UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA

JEYSEN ZIVAN YOGARATNAM	**CIVIL ACTION**
VERSUS	**NO: 24-393**
DEFENDANT "1" a/k/a "DARINA DUBOIS" and JOHN DOES 1-20, as yet unidentified Individuals, Business Entities and/or Unincorporated Associations	**SECTION: "G" (4)**

ORDER AND REASONS

Before the Court is Plaintiff's **Ex Parte Motion for Non-Party Discovery and Leave to Serve Third-Party Subpoenas (R. Doc. 23)**, seeking leave to conduct expedited discovery and serve third-party subpoenas before the Rule 26(f) Conference. Plaintiff contends that the expedited discovery is necessary to identify and serve the John Doe Defendants, prevent further dissipation of the funds at issue, and allow the case to proceed. R. Doc. 23 at 1.

I. Factual Background and Procedural History

This litigation arises from an alleged "pig butchering scam", "a type of investment scam in which the perpetrators deceive victims into depositing their assets on a fake-but-realistic-looking 'trading' or 'investment' platform, where no trading or investment ever occurs. Instead…the assets are simply stolen." *Cohn v. Popescu*, No. 24-337, 2024 WL 4525500, at *1 (E.D. Tex. Sept. 13, 2024) (Truncale, M.). According to an FBI report from September 9, 2024, cryptocurrency scams like "pig butchering scams" are one of the most prevalent and damaging fraud schemes today.[1]

These scams, named in reference to the practice of fattening a pig before slaughter, involve perpetrators using fake profiles to contact a victim through text messages, dating apps, and social

[1] Sofia Kettler, *FBI Releases 2023 Cryptocurrency Fraud Report*, FBI (September 9, 2024) https://www.fbi.gov/contact-us/field-offices/philadelphia/news/fbi-releases-2023-cryptocurrency-fraud-report#:~:text=If%20you%20believe%20you%20are,Complaint%20Center%20at%20ic3.gov..

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

media platforms; as in this case, LinkedIn.[2] According to the Complaint, Plaintiff met "Darina Dubois" in March 2023, who communicated with him via LinkedIn. R. Doc. 1 at 3. "Dubois", who Plaintiff never met in person, represented herself as a person experienced in cryptocurrency trading and who was willing to teach the Plaintiff her cryptocurrency trading methods that would purportedly result in high yield returns. *Id.* at 4. This follows the playbook of a typical perpetrator in a "pig-butchering scam", who appeals to the person's business investment interest.[3] Perpetrators routinely offer "high-yield investment opportunities in virtual assets, such as cryptocurrency", and instruct the victim to open accounts on online investment websites; as allegedly occurred in our case. Plaintiff alleges that "Dubois" encouraged him to invest in CTRL-FX, a fraudulent cryptocurrency exchange purportedly based out of the UK. R. Doc. 1 at 4.

Plaintiff alleges that he transferred money from his legitimate cryptocurrency accounts in the United States on or about March 23, 2023, into the fraudulent wallet with the hopes of securing high yield returns. R. Doc. 1 at 4-5. These transfers were between Plaintiffs' custodial wallets on Coinbase and Kraken, which means that it was a peer-to-peer transfer with no third party involved, unlike normal bank transactions.[4] *Id.*

"Dubois" allegedly built a connection with Plaintiff by leading him to believe that his investment had ballooned from $294,215 to $2,288,378.89 within four months, which was purportedly displayed on the fraudulent CTRL-FX mobile account. R. Doc. 1 at 6-7. Plaintiff then decided to withdraw his huge profit, along with his original investment, back to his legitimate accounts on Coinbase and Kraken. *Id.* at 7. Unfortunately for Plaintiff, it was indeed too good to be true.

---

[2] *Pig Butchering Scams*, OFFICE OF INSPECTOR GENERAL FEDERAL DEPOSIT INSURANCE CORPORATION, https://www.fdicoig.gov/pig-butchering-scams

[3] The perpetrators often attempt to develop a meaningful relationship and gain the victim's trust, by posing as individuals interested in friendship, romantic relationships, or business investments. *Id.*

[4] *See id.*

When Plaintiff attempted the withdrawal, he was allegedly told that he could not withdraw his original investment and profit from four months of trying his hand at high-yield cryptocurrency investing. R. Doc. 1 at 6-7. Instead, he needed to invest additional money, $484,460.83, by transfer to a CTRL-FX bank account located in Hong Kong, purportedly to cover taxes and fees. *Id. See Cohn*, No. 24-337 at *1 (a cryptocurrency scammer case in which the plaintiff met the alleged perpetrator on a dating website, was lured into investing on a fraudulent cryptocurrency platform, and was told that he could not withdraw funds without depositing more money).

Plaintiff paid the money but could not access his original investment or the purported profit. R. Doc. 1 at 7. As a result, Plaintiff filed this suit against "Darina Dubois" and John Doe Defendants 1-20. However, the Original Complaint set forth no allegations against anybody except "Dubois." *Id.* Nevertheless, the Court subsequently granted a default judgment and permanent injunction against "Dubois" and the 20 Doe Defendants, which were later revoked and rescinded at the Plaintiff's request. *See* R. Doc. 17. *See also* R. Doc. 19. After getting the case reopened, Plaintiff filed an Amended Complaint adding RICO claims and reducing the number of Doe Defendants from 20 to 4. *See* R. Doc. 20. Plaintiff alleges that Doe Defendants 1-4 are the owners of four cryptocurrency wallets at Bitkub, Binance, Blofin, and Tokenlon that his cryptocurrency was purportedly traced to by his forensic cryptocurrency experts. *Id.* at 1-2. Plaintiff seeks to recover the alleged current value of the invested cryptocurrency funds, which the Court notes is significantly less than $2,288,378.89.[5]

Plaintiff now seeks authorization to issue Rule 45 subpoenas to Bitkub, Binance, Blofin, and Tokenlon, all cryptocurrency exchanges located in foreign countries, to purportedly secure the

[5] The actual amount that Plaintiff seeks to recover is ~$500,000. *See* R. Doc. 23 at 2 (reporting that the approximate value of the allegedly stolen cryptocurrency was $574,790.81). *See also* R. Doc. 1 at 1 (reporting that the approximately value of the allegedly stolen cryptocurrency was $509,470.14625).

identity of John Doe Defendants 1-4, which now includes "Dubois." R. Doc. 23 at 1. Plaintiff contends that he seeks this information to be able to properly name the Doe Defendants to sue and place them on notice of his cryptocurrency conversion claim, unjust enrichment claim, imposition of constructive trust and disgorgement of funds, conspiracy, and purported RICO claim against them. R. Doc. 23 at 1.

II. Standard of Review

Federal Rule of Civil Procedure Rule 26(d) provides that "[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except…when authorized by these rules, by stipulation, or by court order." FED. R. CIV. P. 26(d)(1).

Under federal jurisprudence, expedited discovery is highly disfavored and should only be granted where the movant has made an affirmative showing of good cause. *See Bryan v. Walmart Inc.*, No. 23-7116, 2023 WL 8890341, at *3 (E.D. La. Dec. 26, 2023) (Ashe, B.). Although the Fifth Circuit has not articulated a specific standard for establishing good cause for expedited discovery, courts generally consider the breadth of the discovery requests, the purpose of the expedited discovery, the burden complying with the request puts on the defendants, "and how far in advance of the typical discovery process the request was made." *Bryan*, No. 23-7116 at *3 (quoting *D.H. Griffin Wrecking Co. v. 1031 Canal Dev., L.L.C.,* No. 20-1051, 2020 WL 8265341, at *2 (E.D. La. Apr. 16, 2020) (Douglas, M.J.)).

III. Analysis

Plaintiff seeks to issue Rule 45 subpoenas to Bitkub, Binance, Blofin, and Tokenlon requesting information related to the wallets associated with the alleged theft, namely: (1) the account holder's name, address, phone number, and email address; (2) the Know Your Customer

(KYC) and Anti-Money Laundering (AML) information; (3) the account balances and transaction history; and (4) the record of transfers to/from the relevant wallet addresses. R. Doc. 23 at 4.

Plaintiff contends that there is good cause for such expedited discovery because the requested information is necessary to identify and serve the Doe Defendants. R. Doc. 23 at 3. Plaintiff further alleges that his cryptocurrency assets may be further transferred or dissipated if discovery is delayed. *Id.* Plaintiff also alleges that the requested discovery is narrowly tailored to the information necessary to identify the Doe Defendants and prevent the dissipation of remaining assets at the subpoenaed cryptocurrency exchanges. *Id.* Finally, Plaintiff alleges that the subpoenaed cryptocurrency exchanges, which Plaintiff clarifies are third parties in this matter, will not be unduly burdened by the requested subpoenas. *Id.* at 4.

Under Fifth Circuit jurisprudence, where a plaintiff seeks to identify a Doe defendant through expedited discovery, the court generally considers whether the plaintiff has identified the "the missing party with sufficient specificity, the previous steps taken to locate the elusive defendant, and whether the plaintiff's claims would withstand a motion to dismiss." *Mary Kay v. Beyou-Cosmetics storefront of www.ebay.com*, No. 21-1074, 2021 WL 2315097, at *1 (N.D. Tex. Jun. 7, 2021) (Horan, M.J.) (quoting *Combat Zone Corp. v. Does*., 12-2750, 2012 WL 12898022, at *1-2 (S.D. Tex. Sept. 17, 2012) (Lake, S.)). The Court has noted an additional requirement developing in district courts within the Ninth Circuit, which is whether the movant has "prove[n] that discovery is likely to lead to identifying information that will permit service of process." *Jacobo v. Doe*, No. 22-672, 2022 WL 2079766, at *2 (E.D. Cal. Jun. 9, 2022) (Dorzd, D.) (quoting *ZG TOP Technology Co. Ltd. v. Doe*, 19-92, 2019 WL 917418, at *2 (W.D. Wash. Feb. 25, 2019) (Jones, R.)).

A. Identification of the Doe Defendants

In the Amended Complaint, Plaintiff contends that "Dubois" had cohorts and that there must be 4 Doe Defendants who are now the account holders of the cryptocurrency deposit wallets at issue.[6] R. Doc. 20 at 3. In support, Plaintiff cites to a report from Georgiy Stanev, a Certified Cryptocurrency Investigator with CNC Intelligence Inc., who allegedly conducted a blockchain tracing analysis of Plaintiff's stolen cryptocurrency. R. Doc. 20-1.

In considering this matter, the Court finds that there is an inherent contradiction in the representations made by the Plaintiff in the Motion. Plaintiff's expert report states that his analysis was based on a list of transactions provided by the Plaintiff, that were initiated between March and April of 2023, and sent digital payments to an alleged fraudulent organization. R. Doc. 20-1 at 7. Based on the information that the expert received from the Plaintiff, the report calculates Plaintiff's loss to be approximately $294,215, which is a bit less than half of what Plaintiff has represented that he lost. *Id. See* R. Doc. 20. The report does not provide any explanation of how this loss was calculated.

Additionally, the report contends that seven traces were conducted to track the movement of Plaintiff's cryptocurrency to four cryptocurrency exchanges: Bitkub, Binance, Blofin, and Tokenlon. R. Doc. 20-1 at 7-8. The report therefore recommends that these four exchanges be contacted and sent a request for the KYC information of the beneficiaries of the relevant cryptocurrency transactions. *Id.* at 8. In support, the report provides a ledger-like summary of the alleged cryptocurrency transactions along with five **potential** methods for analyzing them that purportedly led the expert to conclude that Plaintiff's cryptocurrency is located in four wallets in

[6] The following cryptocurrency deposit wallets were identified in the Amended Complaint as the locations of Plaintiff's stolen cryptocurrency: 0x7b7b86bfe06929a7a32aaf9c7bb87c27a816cc7b ("Bitkub Wallet"), 0xc383e037 ab6872adae3ec35714b8d8cc46bea867 ("Blofin Wallet"), 0x376795c8b53b69a712f1024cf8537f980eb3bcbf; ("Binance Wallet"), and 3JA4StsiJwsgMvnxj8JgchmBEZMTH9mUWm ("Tokenlon Wallet"). R. Doc. 20 at 3.

Bitkub, Binance, Blofin, and Tokenlon. *Id.* at 38-39. However, the report fails to identify which of these methods was utilized or how the Plaintiff's cryptocurrency was identified. Additionally, the expert report concedes that "[e]ach transaction may have multiple inputs and outputs", and that tracing methodologies simply "reveal the most likely path to a relevant VASP." *Id.* at 6.

Unlike a bank, cryptocurrency exchanges do not exercise complete control over validating the transactions in its ledgers. *See Friel v. Dapper Labs, Inc.*, 657 F.Supp.3d 422, 426-28 (S.D. N.Y. Feb. 22, 2023) (Marrero, V.). Instead, cryptocurrency exchanges utilize a "blockchain", a decentralized digital ledger that is validated by the cryptocurrency exchange's network of users. *Friel*, 657 F.Supp.3d at 427-28. Additionally, "[b]lockchains do not record real names or physical addresses, but only the transfers between digital wallets, thus maintaining a degree of anonymity for users." *Van Loon v. Department of Treasury*, 688 F.Supp.3d 454, 458-59 (W.D. Tex. Aug. 17, 2023) (Pitman, R.). Fraudsters utilizing cryptocurrency exchanges may also fraudulently register their accounts. *Licht v. Ling*, No. 23-1018, 2023 WL 4504585, at *2-4 (N.D. Tex. Jun. 20, 2023) (Starr, B.). Therefore, the identifying information associated with the alleged fraudster's wallets and accounts may be fictitious or based on an innocent individual's stolen identity.

Plaintiff's Motion and expert report do not address these issues. A review of the report shows that, at most, what Plaintiff has identified are cryptocurrency wallet accounts which by the very nature of blockchain transactions do nothing but show that a transaction occurred. It does not identify the method used to identify these wallets, nor definitively show that the listed transactions included Plaintiff's alleged stolen cryptocurrency. Additionally, the expert conceded in his report that this attempt to identify the Doe Defendants may not be successful. *See* R. Doc. 20-1 at 16 (showing that the transactions of Plaintiff's alleged stolen cryptocurrency include "hotwallet" exchanges, which may not give an individual's identifying information). The Court therefore finds

that Plaintiff has not met his burden of identifying Doe Defendants 1-4 with specificity. Accordingly, this factor weighs against granting Plaintiff's request for expedited discovery to identify the Doe Defendants.

B. Identification of the Steps Taken to Locate the Doe Defendants

Plaintiff contends that his forensic cryptocurrency tracing experts have traced Plaintiff's stolen assets to electronic wallets at four cryptocurrency exchanges through the blockchain: Bitkub, Binance, Blofin, and Tokenlon. R. Doc. 23 at 2. Plaintiff further states that he has attempted to obtain the identities and physical addresses of the Doe Defendants from these four cryptocurrency exchanges through informal requests, which Plaintiff asserts were unsuccessful. *Id.* Plaintiff does not identify the timeline or method of these informal requests, nor provide any evidence that they occurred. *Id.*

The report contains contact information for each exchange. However, while the expert says that they prepared a letter for the Plaintiff to send to the cryptocurrency exchanges, there is no evidence in the record that shows that Plaintiff actually sent the letters to the email contacts provided by his own expert. Therefore, this factor weighs against granting the request and there is no evidence of the steps taken to locate the Doe Defendants.

C. Whether Plaintiff's Claims Would Withstand a Motion to Dismiss

Plaintiff's Motion does not address the issue of whether his claims would withstand a motion to dismiss. *See* R. Doc. 23. Therefore, this factor weighs against granting Plaintiff's request for expedited discovery.

D. Whether the Requested Discovery is Likely to Lead to Identifying Information

Finally, the Court considers whether issuing the requested Rule 45 subpoenas to Bitkub, Binance, Blofin, and Tokenlon will likely lead to identifying information for the Doe Defendants

in this matter. Plaintiff alleges that subpoenas will obtain identifying information because the Doe Defendants were required to provide such information to the exchanges, including copies of their passports or driver's licenses, when they opened cryptocurrency accounts. R. Doc. 23 at 1.

Plaintiff's expert report states that "CNC Intelligence Inc. has identified the information needed to ascertain the identity of the suspect." R. Doc. 20-1 at 8. However, the report does not clearly identify what this information is. Instead, the report simply recommends that Plaintiff contact the four cryptocurrency exchanges above and request the KYC information for the wallets that purportedly received Plaintiff's stolen cryptocurrency. *Id.* at 9.

As Plaintiff's expert report indicates, these four cryptocurrency exchanges are not located in the United States. R. Doc. 20-1 at 33-36. Bitkub[7] is a Thailand-based cryptocurrency exchange company founded in 2018. *Id.* at 33. Binance[8] is a global cryptocurrency platform owned by a parent company, Binance Holdings Limited, and is comprised of a whole ecosystem of websites, clients, and independently operated applications within its platform. *Id.* at 35. Binance launched in 2017 was originally based in China, but later moved to Japan and then Malta.[9] While Binance Holdings Limited is based in the Cayman Islands, Binance has stated that it does not have a headquarters. *Id.* Blofin appears to refer to both a cryptocurrency exchange software created in 2019, and a cryptocurrency exchange company founded in Grand Caymen in 2018. *Id.* at 33.

---

[7] Plaintiff's expert states that the following is Bitkub's contact information: URL: http://bitkub.com; Address: 2525, FYI Center, Tower 2, 11th floor, Unit 2/1101-2/1107, Rama 4 Road, Klongtoei Sub-district, Klongtoei District, Bangkok 10110; Affiliations: BTC Korea.com Co. Ltd; Hosting Company, Cloudflare, Inc.; Domiciled in Thailand. R. Doc. 20-1 at 33-34.

[8] Plaintiff's expert states that the following is Binance's contact information: URL: http://binance.com; Address: Harbour Place, 2nd Floor North Wing, George Town, Grand Cayman Islands; Hosting Company: Cloudflare, Inc; Domiciled in Hong Kong. R. Doc. 20-1 at 35.

[9] Tom Wilson and Hannah Lang, *Binance, World's Top Crypto Exchange, at Center of US Investigations*, REUTERS (June 5, 2023) https://www.reuters.com/technology/binance-worlds-top-crypto-exchange-center-us-investigations-2023-03-27/

Finally, Tokenlon is a Singapore-based decentralized exchange and payment settlement protocol based on blockchain technology. *Id.* at 34.

Generally, Rule 45 subpoenas are subject to a geographic limitation. Namely, "[a] subpoena may command…production of electronically stored information…at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person." FED. R. CIV. P. 45(c)(2)(A). This geographic limitation concerns not only the requested discovery, but also "the location where a motion to quash is to be filed and resolved." *In re Highground Holdings, LLC*, No. 22-267, 2022 WL 4593088, at *3-4 (M. D. La. Sept. 29, 2022) (Bourgeois, M.J.). Fifth Circuit jurisprudence recognizes that where a plaintiff's subpoena to a non-party seeks compliance outside Rule 45's 100-mile geographic limitation and the non-party does not agree to send the requested discovery by email, the subpoena may be properly quashed. *In re Highground Holdings, LLC*, No. 22-267 at *3-4. Additionally, given the location of the international non-parties in this matter, service would likely be more complex than traditionally perceived, which the Court does not decide here.[10]

In *Licht v. Ling*, the Court granted a plaintiff's request for expedited discovery on June 20, 2023, for the purpose of identifying Doe defendants in a similar "pig-butchering scam" involving stolen cryptocurrency. No. 23-1018 at *2-4. In that case, the plaintiff's expert similarly identified specific wallets that allegedly received the plaintiff's stolen cryptocurrency. *Licht*, No. 23-1018 at *3. The plaintiff's expert conceded that it was impossible to know which accounts have remaining balances and admitted "that some may be fraudulently registered or belong to third parties who transacted with the alleged fraudsters." *Id.* Instead, the expert asserted that the wallets were "relatively closely linked to the fraud" and that the wallets are likely "intermediary addresses used

[10] The Court notes that issuance of a Rule 45 subpoena to international third parties may implicate the Hague Convention.

in an obfuscation effort." *Id.* Despite the acknowledgement by the expert, he held fast to his belief that issuing the subpoena would result in identifying the identity of the Doe defendants. *Id.* However, it appears that the subpoena did not result in favorable identity information because no motion to amend was ever subsequently filed. Further, no appearance has been made by the alleged Doe defendants in *Licht*.

It is the movant's burden to establish that the requested discovery is likely to lead to identifying information of the alleged defrauders. Given that the series of events at issue began with a fraudulent exchange on a fraudulent platform, Plaintiff has not established that issuing subpoenas would produce identifying information. This is corroborated by the expert report, which concedes that that the tracing methodologies lead only to a "likely" end point for the traced cryptocurrency.[11]

IV. Conclusion

Accordingly,

IT IS ORDERED that the Plaintiff's **Ex Parte Motion for Non-Party Discovery and Leave to Serve Third-Party Subpoenas (R. Doc. 23)** is **DENIED.**

New Orleans, Louisiana, this 29th day of October 2024.

KAREN WELLS ROBY
UNITED STATES MAGISTRATE JUDGE

[11] The Court's review of caselaw on this issue reveals that even where such discovery is granted, such cases are subsequently voluntarily dismissed by the Plaintiffs. *See e.g. Jacobo v. Doe*, No. 22-672, 2022 WL 2079766, at *1-4 (E.D. Cal. Jun. 9, 2022) (Drozd, D.) (in this case, the court granted a plaintiff's request for expedited discovery of Doe defendants in similar "pig butchering scam" case on June 9, 2022; however, the plaintiff subsequently informed the court that she had not found sufficient information or documents to identify the Doe defendants as of July 8, 2022, and voluntarily dismissed the case on February 16, 2023).