

**IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT
IN AND FOR MIAMI-DADE COUNTY, FLORIDA**

ANTHONY APOLLO,

Plaintiff,

v.

JOHN DOES 1-25,

Defendants.

COMPLAINT

Plaintiff ANTHONY APOLLO (“Plaintiff” or “Apollo”), by and through his undersigned counsel, hereby sues Defendant JOHN DOES 1-25 (“Defendants”), and alleges as follows:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff ANTHONY APOLLO is an individual residing in Miami-Dade County.
2. At all times material hereto, Plaintiff owned and controlled the Bitcoin (“BTC”) and Ethereum (“ETH”) digital assets that are the subject of this action.
3. Defendants are individuals whose identities are presently unknown. Defendants participated in, directed, carried out, and/or benefitted from the fraudulent scheme described herein, including the unauthorized access to and theft of Plaintiff’s digital assets and the subsequent transfer, concealment, and movement of those assets and their proceeds.
4. Defendants’ identities are presently unknown to Plaintiff because Defendants utilized false identities, impersonated legitimate technology and cryptocurrency service providers,

and utilized cryptocurrency wallets and accounts that do not publicly disclose the identity of their owners or users.

5. Plaintiff's stolen digital assets were transferred through a series of cryptocurrency wallets and transactions following the unauthorized removal of the assets from Plaintiff's wallets. Through blockchain forensic analysis, portions of Plaintiff's stolen BTC and ETH have been traced to deposit addresses associated with cryptocurrency exchanges and digital asset service providers.
6. Specifically, the investigation has identified the following exchange and service-provider deposit addresses through which assets attributable to Plaintiff were transferred:

- **Coinbase (BTC):** 35FQsfKkSFbBCZGT2YEnYpwW9Q6tR4MGbL
- **Binance (ETH):** 0x3e45f96400dac2cbd0eaf213d2d726f1b65cf0b8
- **Binance (ETH):** 0xd0e83490a55e671b3cf39cd027f0f9035ec5a1ef
- **Binance (ETH):** 0x8c349a9347933aee850574244f849a4030a9f65c
- **MEXC (ETH):** 0x1fee6ec9bee894187f1b2ca15b5ca19db32a0fbf
- **KuCoin (ETH):** 0x607d7a7a12ca3442fb8e63e253d393d4e47cf199
- **KuCoin (ETH):** 0x03e62af9add6195fd4a4d8d259a1bafdfc3b11eb
- **Cryptomus (ETH):** 0x57e547304ef1eb61935f250f667691acbf7f0057
- **Swapuz (ETH):** 0x283edf0f2abc65a19ad7a0e72ea322c118f3flac

7. Upon information and belief, the foregoing cryptocurrency exchanges and digital asset service providers maintain information concerning the accounts associated with these deposit addresses, including information capable of identifying the persons or entities that

received, possessed, transferred, or exercised control over assets traceable to Plaintiff's stolen cryptocurrency.

8. Plaintiff has commenced an investigation into the theft and subsequent movement of his digital assets through Inca Digital.
9. That investigation has identified blockchain transactions, cryptocurrency wallet addresses, and accounts and infrastructure associated with third-party cryptocurrency exchanges and services through which assets traceable to Plaintiff's stolen cryptocurrency were transferred.
10. This action seeks damages in excess of \$50,000.00, exclusive of interest, attorneys' fees, and costs, and is otherwise within the subject matter jurisdiction of this Court.
11. Plaintiff has retained the undersigned counsel and is required to pay reasonable attorneys' fees.

STATEMENT OF FACTS

The Fraudulent Scheme

12. On August 2, 2026, Plaintiff received several security alerts concerning attempts to access and/or reset the password associated with his personal Google account.
13. By the time Plaintiff reviewed the alerts and attempted to deny the unauthorized activity, the alerts had expired.
14. On the morning of August 3, 2026, Plaintiff received additional indications of attempted unauthorized access to his Google account and, in response, reset his password.
15. At approximately 11:34 a.m. Mountain Time that same day, Plaintiff received a telephone call from an individual purporting to be a representative of Google and identifying himself as "Brian Manley."

16. The incoming call appeared on Plaintiff's telephone as originating from "Google" and displayed a verified checkmark, giving the call the appearance of legitimacy.
17. The purported Google representative informed Plaintiff that his Google account, including his Gmail and Google Drive, had been compromised through an unauthorized "App Password" associated with a service identified as "Nifty Crypto."
18. The purported Google representative further represented that an individual identified as "Nirit" had obtained unauthorized access to Plaintiff's Google account and purported to assist Plaintiff in removing that access and securing his account.
19. As part of the purported account-recovery process, Plaintiff received a recovery email appearing to originate from Google at noreply@google.com and containing a code to establish a recovery email.
20. At approximately the same time, Plaintiff received an additional security communication appearing to originate from Google at no-reply@accounts.google.com. The communication concerned the email address "nirit.x.reichman@gmail.com" and directed Plaintiff to a webpage hosted at sites.google.com in connection with the purported Google support process.
21. Because the communications appeared to originate from legitimate Google email addresses, were received contemporaneously with the telephone call, and related directly to the security compromise being described by the caller, Plaintiff believed that he was participating in a legitimate Google account-recovery process.
22. During the ensuing communications, the purported Google representative described features of Google's Advanced Protection Program and represented that Google

maintained an advanced support feature through which certain deleted communications associated with the purported compromise could be identified.

23. The purported Google representative further informed Plaintiff that attempts had been made to access several of Plaintiff's other accounts, including accounts associated with Kraken, Gemini, and Ledger.

24. The purported Google representative advised Plaintiff that an incident report concerning the compromise would be provided and that representatives of other affected service providers might contact Plaintiff regarding the security incident.

The Purported Ledger Representative and Compromise

25. At approximately 12:14 p.m. Mountain Time on August 3, 2026, Plaintiff received a telephone call from an individual purporting to be a representative of Ledger and identifying himself as "Alexander Robins."

26. Plaintiff also received an email concerning the purported assignment of "Alexander Robins" to assist with the security incident. The email appeared to originate from Ledger at support@ledger.com.

27. The purported Ledger representative informed Plaintiff that the compromise of Plaintiff's Google account may have resulted in the disclosure of information associated with Plaintiff's cryptocurrency wallet through the "Ledger Recover" process.

28. The caller possessed specific information concerning Plaintiff and his cryptocurrency holdings and security devices, including Plaintiff's Social Security number, identification information, an Ethereum public wallet address ending in "-cdfc," and the model of Plaintiff's Ledger hardware device.

29. The caller also referenced the existence of a second Ledger device associated with Plaintiff's account, despite Plaintiff not having previously disclosed the existence of that device during the conversation.
30. The purported Ledger representative informed Plaintiff that the information already possessed by the alleged attacker created a significant risk that Plaintiff's private keys had been compromised.
31. The caller further represented that, if Plaintiff could verify the compromise through the purported Google support process, Ledger would provide insurance coverage for any resulting loss and provide Plaintiff with a replacement device.
32. As part of the purported verification process, the caller instructed Plaintiff to use the previously referenced Google support webpage and enter information associated with Plaintiff's wallet recovery phrase into the "Describe your issue" field.
33. Plaintiff did not provide his complete recovery phrase.
34. Plaintiff initially entered four of the twenty-four words comprising his recovery phrase into the webpage, but received no response. Plaintiff thereafter attempted six words, again without receiving a response.
35. The purported Ledger representative then instructed Plaintiff to enter only the first few letters of each word comprising the recovery phrase.
36. Believing that providing only limited portions of the recovery phrase would not be sufficient to compromise his wallet, and believing that he was participating in the security-verification process described by the purported Google and Ledger representatives, Plaintiff followed the instruction and entered the first few letters of the words into the webpage.

37. Shortly thereafter, while Plaintiff was independently attempting to secure and relocate his cryptocurrency holdings, Plaintiff discovered that his wallet had been compromised and that unauthorized transfers of his digital assets were underway.

The Unauthorized Transfer and Theft of Plaintiff's Digital Assets

38. At approximately 12:57 p.m. Mountain Time on August 3, 2026, Plaintiff observed through the Ledger Live application that an unauthorized Bitcoin transaction had been initiated from his wallet.

39. Plaintiff immediately attempted to cancel the transaction through the functionality available within the Ledger Live application, but was unable to stop or reverse the transfer.

40. Plaintiff immediately informed the purported Ledger representative of the unauthorized transaction. The purported Ledger representative told Plaintiff to expect an email concerning insurance coverage and then abruptly terminated the telephone call.

41. Recognizing that his cryptocurrency holdings were being compromised, Plaintiff immediately attempted to transfer approximately 69 ETH from his Ethereum wallet ending in “-cdfc” to a separate MetaMask wallet under his control.

42. Before Plaintiff could complete that transfer, Plaintiff's ETH was likewise transferred from his wallet without his authorization.

43. As a result of the unauthorized transactions, approximately 1.1 BTC and approximately 69 ETH belonging to Plaintiff were removed from wallets under Plaintiff's control.

44. The principal unauthorized Bitcoin transaction is recorded on the Bitcoin blockchain under the following transaction hash:

f515a501048ce072ccc16f40e3309f10d3827b4ef8b9f6c1f17b41a80f46f9a0

45. The principal unauthorized Ethereum transaction is recorded on the Ethereum blockchain under the following transaction hash:

0xd237d032b9a7730f345808eeaab4db67d074bfc4447e124c56b442ca1cd7bb4c

46. An additional unauthorized Ethereum transaction associated with the draining of Plaintiff's wallet is recorded under the following transaction hash:

0x609b2a8df8ff04013e9b82783cc1d075b9221e8482b6800a546190c85fc92825

47. Plaintiff did not authorize Defendant or any other person involved in the fraudulent scheme to transfer, receive, possess, or exercise control over his BTC or ETH, and Plaintiff received no consideration in exchange for the unauthorized transfers.

48. Immediately following the unauthorized transfers, Plaintiff attempted to contact the telephone number used by the purported Ledger representative, but the number had been disconnected.

49. Plaintiff also attempted to contact the telephone number used by the purported Google representative. The call initially resulted only in static, after which Plaintiff received a return call from an individual claiming to be associated with Google Ads. Plaintiff terminated the call.

50. Plaintiff thereafter undertook efforts to investigate the theft, trace the movement of his stolen digital assets, and identify the individual or individuals responsible for the fraudulent scheme.

The Forensic Investigation and Tracing of the Stolen Assets

51. Following discovery of the unauthorized transfers, Plaintiff commenced an investigation into the theft and subsequent movement of his stolen digital assets.

52. As part of that investigation, blockchain forensic analysis was conducted to identify wallets involved in the unauthorized transfers, trace the subsequent movement of Plaintiff's stolen BTC and ETH, and identify destinations to which assets attributable to Plaintiff were ultimately transferred.
53. Transactions involving Bitcoin and Ethereum are recorded on their respective public blockchains, creating a record through which transfers of digital assets may be traced between wallet addresses.
54. Through blockchain forensic analysis, the movement of Plaintiff's stolen digital assets was reconstructed through a series of intermediary wallets and subsequent transactions.
55. The investigation revealed that Defendant did not simply retain Plaintiff's stolen digital assets in the wallets to which they were initially transferred. Instead, the stolen assets were subsequently moved through additional cryptocurrency wallets and transactions.
56. The investigation identified multiple wallets used in connection with the subsequent movement of Plaintiff's stolen BTC and ETH, including wallets characterized in the forensic analysis as attacker-controlled, holding, staging, and pass-through wallets.
57. Despite the movement of Plaintiff's stolen assets through intermediary wallets and transactions, the forensic analysis was able to trace portions of those assets to deposit addresses associated with centralized cryptocurrency exchanges and other digital asset service providers.
58. Specifically, the investigation traced BTC attributable to Plaintiff to a deposit address associated with Coinbase and ETH attributable to Plaintiff to deposit addresses associated with Binance, MEXC, KuCoin, Cryptomus, and Swapuz.

59. The investigation traced approximately 0.558243 BTC attributable to Plaintiff to the following Coinbase deposit address: 35FQsfKkSFbBCZGT2YEnYpwW9Q6tR4MGbL

60. The investigation further traced ETH attributable to Plaintiff to the following Binance deposit addresses:

0x3e45f96400dac2cbd0eaf213d2d726f1b65cf0b8

0xd0e83490a55e671b3cf39cd027f0f9035ec5a1ef

0x8c349a9347933ace850574244f849a4030a9f65c

61. According to the forensic analysis, approximately 0.94550899 ETH, 2.83652263 ETH, and 1.04005989 ETH, respectively, attributable to Plaintiff were transferred to the foregoing Binance deposit addresses.

62. The investigation traced approximately 2.83652544 ETH attributable to Plaintiff to the following MEXC deposit address: 0x1fee6ec9bee894187f1b2ca15b5ca19db32a0fbf

63. The investigation traced approximately 2.69751007 ETH attributable to Plaintiff to the following KuCoin deposit address: 0x607d7a7a12ca3442fb8e63e253d393d4e47cf199

64. The investigation traced approximately 0.05059011 ETH attributable to Plaintiff to the following Cryptomus deposit address: 0x57e547304ef1eb61935f250f667691acbf7f0057

65. The investigation traced approximately 0.05332 ETH attributable to Plaintiff to the following Swapuz deposit address: 0x283edf0f2abc65a19ad7a0e72ea322c118f3flac

66. The foregoing tracing demonstrates that portions of Plaintiff's stolen digital assets were transferred into deposit addresses associated with identifiable cryptocurrency exchanges and digital asset service providers.

67. Upon information and belief, the exchanges and service providers associated with the identified deposit addresses maintain account and transaction records capable of identifying the account holders who received the assets, including Know Your Customer (“KYC”) information, account registration information, transaction histories, withdrawal records, login information, IP addresses, device identifiers, and related account activity.
68. Upon information and belief, such records are capable of identifying Defendant and/or other persons or entities who received, transferred, possessed, or exercised control over Plaintiff’s stolen digital assets and the proceeds thereof.
69. Plaintiff’s stolen digital assets and proceeds derived therefrom remain subject to further transfer, withdrawal, conversion, or dissipation, which threatens Plaintiff’s ability to identify and recover his property.
70. As described above, the forensic investigation has traced portions of Plaintiff’s stolen assets to identifiable cryptocurrency exchange and digital asset service-provider deposit addresses. Because digital assets can be transferred rapidly and across multiple wallets and platforms, the assets and proceeds traceable to Plaintiff’s stolen cryptocurrency are subject to further transfer or dissipation.
71. Preservation of the traceable assets and proceeds is therefore necessary to prevent further dissipation and to preserve Plaintiff’s ability to recover his property pending identification of Defendant and resolution of this action.
72. All conditions precedent to bringing this action have occurred, have been performed, or have otherwise been waived.
73. Plaintiff retained the undersigned counsel to represent them in this matter and have and will incur reasonable attorneys’ fees and costs.

COUNT I
CONVERSION
(Against Defendants)

74. Plaintiff re-alleges and incorporates paragraphs 1 through 73 as if fully set forth herein.
75. At all times material hereto, Plaintiff was the lawful owner of, and had the immediate right to possess and control, the BTC and ETH described in this Complaint.
76. The digital assets at issue constitute specific and identifiable property capable of ownership, possession, tracing, recovery, and return.
77. Defendants intentionally and wrongfully obtained and exercised dominion and control over Plaintiff's digital assets without Plaintiff's authorization or consent.
78. Defendants' exercise of dominion and control over Plaintiff's digital assets was inconsistent with and in derogation of Plaintiff's ownership and possessory rights.
79. Following the unauthorized transfers, Defendant transferred, concealed, retained, and otherwise exercised control over Plaintiff's stolen digital assets and proceeds derived therefrom.
80. As alleged above, blockchain forensic analysis has traced portions of Plaintiff's stolen digital assets through intermediary wallets and transactions to identifiable cryptocurrency exchange and digital asset service-provider deposit addresses.

81. Plaintiff never authorized Defendants to possess, transfer, dispose of, or otherwise exercise control over the stolen digital assets.

82. Defendants' unauthorized taking and exercise of dominion and control over Plaintiff's digital assets constitutes conversion.

83. As a direct and proximate result of Defendants' conversion, Plaintiff has suffered damages, including the loss of approximately 1.1 BTC and 69 ETH, in an amount to be proven at trial.

WHEREFORE, Plaintiff ANTHONY APOLLO, respectfully requests that this Court enter judgment in his favor and against Defendants JOHN DOES 1-25, award compensatory damages in an amount to be proven at trial, prejudgment interest, taxable costs, and all other relief available under law and equity.

COUNT II
DECLARATORY JUDGMENT
(Against Defendants)

82. Plaintiff re-alleges and incorporates Paragraphs 1 through 73 as if fully set forth herein.

83. This is an action for declaratory relief pursuant to Chapter 86, Florida Statutes.

84. A bona fide, actual, present, and practical need exists for a judicial declaration concerning the ownership, possession, control, and disposition of the digital assets and proceeds traceable to the unauthorized transfers described herein.

85. Plaintiff contends that the stolen digital assets and identifiable proceeds derived therefrom belong to Plaintiff and that Plaintiff's ownership interest in such assets is superior to any interest claimed by Defendants.

86. Defendants have exercised possession, dominion, and control over Plaintiff's stolen digital assets and/or proceeds derived therefrom in a manner directly adverse to Plaintiff's ownership rights.

87. As alleged above, Plaintiff's investigation has traced portions of the stolen digital assets through intermediary wallets and transactions to identifiable cryptocurrency exchange and digital asset service-provider deposit addresses.

88. An actual controversy therefore exists concerning the ownership, possession, control, and disposition of the stolen digital assets and identifiable proceeds derived therefrom.

89. Plaintiff contends that all identifiable assets traceable to his stolen BTC and ETH, together with any identifiable proceeds, substitutions, derivatives, or property acquired therefrom, are subject to Plaintiff's superior ownership and possessory rights.

90. Defendants' interests in the stolen assets are adverse and directly contrary to Plaintiff's ownership rights.

91. A judicial declaration is necessary to determine the parties' respective ownership and possessory rights and facilitate the recovery and return of Plaintiff's stolen property.

WHEREFORE, Plaintiff ANTHONY APOLLO, respectfully requests that this Court enter a declaratory judgment determining that: (a) Plaintiff possesses the superior ownership interest in the stolen digital assets and identifiable assets and proceeds traceable thereto; (b) Defendants possess no lawful ownership interest in such assets; (c) any identifiable assets, proceeds, substitutions, or derivative property traceable to Plaintiff's stolen BTC and ETH are subject to Plaintiff's superior ownership rights; and (d) Plaintiff is entitled to recover such assets and proceeds, together with such other and further relief as the Court deems just and proper.

COUNT III
REQUEST FOR INJUNCTIVE RELIEF
(Against Defendants)

92. Plaintiff re-alleges and incorporates Paragraphs 1 through 73 as if fully set forth herein.

92. Plaintiff requests an injunction freezing and preserving all accounts associated with the cryptocurrency exchange and digital asset service-provider deposit addresses identified herein to the extent such accounts contain Plaintiff's stolen digital assets or proceeds traceable thereto.

93. Such a freeze is necessary to preserve the possibility of restitution and recovery of Plaintiff's stolen property.

94. Plaintiff has no adequate remedy at law to prevent the further transfer or dissipation of the specific and identifiable digital assets and proceeds traceable to his stolen cryptocurrency.

95. Plaintiff will suffer irreparable harm if an injunction is not issued because the stolen digital assets and proceeds traceable thereto are capable of being rapidly transferred, withdrawn, or otherwise dissipated beyond Plaintiff's ability to recover them.

96. Plaintiff has a clear legal right to the stolen digital assets and traceable proceeds that he seeks to preserve through injunctive relief.

97. It is in the public interest for Plaintiff's property to be preserved pending identification of Defendant and adjudication of Plaintiff's claims.

WHEREFORE, Plaintiff ANTHONY APOLLO, respectfully requests that this Court enter an injunction freezing and preserving the accounts associated with the cryptocurrency addresses identified herein to the extent they contain Plaintiff's stolen digital assets or proceeds traceable

thereto, and enter judgment awarding: (1) damages in the amount of the value of Plaintiff's stolen assets at the time of the theft; (2) prejudgment interest; (3) an injunction ordering the return of any remaining stolen assets or proceeds derived therefrom; (4) attorneys' fees and costs incurred in prosecuting this action to the extent recoverable by law; and (5) such other and further relief as the Court deems just and proper.

Respectfully submitted,

XANDER LAW GROUP, P.A.
25 N.E. 2nd Avenue, Suite 808
Miami, Florida 33131
Telephone: (305) 767-2001
Facsimile: (855) 926-3370
service@xanderlaw.com

Attorneys for Plaintiff

By: /s/ Jose Teurbe-Tolon
JOSE TEURBE-TOLON, ESQ.
JOSE@xanderlaw.com
FL BAR NO. 87791