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

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

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.: 5:24-cv-06184-NC

PLAINTIFF'S *EX PARTE* MOTION TO EXPEDITE DISCOVERY AND FOR AN ORDER AUTHORIZING ALTERNATIVE SERVICE

I. INTRODUCTION AND FACTUAL BACKGROUND

Plaintiff Nibi, Inc. ("Nibi" or "Plaintiff") requests an order authorizing early discovery to identify certain malicious attacker Defendants John Doe, et al. ("Doe Defendants" or "Defendants"). These Doe Defendants committed a sophisticated email spoofing attack[1] using the www.deltecsbank.com domain that resulted in the theft of $4 million in crypto assets. Nibi is seeking leave to issue limited subpoenas directed to Deltec as well as others involved in the flow of funds and information related to the attack, based on Nibi's investigation. This early discovery is warranted to uncover the details of the attack so that Nibi can identify the Doe Defendants.

Nibi also requests leave to use alternative service of process on Doe Defendants by delivering a non-fungible token ("NFT") to Doe Defendants' known Ethereum wallet. Alternative service is necessary because Plaintiff has not yet uncovered the identity of Doe Defendants and is therefore unable to effectuate service of the summons and complaint as prescribed by Federal Rule of Civil Procedure 4. This alternative service method has been authorized by courts in similar circumstances and is practical. It is likely to provide actual notice to the Defendants as it directly connects to the wallet used to launder the stolen funds.

Attack Details:

Nibi is a corporation that develops software related to the Nibiru Chain. (Declaration of Jonathan Chang "Chang Decl.," ¶2). The Nibiru Chain is a layer-1 blockchain and smart contract ecosystem,[2] providing a developer- and user-friendly smart contract ecosystem that enables web3 adoption by innovating at each layer of the stack, including decentralized application development, infrastructure, and consensus. (*Id.*)

In May 2024, unknown hackers targeted Nibi in an email spoofing attack, which resulted in the theft of approximately $4 million of the Company's digital assets. (*Id.* at ¶3.) To execute their attack, Doe Defendants intercepted and manipulated an email thread between Nibi and Deltec International Group ("Deltec"), a bank that serves cryptocurrency firms. (*Id.* at ¶3.)

Plaintiff contacted Deltec in Fall of 2023 to open a banking account. After some initial discussions,

[1] A spoofing attack occurs when a hacker pretends to be a trusted source in order to deceive a victim into sharing sensitive information or, in this case, transferring funds to the attacker. Ed Oswald, *What Is Spoofing?*, U.S. News (Oct. 28, 2022), https://www.usnews.com/360-reviews/privacy/what-is-spoofing.

[2] https://nibiru.fi/

Deltec emailed Nibi in January 2024 regarding the account creation process. Plaintiff began communicating with several Deltec employees regarding next steps and how to fund the new account. (Chang Decl. at ¶4). The initial emails from Deltec to Nibi were each sent using the email domain URL www.deltecbank.com. (*Id.*) Over the course of several months, Plaintiff and Deltec exchanged emails regarding how to open the account, addressing issues with documentation, and discussing whether Plaintiff could fund its account with cryptocurrency. (*Id.*) Unfortunately, and unbeknownst to Plaintiff at the time, during the course of these communications, Doe Defendants infiltrated the email thread by introducing a set of imposter email addresses, impersonating Deltec employees using the email domain URL www.deltecsbank.com. (*Id.* at ¶6). This spoofed domain is nearly identical to Deltec's www.deltecbank.com domain, but for the addition of the "s" between the "c" and the "b." (*Id.*). Believing the communications were authentic, Nibi continued to communicate with Doe Defendants via email at the spoofed www.deltecsbank.com domain. (*Id.* at ¶7.)

On May 15, 2024, at 4:46 a.m., Plaintiff received an email in the same chain from vswan@deltecsbank.com. (*Id.* at ¶8.) Nibi understood this email to include wire instructions to fund the account with a stablecoin known as Tether ("USDT"), which is a cryptocurrency that aims to maintain its stable value by pegging it to another asset, here, the U.S. Dollar. (*Id.*) But in reality, the email came from the spoofed Deltec domain, namely, @deltecsbank.com (with an added s in the middle), not @deltecbank.com. (*Id.*) Ultimately, the hacker(s), masquerading as a bank account services manager, exchanged numerous emails with Plaintiff and used this conversation to manipulate Plaintiff, tricking it into sending approximately $4 million in cryptocurrency over the course of several days. (*Id.* at ¶¶9-12.)

Eventually, Plaintiff realized that it had been deceived and initiated an investigation to trace the stolen funds and to better understand the nature and scope of the breach. (*Id.* at ¶13.) This investigation revealed several critical findings, including that Defendants launched their attack through the use of internet protocol ("IP") addresses located in Mountain View, California, to host the malicious www.deltecsbank.com domain. (*Id.*) Plaintiff also learned that Defendants transferred the stolen funds through multiple crypto exchanges to conceal their origins. (*Id.*)

Plaintiff filed its Complaint on August 30, 2024, noting that the identities of the Doe Defendants were unknown.

Requested Discovery & NFT Service:

Now, by this Motion, Plaintiff requests leave to serve early discovery on third parties who have information about the attack. The discovery will enable Plaintiff to learn the attackers' identities and current and permanent addresses so that they can be served and substituted as Defendants in this case. It will also allow Plaintiff to fully understand how the attack occurred so that they may better protect themselves from further victimization. To that end, Plaintiff is seeking the following targeted discovery:

First, Plaintiff is seeking any further information regarding how Doe Defendants infiltrated the email chain with Deltec Bank, and information regarding the scope of the breach. Deltec is likely to have relevant information regarding the identity and whereabouts of Doe Defendants. Plaintiff is also informed and believes that there have been other victims of a similar attack involving Deltec. Discovery to Deltec as well as other victims and those who have knowledge of similar attacks is likely to provide information relevant to identify the attacker.

Second, Plaintiff is seeking information related to the attackers' use of Internet and blockchain infrastructure to conduct their attacks. This includes information from digital currency exchanges that Defendants used to receive and transfer the stolen funds. After the attack, Defendants used a series of digital asset exchanges and internet services to attempt to disburse the proceeds and launder the stolen funds. These entities are also likely to have relevant information that could identify the attackers or other information necessary to mitigate the risk of further attacks. Plaintiff is also informed that the attackers used certain Internet Protocol addresses in the attack. The internet service provider who hosted these IP addresses is likely to have relevant information. So too would the ISP and hosting provider related to the spoofed www.deltecsbank.com domain that Defendants used to conduct their attack.

In addition to early discovery, Plaintiff is seeking leave to serve Doe Defendants on the Ethereum wallets identified during its investigation into the incident. Despite Plaintiff's investigation, Plaintiff still has no knowledge of Defendants' whereabouts or identity and, as a result, has been unable to serve them. To that end, Plaintiff retained an expert to create a an NFT containing the summons and Complaint in this matter as well as a special website containing case documents. The proposed NFT contains a notice of this action with summons language and a hyperlink to a specially created website, which includes: (1) a notice of this action, (2) a hyperlink to the summons and Complaint, and (3) all filings and orders in this action.

Plaintiff has good cause to believe that Doe Defendants continue to use their known Ethereum wallet and communication with this wallet address is therefore a reliable form of contact.

II. EARLY DISCOVERY IS WARRANTED BECAUSE OF DOE DEFENDANTS' EFFORTS TO OBFUSCATE THEIR ATTACK AND IDENTITY.

This Court has "broad discretion" to order expedited discovery. *Allen v. Currier*, No. 20CV1389-JLS(LR), 2023 WL 2728718, at *3 (S.D. Cal. Mar. 30, 2023) (citing *Johnson v. Mammoth Recreations, Inc.*, 975 F.2d 604, 609 (9th Cir. 1992)). "Expedited discovery under Rule 45 is appropriate when good cause for the discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *UMG Recordings, Inc. v. Does 1-4*, No. 06-0652 SBA (EMC), 2006 WL 1343597, at *1 (N.D. Cal. Mar. 6, 2006) (citing *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002) (granting expedited discovery under a "balance of hardships" analysis)).

Good cause exists here because third-party discovery is necessary to uncover Doe Defendants' identities, current and permanent addresses, and other information that will enable Plaintiff to identify how the attack occurred so that it may protect itself from further victimization prior to the Rule 26(f) conference in this case. Courts routinely permit accelerated discovery "in the interests of justice" where it is necessary to identify Doe defendants as Plaintiff seeks to do here. *See Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) ("[T]he district court erred in dismissing [plaintiff's] complaint against Doe simply because [plaintiff] was not aware of Doe's identity at the time he filed his complaint."); *see, e.g.*, *ZG Top Tech. Co. v. Doe*, No. C19-92-RAJ, 2019 WL 917418, at *2 (W.D. Wash. Feb. 25, 2019); *SingularDTV GmbH v. Doe*, No. 1:21-CV-06000-VEC , 2021 WL 3668161, at *1 (S.D.N.Y. Aug. 16, 2021); *see also Digital Sin, Inc. v. Does 1–5698*, No. C 11-04397 LB, 2011 WL 5362068 (N.D. Cal. 2011) (granting leave to subpoena internet service provider to identify Doe defendant).

Here, Doe Defendants' identities are essential to Plaintiff's prosecution of its claims. *See Wakefield*, 177 F.3d at 1163. So too is information from Deltec bank about its spoofed domain and interaction with the spoofed emails using its name. Information from exchanges through which the attackers disbursed the proceeds and laundered the funds gained through their attack as well as from other victims is highly relevant as well. Where discovery will "substantially contribute to moving th[e] case forward[,]" as here, courts grant it. *Semitool*, 208 F.R.D. at 277. The attackers may have left details that help to identify them during their abuse

of the exchanges and other internet services.

Further, early discovery is also warranted because it is likely that Doe Defendants will attempt to hide evidence of their attack, reducing the chance of catching them and increasing the likelihood that they will launch a similar attack against another party. Discovery will make it more likely the attackers will be apprehended and stopped from making off with the stolen assets.

Granting Plaintiff's request for early third-party discovery would not prejudice any of the Doe Defendants in any way. Plaintiff's request is limited in scope to information relevant to its claims that would identify the Doe Defendants and their methods of attack. Plaintiff will use this information to name the Defendants in the case, serve them, and move the case forward. Plaintiff is also at continued risk of further victimization, and the information will help it to protect itself. Any information Plaintiff receives will be shared with Doe Defendants as soon as they are named in the case. In such contexts, courts find that the good cause for expedited discovery of Doe defendants' identities "outweighs any prejudice" they may face. *See UMG Recordings,* 2006 WL 1343597, at *1 (concluding that good cause for expedited discovery of Doe defendants' identities "outweighs any prejudice . . . for several reasons"); *Semitool*, 208 F.R.D. at 277.

III. PLAINTIFF SHOULD BE PERMITTED TO EFFECTUATE SERVICE ON DOE DEFENDANTS BY NFT

Plaintiff also moves this Court for an order permitting alternative service of process on Doe Defendants through service of an NFT to Doe Defendants' known Ethereum wallet. An alternative method of service is permissible where it is reasonably calculated to apprise the defendants of the pendency of the case. *See Rio Properties, Inc. v. Rio Intern. Interlink*, 284 F.3d 1007, 1016 (9th Cir. 2002). Rule 4(e) provides that process may be served upon an individual located in a judicial district of the United States by "following the local state law for serving a summons in an action brought in courts of general jurisdiction in the state where the district court is located or where service is made." Because this Court sits in California, service on defendants located in the United States can be made by any method authorized by California law. Cal. Civ. Proc. Code § 413.30 provides that "[w]here no provision is made in this chapter or other law for the service of summons, the court in which the action is pending may direct that summons be served in a manner which is reasonably calculated to give actual notice to the party to be served and that proof of such service be made as prescribed by the court."

Where service must be made on a litigant outside the United States, Federal Rule of Civil Procedure 4(f)(3) permits litigants in the United States to serve process by "means not prohibited by international agreement, as the court orders." All that is required is that the proposed service is not prohibited by international agreement and such service comports with Constitutional due process, meaning that it is "reasonably calculated" to provide the defendants notice and an opportunity to defend. *See Rio Props*., 284 F.3d at 1016; *Chanel, Inc. v. Zhixian*, 2010 WL 1740695, at *2, 2010 U.S. Dist. LEXIS 50745, at *8 (S.D. Fla. Apr. 29, 2010).

The primary consideration is whether the manner of service is likely to provide the defendant with legally sufficient notice. To this end, a court may permit service of process by any means reasonably calculated to give actual notice to the defendant. *Greene v. Lindsey* (1982) 456 U.S. 444, 449 ("An elementary and fundamental requirement of due process in any proceeding which is to be accorded finality is notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.") (citation omitted); *Mullane v. Central Hanover Bank & Trust Co*., 339 U.S. 306, 314 (1950) (to satisfy due process, any alternative means of service must be "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.")

Service by delivering an NFT to Doe Defendants' [wallet] is reasonably calculated to give actual notice to Doe Defendants. While the identities of Doe Defendants are unknown, Plaintiff's investigation has revealed that Defendants regularly use the Ethereum wallets used to launder funds and are thus likely to receive the NFT. Doe Defendants conducted their scheme to defraud Plaintiff using Ethereum wallets, indicating their familiarity with blockchain technology, further demonstrating the reasonableness of service in this manner. *K.A. v. J.L.*, 450 N.J. Super. 247, 253 (2016) ("Given that the Facebook and Instagram accounts at issue are the sole conduits of the purported harm, service via Facebook is reasonably calculated to apprise the account holder of the pendency of this action and afford him or her an opportunity to defend against plaintiffs' claims [after service via certified mail was ineffective].")

Other courts have determined that, in similar situations, service by NFT is the means most likely to provide notice to Defendants. *See, e.g.*, *Stil Well v. Defendant "*1", No. 23-21920-CIV, 2023 WL 5670722 (S.D. Fla. Sept. 1, 2023) (authorizing service via transfer of NFT and posting process on a designated

serving notice website); *see also In re Celsius Network LLC*, No. 22-10964 (MG), 2024 WL 4564196 (Bankr. S.D.N.Y. Oct. 24, 2024) (authorizing service via NFT to specific wallet addresses.).

Though service via NFT is a newer concept, courts routinely allow other forms of electronic service, such as email or service via social media. *Chung v. Chih-Mei*, No. 22-cv-01983-BLF, 2022 WL 17584243, at *2 (N.D. Cal. Dec. 12, 2022) ("[C]ourts in this district have authorized service of process by social media."); *Fabian v. LeMahieu*, No. 4:19-cv-00054-YGR, 2020 WL 3402800, at *3 (N.D. Cal. June 19, 2020); s*ee also St. Francis Assisi v. Kuwait Fin. House,* No. 3:16-cv-3240 (LB), 2016 WL 5725002, at *2, *3 (N.D. Cal. Sep. 30, 2016) (Twitter (now X)); *UBS Fin. Servs. v. Berger*, No. 13-cv-03770 (LB), 2014 WL 12643321, at *2,*5 (N.D. Cal. Apr. 24, 2014) (LinkedIn); *Fed. Trade Comm'n v. Pecon Software*, 2013 WL 4016272, at *5 (S.D.N.Y. Aug. 7, 2013) ("Service by email alone comports with due process where a plaintiff demonstrates that the email is likely to reach the defendant.")

Doe Defendants are malicious attackers who have struck multiple victims and are attempting to conceal their identity to avoid detection. Any attempts to serve by traditional service are unlikely to succeed. These Doe Defendant attackers still use the addresses identified and continue to have access to these accounts. An NFT directing Defendants to a website that contained the service documents and confirming receipt of the documents would consequently reach them and provide them with the constitutionally required notice.

For the reasons set forth above, service via NFT is appropriate.

IV. CONCLUSION

For the above reasons, Nibi respectfully requests that the Court grant Plaintiff's Motion and issue an order (1) authorizing limited discovery, and (2) authorizing service by NFT.

DATED: November 29, 2024

GREENBERG TRAURIG, LLP

By /s/ *Michael Burshteyn*
Michael Burshteyn

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

-and-

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

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

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

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.: 5:24-cv-06184-NC **DECLARATION OF JONATHAN CHANG IN SUPPORT OF PLAINTIFF'S *EX PARTE* MOTION TO EXPEDITE DISCOVERY AND FOR AN ORDER AUTHORIZING ALTERNATIVE SERVICE**

DECLARATION OF JONATHAN CHANG

I, Jonathan Chang, declare as follows:

1. I am the Chief Operative Officer of Nibi, Inc. ("Nibi" or the "Company") I have personal knowledge of the facts set forth in this Declaration based on my role within the Company and review of Company materials, and, if called and sworn as a witness, I could and would testify competently with respect thereto.

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

3. In May 2024, Nibi was the victim of an email spoofing attack involving an email thread between Plaintiff and Deltec International Group ("Deltec"), a bank that serves cryptocurrency firms, wherein certain unknown hackers stole approximately $4 million of the Company's digital assets.

4. Nibi engaged in discussions with Deltec to open an account beginning in the Fall of 2023. After some discussions, Deltec emailed Nibi in January 2024 regarding the account creation process. On that email thread, Nibi personnel communicated regularly with several Deltec employees about next steps and how to open and fund the account. Each of the Deltec employees on the thread used the email domain URL www.deltecbank.com.

5. Nibi followed up regularly with Deltec employees about the status of the account and received several follow up inquiries from the Deltec account manager on matters like the access level and approved users. In April 2024, Nibi sent an email asking for instructions on how to fund the account using cryptocurrency. Deltec responded, stating that the Company would need to open an account with its sister company, Delchain, which Nibi endeavored to do. Nibi exchanged regular emails with the Deltec account manager wherein she provided specific information on how to complete the forms necessary to open and fund the account.

6. Unfortunately, during the course of these communications, Doe Defendants infiltrated the email thread by introducing a set of imposter email addresses, impersonating Deltec employees using the

email domain URL www.deltecsbank.com. This spoofed domain is nearly identical to Deltec's www.deltecbank.com domain, but for the addition of the "s" between the "c" and the "b."

7. Nibi's personnel on the thread, including me, did not realize that hackers had infiltrated the email chain and continued to provide information requested.

8. On May 15, 2024, at 4:46 a.m., Nibi received an email in the same chain from vswan@deltecsbank.com. Nibi understood this email to include wire instructions to fund the account with a stablecoin known as Tether ("USDT"), which is a cryptocurrency that aims to maintain its stable value by pegging it to another asset, here, the U.S. Dollar, but in reality, the email came from the spoofed Deltec domain, namely, @deltecsbank.com (with an added s in the middle), not @deltecbank.com.

9. On May 16, 2024, Nibi initiated a 100 USDT test transaction, which Doe Defendants posing as Deltec confirmed was successful. After receiving confirmation that the transaction was successful, the Company sent a larger transaction of 500,000 USDT to the recipient address that the attackers provided.

10. The attackers confirmed receipt of the $500,000 payment the day after it was sent and sent me an email directing Nibi to send more funds. They claimed—in another email communication sent on the thread that Deltec had initiated in January 2024—that "the initial funding needs to be at least 10% of the potential AUM in order to activate the account."

11. The Company sent an additional 1,200,000 USDT, which the attackers confirmed receiving the same day on May 20, 2024. This brought the total amount to $1,700,100, or 10% of the AUM referenced in the attackers' May 17, 2024 email. Then, the attackers claimed that the percentage funding amount was, based on direction from Deltec's management team, 20% rather than 10%. Although Nibi did not want to send more funds, Nibi was assured that it was necessary, and upon receiving this assurance, sent an additional 300,000 in USDT.

12. Finally, on May 23, 2024, the attackers, still 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. That same day, May 23, 2024, Nibi sent a final 2,000,000 USDT payment to fund the account, bringing the total sum Nibi had now sent amounted to $4,000,100 in digital assets.

13. Eventually, Nibi realized that Nibi was actually the victim of an email spoofing attack and launched an investigation to trace the stolen funds. This investigation revealed several critical findings, including that Defendants launched their attack through the use of internet protocol ("IP") addresses located in Mountain View, California, to host the malicious www.deltecsbank.com domain. Nibi also learned that the attackers had transferred the stolen funds through multiple crypto exchanges to conceal their origins. The investigation also revealed on-chain wallet addresses that the attackers were utilizing as part of their scheme. Further, the investigation has revealed that there are multiple other victims of similar attacks that appear to come from the same Doe Defendants, at least one of which involved Deltec Bank.

14. Nibi does not have any further information about the identity of the attackers or where they are located.

15. I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct and that this declaration was executed on November 29, 2024 in India.

/s/