proximate result of Doe's fraudulent conduct, Plaintiff has suffered damages in the amount of approximately \$919,336, representing the value of the cryptocurrency assets transferred and lost.

111. Doe's conduct was willful, malicious, and undertaken with the intent to defraud Plaintiff, entitling Plaintiff to all available legal and equitable relief.

III. COUNT III – CONSTRUCTIVE TRUST (ALL DEFENDANTS)

112. Plaintiff repeats and realleges paragraphs 1–89.

113. Plaintiff transferred specific, identifiable cryptocurrency assets, including 196.1874 Ethereum and 3.03723 Bitcoin, in reliance on representations that such assets would be held, invested, and made available for withdrawal.

114. These assets constitute specific, segregated, and traceable property, identifiable through public blockchain records, including wallet addresses, transaction hashes, and transfer histories.

115. Blockchain tracing demonstrates that Plaintiff's assets were transferred through a series of intermediary wallets and ultimately routed, in whole or in part, to wallets, accounts, and transaction pathways associated with Defendants, including Binance and Tokenlon.

116. Upon information and belief, a portion of Plaintiff's assets, or proceeds thereof, were transferred to and/or through cryptocurrency addresses associated with Binance, a centralized exchange that maintains custody and control over user accounts and deposited assets.

117. Binance possesses, controls, or has the ability to identify accounts holding assets derived from Plaintiff's cryptocurrency and has the technical capability to freeze funds, restrict withdrawals, and preserve assets pending judicial direction.

118. To the extent Binance holds, controls, or has custody over assets traceable to Plaintiff's transfers, it holds such assets under circumstances in which it would be inequitable and contrary to principles of justice and good conscience to permit retention of those assets or the benefits derived therefrom.

119. Plaintiff's assets were also routed, in whole or in part, through Tokenlon, which provides decentralized routing, execution, and liquidity infrastructure used to facilitate cryptocurrency transactions.

120. Upon information and belief, Tokenlon facilitated, processed, and/or participated in the transfer, routing, and conversion of Plaintiff's cryptocurrency assets, including through routing mechanisms, smart contract execution, liquidity pools, and related infrastructure.

121. Upon further information and belief, to the extent Plaintiff's assets were routed through Tokenlon's infrastructure, such assets or their proceeds may remain within, be associated with, or be recoverable through wallets, smart contracts, liquidity pools, or accounts connected to or accessible through Tokenlon.

122. To the extent Tokenlon possesses, controls, has access to, or facilitated the conversion of assets traceable to Plaintiff's cryptocurrency, it has retained or derived benefits—including transaction fees, liquidity participation, or execution-related gains—under circumstances rendering such retention inequitable.

123. Defendants have obtained, possessed, controlled, or facilitated the transfer and disposition of Plaintiff's cryptocurrency assets under circumstances involving fraud, deception, and inequitable conduct.

124. Plaintiff has been deprived of his property, while Defendants have retained possession, control, access to, or benefits derived from assets and proceeds that are directly traceable to Plaintiff's transfers.

125. Under these circumstances, it would be inequitable and contrary to principles of justice and good conscience to permit Defendants to retain the benefit of Plaintiff's property.

126. Equity therefore requires the imposition of a constructive trust over all cryptocurrency assets, funds, and proceeds traceable to Plaintiff's transfers, wherever located and in whatever form they currently exist.

127. Plaintiff is entitled to an order imposing a constructive trust and directing that all such traceable assets be identified, preserved, accounted for, and ultimately returned to Plaintiff.

IV. COUNT IV – UNJUST ENRICHMENT (TOKENLON & BINANCE)

128. Plaintiff repeats and realleges paragraphs 1–89.

129. Plaintiff conferred a direct and/or indirect benefit upon Defendants by transferring cryptocurrency assets—specifically 196.1874 Ethereum and 3.03723 Bitcoin, valued at approximately \$919,336—which were subsequently received, routed, processed, converted, and/or otherwise handled through infrastructure associated with Defendants.

130. These assets, and the proceeds thereof, were transmitted through identifiable blockchain transactions and are traceable, in whole or in part, to wallets, accounts, liquidity pools, or transaction pathways associated with Binance and Tokenlon.

131. Upon information and belief, a portion of Plaintiff's assets, or proceeds thereof, were transferred to and/or through cryptocurrency addresses associated with Binance, which operates as a centralized exchange and custodian of digital assets.

132. Binance received and retained benefits in connection with these transactions, including but not limited to trading fees, transaction fees, custody-related benefits, and the use of Plaintiff's assets within its platform ecosystem.

133. To the extent Binance holds, controls, or has custody over assets traceable to Plaintiff's cryptocurrency, it has also received the benefit of those assets themselves.

134. Plaintiff's assets were also routed, in whole or in part, through Tokenlon, which provides decentralized routing, execution, and liquidity infrastructure for cryptocurrency transactions.

135. Through its routing, execution, and liquidity functions, Tokenlon received benefits from Plaintiff's assets, including transaction fees, routing fees, liquidity participation, and execution-related gains associated with the transfer and conversion of those assets.

136. Upon information and belief, Plaintiff's assets or their proceeds may remain within, be associated with, or be recoverable through wallets, smart contracts, or liquidity pools connected to or accessible through Tokenlon's infrastructure.

137. Defendants knowingly accepted and retained these benefits under circumstances in which it would be inequitable to permit them to retain such benefits without compensating Plaintiff.

138. Plaintiff has been deprived of his cryptocurrency assets, while Defendants have retained the benefits derived from those assets and their transfer, conversion, and/or custody.

139. Defendants' retention of these benefits is unjust, as the underlying transfers were induced by fraud and resulted in the wrongful diversion of Plaintiff's property.

140. Under Florida law, Defendants are obligated to disgorge all benefits unjustly obtained from Plaintiff's assets.

141. Plaintiff is entitled to restitution, disgorgement, and all equitable relief necessary to prevent Defendants' continued unjust enrichment, including the return of all assets and proceeds traceable to Plaintiff's transfers.

V. COUNT V – AIDING AND ABETTING CONVERSION (TOKENLON & BINANCE)

142. Plaintiff repeats and realleges paragraphs 1–89.

143. As set forth above, an underlying conversion occurred in which Plaintiff's specific, identifiable cryptocurrency assets—including 196.1874 Ethereum and 3.03723 Bitcoin—were wrongfully transferred and misappropriated without Plaintiff's authorization.

144. Upon information and belief, Defendants Binance and Tokenlon had actual knowledge of the underlying conversion, or were willfully blind to it, as demonstrated by the nature, structure, and pattern of the transactions at issue.

145. Defendants' knowledge may be inferred from, inter alia:

- a. The rapid movement of large-value cryptocurrency transfers through multiple intermediary wallets;
- b. The use of multi-hop transactions designed to obscure the origin of funds;
- c. Transaction patterns consistent with widely recognized cryptocurrency fraud schemes, including "pig butchering" scams;
- d. The size, frequency, and structure of the transactions relative to ordinary user activity; and
- e. Defendants' own monitoring capabilities, including blockchain analytics, transaction surveillance systems, and anti-money laundering controls.

146. Despite these indicia of fraudulent activity, Defendants processed, routed, facilitated, and/or failed to halt the transfer and conversion of Plaintiff's assets.

147. Defendant Binance substantially assisted in the conversion by receiving deposits of Plaintiff's cryptocurrency into exchange-linked addresses, maintaining custody and control over those assets, and providing the infrastructure necessary to transfer, convert, or withdraw those assets.

148. Binance's services were a necessary and integral component of the conversion, as they enabled the consolidation, custody, and potential dissipation of Plaintiff's assets.

149. Upon information and belief, Binance had the ability to restrict withdrawals, freeze accounts, and preserve assets associated with Plaintiff's cryptocurrency, yet failed to do so.

150. Defendant Tokenlon substantially assisted in the conversion by facilitating the routing, execution, and/or conversion of Plaintiff's cryptocurrency through its decentralized infrastructure, including routing mechanisms, smart contract execution, and liquidity pools.

151. Tokenlon's services enabled the movement, conversion, and potential concealment of Plaintiff's assets and were an integral component of the transaction pathway through which those assets were transferred.

152. Upon information and belief, Tokenlon's infrastructure was used to process transactions involving Plaintiff's assets despite the presence of indicia of fraudulent activity.

153. Defendants' knowing participation and substantial assistance in the transfer, routing, and conversion of Plaintiff's cryptocurrency directly and proximately caused Plaintiff's loss of control and possession of his assets.

154. As a result of Defendants' conduct, Plaintiff has suffered damages in the amount of approximately \$919,336, representing the value of the converted cryptocurrency at the time of transfer.

155. By knowingly and substantially assisting in the conversion of Plaintiff's assets, Defendants Binance and Tokenlon are liable for aiding and abetting conversion under Florida law.

VI. COUNT VI – PRELIMINARY INJUNCTION / EQUITABLE RELIEF (TOKENLON & BINANCE)

156. Plaintiff repeats and realleges paragraphs 1–89.

157. Plaintiff is likely to succeed on the merits of his claims, including conversion, fraud, and constructive trust, because the cryptocurrency assets at issue are specific, identifiable, and traceable through publicly verifiable blockchain transactions.

158. Blockchain analysis demonstrates a clear and continuous flow of Plaintiff's assets from his originating wallets through intermediary addresses and into accounts and transaction pathways associated with Defendants.

159. With respect to Ethereum, approximately 196.1874 ETH was transferred through a series of wallets, including from 0x8E2a33cCCBdd8c9fCd627a75Acd1A6D283cdfF1c to 0x261299677F399D398137c7d022438D75b1c83ceF, and thereafter routed to addresses associated with Binance, including 0x4b92cC0b53E3C3F70EcF190a35E2f86a80Fc9A78, as well as

through Tokenlon infrastructure, including 0x7F4B435A3366Fab16627c2d0E0aB1AA55BFCAb55.

160. With respect to Bitcoin, Plaintiff's assets were transferred through intermediary wallets and ultimately deposited into a Binance-associated address, including 1Dwv6NFLD41XGQAJLpu9QYm5TJf3PuhBsQ, reflecting a consistent pattern of movement from Plaintiff's control to exchange-linked endpoints.

161. These transactions are recorded on immutable public ledgers and confirm that Plaintiff's assets are traceable, identifiable, and capable of recovery if preserved.

162. Plaintiff will suffer immediate and irreparable harm absent injunctive relief.

163. Cryptocurrency assets are uniquely susceptible to rapid transfer, concealment, and dissipation across wallets, platforms, and jurisdictions, often within minutes.

164. The multi-hop transfer patterns already reflected in the blockchain demonstrate that dissipation is ongoing and not speculative.

165. Once further transferred, converted, or commingled, Plaintiff's assets will likely become permanently unrecoverable, and monetary damages alone will be inadequate to remedy such loss.

166. The balance of equities strongly favors Plaintiff.

167. Plaintiff has lost approximately \$919,336 in cryptocurrency assets and faces the imminent risk of permanent loss.

168. By contrast, the requested relief imposes only a narrow and temporary burden on Defendants, requiring the preservation of assets already within their custody, control, or infrastructure.

169. Such relief does not require adjudication of ultimate liability, but merely preserves the status quo pending resolution of Plaintiff's claims.

170. The requested injunction serves the public interest by preventing the laundering and dissipation of stolen digital assets and promoting the integrity and accountability of cryptocurrency markets.

171. Courts have a strong interest in preserving identifiable property and preventing the misuse of financial infrastructure to facilitate fraud.

172. Defendant Binance, as a centralized exchange, maintains custody and control over user accounts receiving cryptocurrency deposits and has the technical ability to freeze assets, restrict withdrawals, and preserve account data.

173. Defendant Tokenlon, through its routing, execution, and liquidity infrastructure, facilitated the transfer and potential conversion of Plaintiff's assets and, upon information and belief, may provide access to or be associated with wallets, smart contracts, or liquidity pools containing traceable proceeds.

174. The requested relief is therefore technologically feasible and capable of immediate implementation, at least with respect to assets within Binance's custody and, to the extent applicable, assets accessible through Tokenlon's infrastructure.

175. Plaintiff seeks a preliminary injunction and equitable relief:

- a. Freezing all cryptocurrency assets, funds, and proceeds traceable to Plaintiff's transfers, including those held in or associated with Binance accounts and Tokenlon-related wallets, contracts, or liquidity pools;
- b. Prohibiting Defendants from transferring, dissipating, converting, or otherwise disposing of such assets;
- c. Requiring Defendants to identify, preserve, and maintain all accounts, wallets, smart contracts, transaction records, and user information associated with such assets; and

- d. Granting such further equitable relief as necessary to preserve Plaintiff's property pending adjudication of this action.

VII. COUNT VII – DECLARATORY RELIEF

176. Plaintiff repeats and realleges paragraphs 1–89.

177. This is an action for declaratory relief pursuant to Chapter 86, Florida Statutes, seeking a judicial determination of the parties' rights and interests in specific, identifiable cryptocurrency assets and their traceable proceeds.

178. An actual, present, and justiciable controversy exists between Plaintiff and Defendants concerning the ownership, control, and disposition of cryptocurrency assets transferred from Plaintiff's wallets and subsequently traced to accounts, addresses, and transaction pathways associated with Defendants.

179. Plaintiff contends that he is the rightful owner of cryptocurrency assets, including 196.1874 Ethereum and 3.03723 Bitcoin, and all proceeds traceable thereto, which were wrongfully transferred and remain identifiable through blockchain analysis.

180. Plaintiff further contends that Defendants have no lawful ownership interest in such assets and have no right to retain, transfer, convert, or otherwise exercise dominion over them.

181. Upon information and belief, Defendant Binance maintains custody or control over accounts holding assets traceable to Plaintiff's cryptocurrency and has the ability to identify, restrict, and preserve such assets.

182. Upon information and belief, Defendant Tokenlon, through its routing, execution, and liquidity infrastructure, facilitated the transfer and potential conversion of Plaintiff's assets and may be associated with or provide access to wallets, smart contracts, or liquidity pools containing traceable proceeds.

183. A judicial declaration is necessary and appropriate to determine:

- a. That Plaintiff is the lawful owner of all cryptocurrency assets and proceeds traceable to his transfers;
- b. That such assets constitute specific, identifiable property subject to recovery;
- c. That Defendants have no lawful ownership or superior claim to such assets; and
- d. That Defendants are required to preserve, identify, and refrain from transferring such assets pending further proceedings.

184. Without such declaratory relief, uncertainty will persist regarding the parties' rights and obligations, and Plaintiff will be prejudiced in his ability to recover and protect his property.

185. Plaintiff is therefore entitled to a declaration of rights consistent with the foregoing, together with such further relief as the Court deems just and proper.

PRAYER FOR RELIEF

186. WHEREFORE, Plaintiff respectfully requests that this Court:

- a. Issue a temporary, preliminary, and permanent injunction:
 - (i) Freezing all cryptocurrency assets, funds, and proceeds traceable to Plaintiff's transfers, including but not limited to assets held in, associated with, or accessible through:
 - (1) Binance accounts and deposit addresses, including but not limited to 0x4b92cC0b53E3C3F70EcF190a35E2f86a80Fc9A78 and 1Dwv6NFLD41XGQAjLpu9QYm5TJf3PuhBsQ; and
 - (2) Tokenlon-related wallets, smart contracts, routing pathways, and liquidity pools;
 - (ii) Prohibiting Defendants, and any persons or entities acting in concert with them, from transferring, dissipating, converting, withdrawing, or otherwise disposing of such assets;
 - (iii) Requiring Defendants to identify, locate, and preserve all accounts, wallets, smart contracts, and assets traceable to Plaintiff's cryptocurrency;

- (iv) Requiring Defendants to preserve and maintain all books, records, account information, communications, and transaction data relating to such assets;
- b. Impose a constructive trust over all cryptocurrency assets, funds, and proceeds traceable to Plaintiff's transfers, wherever located and in whatever form they currently exist, and order that such assets be returned to Plaintiff;
- c. Award Plaintiff compensatory damages in the amount of approximately \$919,336, representing the value of the converted cryptocurrency at the time of transfer, or such greater amount as may be proven at trial;
- d. Award damages against Defendant Jane Doe for fraud, including all available legal and equitable relief;
- e. Order Defendants to disgorge all fees, profits, and benefits derived from Plaintiff's assets, including but not limited to:
 - (i) transaction fees
 - (ii) routing fees
 - (iii) liquidity participation
 - (iv) execution-related gains
- f. Award restitution of all amounts unjustly retained by Defendants;
- g. Enter a declaratory judgment that:
 - (i) Plaintiff is the lawful owner of all cryptocurrency assets and proceeds traceable to his transfers;
 - (ii) Such assets constitute specific, identifiable property subject to recovery;
 - (iii) Defendants have no lawful ownership interest in such assets; and
 - (iv) Defendants are required to preserve and refrain from transferring such assets pending final resolution of this action;
- h. Order Defendants to provide a full accounting of all transactions involving Plaintiff's assets, including:
 - (i) wallet addresses
 - (ii) account identifiers
 - (iii) transaction histories

- (iv) counterparties
- (v) balances and transfers
- i. Award Plaintiff his costs of suit, and such attorneys' fees as permitted by law; and
- j. Grant such other and further legal and equitable relief as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

ZOELLER, HAYDEN &
THRON, PLLC.
Attorneys for Plaintiff
2845 PGA Blvd.
Palm Beach Gardens, FL 33410
(561) 689-8180

By: /s/ Phillip W. Thron, Esq.
PHILLIP W. THRON
Fla. Bar No.: 165964
pthron@zoellerlaw.com
ckincaid@zoellerlaw.com
apaltin@zoellerlaw.com

T. Liam Murphy, Esq.
N.Y. Bar # 5853759
**MURPHY'S LAW: THE
CRYPTO LAW FIRM**
murphyslawcrypto.com
353 Lexington Avenue
4th Floor, Suite 400
New York, New York 10016
liam@murphyslawcrypto.com
(913) 575-0540

Counsel for Plaintiff