

Michael Burshteyn (SBN 295320)
Michael.Burshteyn@gtlaw.com
Kristin O'Carroll (SBN 312902)
kristin.ocarroll@gtlaw.com
GREENBERG TRAUIG, LLP
101 Second Street, Suite 2200
San Francisco, CA 94105
Telephone: 415.655.1300
Facsimile: 415.707.2010

Arda Goker (*pro hac vice forthcoming*)
Arda.Goker@gtlaw.com
GREENBERG TRAUIG, P.A.
450 South Orange Avenue, Suite 650
Orlando, FL 32801
Telephone: 407.420.1000
Facsimile: 407.420.5909

Mackenzie Cannon (*pro hac vice forthcoming*)
Mackenzie.Cannon@gtlaw.com
GREENBERG TRAUIG, LLP
77 West Wacker Drive, Suite 3100
Chicago, IL 60601
Telephone: 312.456.8400
Facsimile: 312.456.8435

Attorneys for Plaintiff
NIBI, INC.

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

NIBI, INC.,

Plaintiff,

v.

JOHN DOE, ET AL.,

Defendants.

Case No.:

COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Nibi, Inc. (“Nibi” or “Plaintiff”) by and through its undersigned counsel, alleges
2 as follows against Defendants John Doe, et al. (“Doe Defendants” or “Defendants”) on behalf of
3 itself and several other victims who have assigned their claims to Nibi:

4 **INTRODUCTION**

5 1. Nibi and others are victims of unidentified attackers—the Doe Defendants—who
6 stole approximately \$4 million of digital assets. The attackers did so through a malicious email
7 spoofing attack where they impersonated an email domain of the Deltec International Group bank
8 (“Deltec”).

9 2. Nibi is a Delaware corporation that develops software related to the Nibiru Chain.
10 Nibiru is a layer-1 blockchain and smart contract ecosystem.¹ Its developer-friendly and user-
11 friendly smart contract ecosystem enables web3 adoption by innovating at each layer of the stack,
12 including decentralized application development, infrastructure, and consensus.

13 3. Over the course of several months, Nibi exchanged emails with Deltec regarding
14 opening a new bank account. Nibi did so as part of its services agreement with MTRX Services
15 Ltd., a British Virgin Islands company and Matrix Foundation, a Cayman Islands Foundation
16 (collectively “MTRX”), which maintain a treasury of digital assets—including those that were
17 stolen in the attack at issue—and provide services related to the Nibiru Chain as well. MTRX has
18 assigned its claims arising out of the attack to Nibi for purposes of this action.

19 4. When Nibi was working to open an account with Deltec, Deltec sent its
20 communications to Nibi using the email domain URL www.deltecbank.com. During the course
21 of these communications, malicious attackers compromised the email thread where Nibi was
22 communicating with Deltec and introduced a set of imposter email addresses impersonating Deltec
23 using the email domain URL www.deltecsbank.com.

24 5. Nibi’s forensic security investigation to date has uncovered no indicators or
25 evidence of compromise of its own email systems related to its email communications with Deltec.
26 It is still unknown how Doe Defendants were able to introduce the imposter www.deltecsbank.com
27 email addresses into the email thread with Deltec and Nibi. Nibi’s investigation has revealed,

28 ¹ <https://nibiru.fi/>

1 however, that the Doe Defendants leveraged malicious Internet Protocol Addresses whose location
2 is in this district, in Mountain View, California.

3 6. Through email communications sent from the spoofed www.deltecbank.com
4 domain on the legitimate email thread between Nibi and Deltec, the Doe Defendants lied to make
5 Nibi and MTRX believe they were legitimate personnel from Deltec. Deltec, during the time that
6 these imposter emails were being sent, or before, did not alert Nibi and MTRX to the fact that the
7 www.deltecbank.com email domain was spoofed through a www.deltecbank.com domain. Nibi
8 and MTRX, as a result, reasonably believed that the imposter email addresses were authentic and
9 did belong to Deltec. Nibi and MTRX were consequently under the false impression that they
10 were communicating with and sending digital assets to Deltec. Due to the spoofing attack,
11 unfortunately, the transactions went to the malicious attackers instead.

12 7. After executing their fraud and theft, the Doe Defendants dissipated the converted
13 digital assets through a series of blockchain wallet addresses and cryptocurrency exchanges.

14 8. Nibi now brings this action to uncover the identity of the malicious Doe Defendant
15 attackers and recover the stolen assets.

16 **JURISDICTION AND VENUE**

17 9. Jurisdiction of this Court is founded upon 28 U.S.C. §1332(a)(2) because Nibi is
18 incorporated in Delaware with its principal place of business in Delaware, and is, therefore, a
19 citizen of Delaware for purposes of diversity jurisdiction. The Doe Defendants are individuals of
20 unknown citizenship. Nibi and Defendants are consequently citizens of different states for
21 purposes of diversity jurisdiction under 28 U.S.C. § 1332(a)(2).

22 10. The matter in controversy exceeds the sum or value of \$75,000.00, exclusive of
23 interest and cost.

24 11. This Court has personal jurisdiction over Doe Defendants because the Doe
25 Defendants launched their attack through the use of Internet Protocol Addresses located in
26 Mountain View, California, to host the malicious www.deltecbank.com domain, within the
27 jurisdiction of this Court.
28

12. Venue of this action is proper in this Court pursuant to 28 U.S.C. §1391 because a substantial part of the events giving rise to Plaintiff's claims occurred in the Northern District of California, based on Defendants' use of Internet Protocol addresses located in Mountain View, California to conduct their attack.

PARTIES

13. Plaintiff Nibi is a Delaware corporation that develops software related to the Nibiru Chain. Nibi also provides services related to the Nibiru Chain, including assisting MTRX with treasury management. The two MTRX entities have assigned all their claims arising from the events at issue in this action to Nibi.

14. Defendants John Doe, et al. are individuals of unknown residence, who on information and belief have targeted Nibi and MTRX and stolen MTRX's digital assets through the malicious use of Internet Protocol addresses located in Mountain View, California. Nibi intends to serve Defendants upon discovering their identities through early discovery. In the event that their identities remain undiscovered, Nibi intends to serve Doe Defendants via their associated cryptocurrency wallets on the blockchain.

FACTUAL BACKGROUND

A. Spoofing Attacks Aim to Steal Funds by Impersonating Legitimate Email.

15. A spoofing attack is a species of cybercrime in which a scammer masquerades as another person or entity. The masquerading scammer does so to defraud their victim and induce them to send funds unknowingly to the attacker.² Spoofing attacks can take many forms. Attackers use SMS text, email, websites, and other channels to socially engineer and exploit their target's trust in a third party.

16. In an email spoofing attack, the attacker mimics a trusted party's email address. The attacker registers an email address to match or closely resemble the trusted email address. Sometimes the spoofed email differs by only a single letter or number in a website's URL. This can be overlooked in an email header and cause the victim to believe they are still interacting with

² Ed Oswald, What Is Spoofing? U.S. News (Oct. 28, 2022), <https://www.usnews.com/360-reviews/privacy/what-is-spoofing>.

the trusted source.³ To mitigate such risks, financial institutions typically purchase common misspellings of their domain names to stop those domains from being used in spoofing attacks.⁴ In more sophisticated email spoofing attacks, the attacker uses the spoofed domain to conduct a series of communications that appear normal. The attacker researchers the target victim and the spoofed domain. They use this research to socially engineer the conversation and make the victim think that they are interacting with the real party—not just due to a similarity in email domain but also due to the authentic-seeming content of the conversation.

17. Once the attacker has deceived their target into believing that they are communicating with the trusted party, the attacker asks the recipient to send money, usually providing a reason that sounds plausible or urgent.

18. This is unfortunately what happened here. The attacker was able to register a domain virtually identical to Deltec’s legitimate domain, because Deltec did not purchase that domain to block such malicious registrations. The attacker then socially engineered the communications between Deltec and Nibi. Through multiple detailed communications, the attacker made it seem like they actually were Deltec and sent authentic-appearing messages about the content of the discussions that Nibi would expect to see. Then the attacker made their move and directed Nibi to send funds to Deltec—but those funds went instead to the attacker.

B. The Attack Occurred When MTRX Attempted to Open a Deltec Account.

19. Beginning in or around August 2023, Nibi and MTRX contacted Deltec to open a bank account. Deltec is a Bahamian bank with a presence in the United States that provides banking services to private and institutional clientele including cryptocurrency companies and services a number of crypto firms. Deltec markets itself as catering to crypto businesses, hosting multi-currency accounts that operate with all major cryptocurrencies. MTRX conducts all

³ See Spoofing and Phishing — FBI at <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing>.

⁴ See, e.g., <https://www.fdic.gov/news/financial-institution-letters/2005/fil6405a.html> (“Financial institutions should diligently manage domain names” and “should investigate the possibility of registering similar domain names.” “Practices to monitor and protect domain names should be regularly reviewed and updated as part of a financial institution’s information security program.”)

1 transactions exclusively in cryptocurrency and relies on specialized vendors that cater specifically
2 to crypto-focused businesses, making banking institutions like Deltec critical to its business.

3 20. MTRX initially spoke to Deltec in August of 2023, before it applied to open a
4 business account through Deltec's website at www.deltecbank.com and corporate portal
5 <https://corpapp.deltecbank.com/>. On November 2, 2023, Nibi virtually met with a Deltec
6 representative to discuss the account. On or around January 3, 2024, Deltec emailed Nibi, who
7 managed the communications for MTRX, from a www.deltecbank.com domain. Deltec provided
8 information on the account funding process. The email chain included several individuals from
9 Deltec, including a Deltec client services manager.

10 21. Over the next several months, Nibi and Deltec exchanged emails regarding the
11 account. These communications covered standard topics around account access and instructions
12 for funding the account.

13 22. Subsequent email exchanges between Nibi and Deltec regarding the MTRX
14 account occurred in the email thread that Deltec initiated in January 2024. When Nibi or Deltec
15 had questions of the other or requested information, they for the most part responded in that same
16 email thread.

17 23. Shortly before the spoofing attack, Deltec and Nibi exchanged several important
18 emails over the course of April and May 2024:

19 24. April 2, 2024. Nibi contacted Deltec to inquire about the status of the account
20 opening. Deltec responded and stated that the account had already been opened "pending
21 funding." Nibi responded the same day requesting information on how to fund the account with
22 digital assets. Deltec confirmed that the account could be funded using digital assets through an
23 affiliate of Deltec called Delchain. Deltec provided information for submitting the necessary
24 application materials to Deltec's Delchain affiliate.

25 25. April 21, 2024. Nibi responded to the same email thread that Deltec had initiated
26 with the information Deltec had requested to process payment through its Delchain affiliated
27 entity.
28

26. April 22, 2024. Deltec responded with feedback on the Delchain materials Nibi had submitted. One of Deltec's follow up questions concerned the assets under management ("AUM") anticipated in the account. Nibi, later that day, returned a revised form.

27. April 25, 2024. Deltec requested an amended submission from Nibi. Nibi submitted the updated form to Deltec, which specified that the potential AUM would be \$10,000,000 in fiat currency, and \$10,000,000 in digital currency.

28. May 10, 2024. Nibi emailed the Deltec team asking them to confirm whether the account was set up. Deltec responded that the account had not been activated because it had not been funded. Deltec provided updated settlement instructions to fund the account using U.S. Dollars.

29. May 13, 2024. Nibi notified Deltec that MTRX would fund the account with a stablecoin known as Tether ("USDT"). USDT is a cryptocurrency that aims to maintain its stable value by pegging it to another asset, here the U.S. Dollar.

C. **The Attackers Spoofed Deltec's Email Domain.**

30. The attackers, on information and belief, infiltrated the email thread at least by May 15, 2024, if not earlier.

31. May 15, 2024. Nibi received an email in the same chain that Deltec had initiated in January 2024, at 4:46 a.m. The email in the thread was sent from the domain www.deltecbsbank.com. This is identical to Deltec's www.deltecbank.com domain, but for the addition of the "s" between the "c" and the "b." Given the similarity in domain names, as well as the context around the transaction—including that the email came from the same thread and Deltec had indicated an affiliated entity would be involved—Nibi and MTRX believed this to be a legitimate email.

32. May 16, 2024. Upon receiving the instructions from the www.deltecbsbank.com domain, Nibi and MTRX proceeded to take steps to fund the account. Nibi and MTRX proceeded with caution, first initiating a 100 USDT test transaction on May 16, 2024. The attackers, continuing to pose as Deltec through the www.deltecbsbank.com domain, confirmed receipt on the

1 same day. Nibi and MTRX then sent a larger transaction of 500,000 USDT to the recipient address
2 that the attackers provided.

3 33. May 17, 2024. The attackers confirmed receipt of the \$500,000 payment the day
4 after it was sent. The attackers then directed Nibi and MTRX to send more funds. They claimed—
5 in another email communication sent on the thread that Deltec had initiated in January 2024—that
6 “the initial funding needs to be at least 10% of the potential AUM in order to activate the account.”
7 The message urged Nibi to fund the account with this additional amount quickly. The attackers
8 indicated, in their email, that the AUM would total \$17,000,000.

9 34. May 20, 2024. Nibi sent an additional 1,200,000 USDT, which the attackers
10 confirmed receiving the same day on May 20, 2024. This brought the total amount to \$1,700,100,
11 or 10% of the AUM referenced in the attackers’ May 17, 2024 email. The attackers continued
12 their scheme through another message. This message claimed that the percentage funding amount
13 was, based on direction from Deltec’s management team, 20% rather than 10%.

14 35. Nibi did not wish to send more funds. It offered to reduce the AUM in the account
15 and submit any other necessary documentation to support this change. The attackers responded
16 that Nibi should fund the 20% and then could place a withdrawal request later. Nibi, upon
17 receiving this assurance, sent an additional 300,000 in USDT. This brought the total sent to
18 \$2,000,100. All the communications and transactions referenced in this paragraph occurred on
19 May 20, 2024.

20 36. Nibi followed up with who they thought was Deltec (but was actually the attacker)
21 on the same day—and clarified that the intended account AUM was \$10,000,000, not \$17,000,000.

22 37. May 21, 2024. The attackers continued to socially engineer the situation. Using
23 Deltec’s spoofed domain, the attackers told Nibi that to change the AUM from \$10,000,000 from
24 \$17,000,000, Nibi and MTRX would need to resubmit a form, which “could further delay the
25 account activation.” The attackers directed Nibi and MTRX to “go ahead and fund the account at
26 20% of the already approved document \$17m AUM to avoid further delay.” Nibi and MTRX did
27 not wish to do so. Nibi responded that the \$17,000,000 figure was not previously approved and
28 should not be used as a baseline to calculate the funding requirement.

38. May 23, 2024. The attackers, using the www.deltecsbank.com domain, claimed that Deltec's management had "advised that 20% of the combined potential AUM in USDT \$10M and USD \$10M" needed to be funded to activate the account. Nibi responded with concern once again. The attackers then introduced a purported attorney for Deltec into the thread, who stated that the account would be activated upon funding and Nibi and MTRX could then withdraw funds.

39. That same day, May 23, 2024, MTRX and Nibi sent a 2,000,000 USDT payment. The total sum MTRX and Nibi had now sent amounted to \$4,000,100 in digital assets.

40. May 24, 2024. Nibi confirmed that the total amount supposedly necessary to activate the account had been sent. The attacker, later that day, confirmed receipt of the payment. These messages, like the others, occurred in the email thread that Deltec had initiated in January 2024.

D. Nibi and MTRX Uncovered the Spoofing Attack.

41. May 28, 2024. Nibi inquired in the email thread it believed to be with Deltec regarding the status of account activation.

42. May 29, 2024. The attacker continued to attempt to socially engineer the situation and steal more funds. In response to Nibi's inquiry, the attacker attempted to steal another \$4,000,000 in digital assets. The attacker introduced a person who claimed to be the "Delbank director of private banking" into the thread. His message stated that there was "confusion" because the "team has not well been updated on the newly regulatory requirement by the central bank" that "our bank is now required to request all potential clients to deposit 40% of the combined potential AUM[.]" The attacker claimed that he was "on standby to approve upon meeting the 40% requirement" and that, once sent, "you can initiate a withdrawal up to the limit of your needs[.]" The attacker claimed the new funding requirement was "for compliance purposes only[.]"

43. This message raised Nibi and MTRX's suspicions, and no further funds were sent.

E. The Attackers Initiate Transfer in Order to Conceal Stolen Funds.

44. When Nibi and MTRX realized that they had been the target of a spoofing attack, they immediately began investigating what had happened.

45. Nibi alerted Deltec on May 29, 2024 that an imposter had appeared in the email

1 thread Deltec initiated in January 2024, and that the imposter was using a spoofed version of
2 Deltec's email domain. Deltec did not respond until June 3, 2024, despite several follow up
3 attempts. Nibi and MTRX, in the meantime, proceeded to investigate.

4 46. Nibi and MTRX retained a blockchain forensic firm to track the assets as well as a
5 cybersecurity forensic firm to investigate how the email thread Deltec initiated in January 2024
6 could have been compromised.

7 47. Nibi's forensic security investigation to date has uncovered no indication of
8 compromise of Nibi's email systems regarding Nibi's email communications with Deltec. It is
9 still unknown how the Doe Defendants were able to introduce the imposter www.deltecsbank.com
10 email domain into the Deltec email thread.

11 48. Nibi's investigation has shown, however, that the Doe Defendants used malicious
12 Internet Protocol addresses based in Mountain View, California, in the course of their attack.

13 49. Nibi's blockchain tracing revealed that the attacker, after receiving funds, worked
14 to dissipate them through a series of cryptocurrency exchanges and wallets. Discovery through
15 this action will be necessary to fully reveal how the attacker was able to leverage exchanges to
16 dissipate these assets.

17 50. As a result of the attackers' conduct, 4,000,100 USDT was stolen from MTRX.
18 Nibi and MTRX have also incurred significant costs in investigating and remediating the attack.
19 The attack has damaged Nibi and MTRX's enterprise value in excess of millions of dollars as well
20 as harmed them through the opportunity cost of the loss of funds.

21 51. Nibi brings this action to enforce its own and MTRX's claims, which have been
22 assigned to Nibi, uncover the identity of the attackers, the source of the compromise of the Deltec
23 January 2024 email thread, and the movement of the funds after their theft, and recover the harm
24 caused by the attack.

25 **FIRST CAUSE OF ACTION**
26 **(CONVERSION)**

27 52. Nibi incorporates by reference as though fully set forth herein the allegations in all
28 of the preceding paragraphs.

53. Doe Defendants purport to exercise the right of ownership over digital assets unlawfully taken from MTRX, the rightful owner.

54. Doe Defendants attacked Nibi and MTRX, taking over \$4,000,000 million in digital assets from MTRX without authorization. Doe Defendants exercised and continue to exercise dominion over the assets, despite their belonging to MTRX.

55. Doe Defendants' conversion directly and proximately caused Nibi and MTRX harm, including loss of digital assets as well as costs of investigation and remediation of the Doe Defendants' attack.

56. As a result of the Doe Defendants' conversion, Plaintiff has suffered damages in an amount to be proven at trial, but in no event less than \$4,000,000, plus interest from and after the time of conversion.

SECOND CAUSE OF ACTION **(UNJUST ENRICHMENT)**

57. Nibi incorporates by reference as though fully set forth herein the allegations in all the preceding paragraphs.

58. Doe Defendants unlawfully obtained access to MTRX’s funds and used this access to steal and receive the benefit of \$4,000,000 in digital assets from MTRX, who has assigned its claims for these losses to Nibi.

59. Doe Defendants unjustly retained control over Plaintiff's assets, depriving MTRX of its right to withdraw, convert, transfer, or otherwise utilize over \$4,000,000 in digital assets.

60. Doe Defendants have gained the benefit of these \$4,000,000 in digital assets, after dissipating them through a series of blockchain wallets and exchanges, and have used these \$4,000,000 in digital assets to unjustly enrich themselves.

61. As a result of Doe Defendants' unjust enrichment, Nibi has suffered damages in an amount to be proven at trial, but in no event less than \$4,000,000, plus interest from and after the time of unjust enrichment and the costs of investigation and remediation of Defendants' attack.

///

///

THIRD CAUSE OF ACTION
(REPLEVIN)

62. Nibi incorporates by reference as though fully set forth herein the allegations in all of the preceding paragraphs.

63. This is an action to recover personal property. The property at issue is 4,000,100 USDT.

64. Upon information and belief, the U.S. Dollar equivalent of the personal property as of the date of theft is approximately \$4,000,000.

65. As of the date of this filing, the personal property is believed to be stored in cryptocurrency wallets controlled by Doe Defendants and has been laundered through digital asset exchanges.

66. At the time of the conversion, MTRX owned and had the right to immediately possess the personal property that was taken from them.

67. Doe Defendants intentionally exercised control and continue to exercise control over the digital assets in such a way as to exclude MTRX and Nibi from using or possessing them.

68. The property has not been taken for taxation, assessment, or fine pursuant to law nor has it been taken under any execution or attachment against Nibi or MTRX's personal property.

69. Nibi therefore demands that the wrongfully obtained property be restored it.

FOURTH CAUSE OF ACTION
(FRAUD)

70. Nibi incorporates by reference as though fully set forth herein the allegations in all of the preceding paragraphs.

71. Doe Defendants spoofed a Deltec email domain in order to defraud Nibi into sending approximately \$4,000,000 worth of USDT to Defendants. Doe Defendants, to conduct their fraud, represented that they were legitimate employees of Deltec and that the funds were necessary to fund the bank account.

72. Doe Defendants made their representations with knowledge of their falsity and with the intention of deceiving Nibi and MTRX.

73. Doe Defendants knowingly made the false representations in order to induce Nibi and MTRX to send funds to crypto wallet addresses held and controlled by Doe Defendants.

74. Nibi and MTRX justifiably relied upon Doe Defendants' false representations they were legitimate Deltec personnel and their instructions for transferring funds.

75. As a result of Nibi and MTRX's reliance upon Doe Defendants' false representations, Nibi and MTRX, whose claims have been assigned to Nibi, suffered millions of dollars in damages.

PRAYER FOR RELIEF

NOW, THEREFORE, Nibi respectfully requests that this Court enter judgment in favor of Nibi as follows:

1. For compensatory, incidental, and consequential damages, in an amount to be determined, for harms Nibi and MTRX suffered by Defendants' unlawful conduct, including the \$4 million in converted assets Doe Defendants stole as well as investigation and enforcement costs to uncover Doe Defendants' identities, uncover the movement of funds, and recover the stolen assets;

2. For punitive, exemplary, and other damages authorized by law;

3. For prejudgment interest and post-judgment interest on the full amount of damages;

4. For injunctive relief, including an order enjoining Doe Defendants, their agents, and relevant third parties from moving and dispersing the stolen digital assets;

5. For costs incurred to investigate and remediate the attack; and

6. For Nibi's attorney fees according to proof and costs incurred to the extent permitted by law.

///

///

///

///


///

///

1 DATED: August 30, 2024

GREENBERG TRAURIG, LLP

2
3 By


Michael Burshteyn
Michael.Burshteyn@gtlaw.com
Kristin O'Carroll
Kristin.Ocarroll@gtlaw.com
GREENBERG TRAURIG, LLP
101 Second Street, Suite 2200
San Francisco, California 94105
Tel: (415) 655-1300
Fax: (415) 707-2010

4
5
6
7
8
9 - and-

10
11 Arda Goker (*pro hac vice forthcoming*)
Arda.Goker@gtlaw.com
GREENBERG TRAURIG, P.A.
450 South Orange Avenue, Suite 650
Orlando, Florida 32801
Tel: (407) 420-1000
Fax: (407) 420-5909

12
13
14
15 - and-

16 Mackenzie Cannon (*pro hac vice forthcoming*)
Mackenzie.Cannon@gtlaw.com
GREENBERG TRAURIG, LLP
77 West Wacker Drive, Suite 3100
Chicago, IL 60601
Tel: (312) 456.8400
Fax: (312) 456.8435