UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 225,364,961 USDT, Defendant *in rem*.	Civil Action No. 25-cv-01907-AHA

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF CLAIMANT INFINIWEB TECHNOLOGY INC.'S MOTION TO DISMISS COMPLAINT FOR FORFEITURE *IN REM*, MOTION TO SUPPRESS, AND MOTION TO STRIKE

Table of Contents

INTRODUCTION 1

I. Infiniweb 4

II. The Government's Warrantless Seizure 7

III. The Complaint 8

ARGUMENT 11

I. THE GOVERNMENT'S COMPLAINT FAILS TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED. 11

A. The Government's Heightened Pleading Burden 11

B. The Government's Forfeiture Theories 13

C. The Complaint Fails to Adequately Plead Wire Fraud Because It Does Not Allege Sufficient Domestic Conduct 13

D. The Complaint Fails to Adequately Plead Money Laundering 18

1. The Government's Money Laundering Allegations Lack Sufficient Domestic Conduct 18

2. The Complaint Alleges No Facts Regarding an Intent to Conceal as Required by the Concealment Money Laundering Statute. 20

E. Because the Complaint Fails to Adequately Plead Wire Fraud or Money Laundering, the Government Is Not Entitled to Forfeit the Defendant Property 22

F. Because the Defendant Property, the Burned Tokens Seized by the Government, and All Related Evidence Is Subject to Suppression, the Complaint Fails to Support a Reasonable Belief that the Government Will Be Able to Meet Its Tracing Burden at Trial 23

G. The Government's Theory of Forfeiture Is Not Viable to the Extent It Is Predicated on Aiding and Abetting and Accessory After the Fact Liability 25

II. THE COMPLAINT FAILS TO ADEQUATELY PLEAD THAT THE GOVERNMENT WILL BE ABLE TO ESTABLISH *IN REM* JURISDICTION. 26

III. THE COURT SHOULD SUPPRESS THE DEFENDANT PROPERTY AND ALL RELATED EVIDENCE. 28

A. The Defendant Property Was Seized Without a Warrant, and No Exception to the Warrant Requirement Applied. 29

B. The Government's Subsequent Seizure of the Defendant Property Pursuant to a Warrant Does Not Render the Property Admissible. 31

C. The Court Should Also Suppress Other Evidence Related to the Defendant Property. ... 32

IV. THE COURT SHOULD STRIKE PARAGRAPHS 239 AND 240 OF THE COMPLAINT, WHICH (INACCURATELY) RECOUNT CONFIDENTIAL SETTLEMENT COMMUNICATIONS THAT ARE INADMISSIBLE UNDER FEDERAL RULE OF EVIDENCE 408 33

CONCLUSION 35

Table of Authorities

Page(s)

Cases

Abitron Austria GmbH v. Hetronic Int'l Inc.,
600 U.S. 412 (2023).....15, 16

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....12

Barham v. Ramsey,
434 F.3d 565 (D.C. Cir. 2006).....30

Cobell v. Norton,
224 F.R.D. 266 (D.D.C. 2004).....33

Coolidge v. New Hampshire,
403 U.S. 443 (1971).....29

European Cmty. v. RJR Nabisco, Inc.,
764 F.3d 129 (2d Cir. 2014), *rev'd on other grounds*, 579 U.S. 325 15

Indep. Ins. Agents of Am., Inc. v. Hawke,
211 F.3d 638 (D.C. Cir. 2000).....26

Lee v. N.E.C.A.,
No. 19-7012, 2019 WL 2563223 (D.C. Cir. June 11, 2019) 21

Lipsky v. Commonwealth United Corp.,
551 F.2d 887 (2d Cir. 1976).....33, 34

Luan v. United States,
722 F.3d 388 (D.C. Cir. 2013).....26

Mincey v. Arizona,
437 U.S. 385 (1978).....31

Morrison v. National Australia Bank Ltd.,
561 U.S. 247 (2010).....15

One 1958 Plymouth Sedan v. Pennsylvania,
380 U.S. 693 (1965).....33

Republic Nat'l Bank of Miami v. United States,
506 U.S. 80 (1992).....26

Ventura Packers, Inc. v. F/V Kathleen,
424 F.3d 852 (9th Cir. 2025) 26

RJR Nabisco, Inc. v. European Cmty.,
579 U.S. 325 (2016).....14, 15

Salmo v. United States,
No. 06-12909, 2006 WL 2975503 (E.D. Mich. Oct. 17, 2006).....29

United States v. $125,938.62,
537 F.3d 1287 (11th Cir. 2008) 22

United States v. $639,558,
955 F.2d 712 (D.C. Cir. 1992).....33

United States v. $8,221,877.16 in U.S. Currency,
330 F.3d 141 (3d Cir. 2003).....22

United States v. All Assets Held at Bank Julius,
251 F. Supp. 3d 82 (D.D.C. 2017).....15, 16

United States v. All Assets Held at Bank Julius Baer & Co., Ltd.,
571 F. Supp. 2d 1 (D.D.C. 2008).....11, 15, 16

United States v. All Funds in Acct. Nos. 747.034/278, 747.009/278, & 747.714/278 in Banco Espanol de Credito, Spain,
295 F.3d 23 (D.C. Cir. 2002).....27

United States v. Chastain,
No. 23-7038, 2022 WL 13833637 (S.D.N.Y. Oct. 21, 2022).....6

United States v. Chinchic,
655 F.2d 547 (4th Cir. 1981) 17

United States v. Cosme,
796 F.3d 226 (2d Cir. 2015).....29, 30, 31

United States v. Dawkins,
17 F.3d 399 (D.C. Cir. 1994).....31, 32

United States v. Funds From Prudential Sec.,
362 F. Supp. 2d 75 (D.D.C. 2005).....12

United States v. Gengler,
No. 1:08CR12, 2009 WL 5549225 (E.D. Va. Oct. 23, 2009).....17

United States v. Hall,
613 F.3d 249 (D.C. Cir. 2010).....19, 20

United States v. One Gulfstream G-V Jet Aircraft,
941 F. Supp. 2d 1 (D.D.C. 2013) 12

United States v. Piervinanzi,
23 F.3d 670 (2d Cir. 1994) 19

United States v. Proctor,
489 F.3d 1348 (D.C. Cir. 2007) 29

United States v. Santos,
553 U.S. 507 (2008) 19

United States v. Sidorenko,
102 F. Supp. 3d 1124 (N.D. Cal. 2015) 15

United States v. Trie,
21 F. Supp. 2d 7 (D.D.C. 1998) 33, 35

United States v. Whitehead,
539 F.2d 1023 (4th Cir. 1976) 17

Wiggins v. Philip Morris, Inc.,
853 F. Supp. 457 (D.D.C. 1994) 33, 35

Wong Sun v. United States,
371 U.S. 471 (1963) 32

Zweibon v. Mitchell,
516 F.2d 594 (D.C. Cir. 1975) 31

Statutes

18 U.S.C. 1956(a)(1)(B)(i) 13

18 U.S.C. § 2 and (2) 25

18 U.S.C. § 3 ..... 24, 25, 26, 28

18 U.S.C. § 981 ..... 3, 22

18 U.S.C. § 981(a)(1) 25

18 U.S.C. § 981(a)(1)(A) 9, 12, 13, 25

18 U.S.C. § 981(a)(1)(C) 13, 25

18 U.S.C. § 981(b)(2) 29

18 U.S.C. § 983(a)(3)(A) 12

18 U.S.C. § 983(d) 7

18 U.S.C. § 1343 17

18 U.S.C. §§ 1343, 1349, 2, and 3 13

18 U.S.C. § 1956 .....13, 19, 20, 23

18 U.S.C. §§ 1956, 1957 25

18 U.S.C. § 1956(a) 18

18 U.S.C. § 1956(a)(1) 19, 20

18 U.S.C. § 1956(a)(1)(B)(i) 19

18 U.S.C. § 1956(c)(7) 25

18 U.S.C. § 1981(a)(1)(A), (C) 23

28 U.S.C. § 1355(b) 3, 27, 28

28 U.S.C. § 1395 27

Other Authorities

Federal Rule of Civil Procedure 8(a) 11

Federal Rule of Civil Procedure 12(f) 4, 33

Federal Rule of Evidence 408 34

Federal Rule of Evidence 410 33

U.S. Dep't of Justice, *Asset Forfeiture Policy Manual* (2025) 31

Supplemental Rule G(2)(f) 2, 12

U.S. Const. amend. IV 29

INTRODUCTION

The Government commenced this matter approximately two years ago with the warrantless, illegal seizure of cryptocurrency assets located outside of the United States. To accomplish that seizure, the Government merely contacted an issuer, or issuers, of certain digital assets and demanded without any finding of probable cause that assets in a broad swath of digital "wallets" be frozen in place until such time as the Government could articulate a basis for its freeze or decide to abandon its warrantless seizure. Despite pronouncements from Department of Justice ("DOJ") leadership abandoning a "freeze now, justify later" approach to individuals and companies transacting in digital assets cases, the Government in this case has continued with precisely that procedure—seizing large quantities of currency held by an innocent actor about whom the Government concededly knows nothing, all on the basis of an ill-defined tracing of a small fraction of purportedly tainted funds within those accounts. In addition to being at odds with DOJ's policy of not treating digital asset companies as *per se* criminal actors, this approach remains extremely prejudicial to a numerous innocent third parties: token issuers, financial services companies, operating businesses, and end-users about whom the Government bothers to gather zero information prior to these sweeping seizures.

Such was the case here. The seized assets were and are the property of claimant Infiniweb Technology Inc. ("Infiniweb" or the "Company"), a gaming and wagering company that is registered in the British Virgin Islands and that operates exclusively outside of the United States. The Government's initial seizure took the form of a November 2023 "freeze" of hundreds of millions of USDT stablecoin tokens owned by Infiniweb. The government finally obtained a warrant in May 2025—***almost a year and a half after the seizure occurred***. As the Government has partially and misleadingly disclosed, Infiniweb attempted to discuss the basis for the Government's warrantless freeze in an attempt to identify tainted funds and to resolve this matter

as to Infiniweb, a business uninvolved in any fraudulent activity that may have tainted some portion of funds long before they arrived in Infiniweb's digital wallets. Like the dollar bills in a person's wallet, digital assets act as a means of exchange between entirely legitimate counterparties even when those assets were, previously, touched by an unrelated and unknown bad actor. By the time of the filing of this matter, the Government apparently recognized that its initial warrantless seizure (the so-called "freeze") could not be retrospectively justified with respect to the majority of the wallets originally frozen through its warrantless seizure, and its post-seizure "clean up" warrant targeted fewer than half of the originally seized wallets—a tacit admission of the initial overbreadth of and lack of articulable probable cause underlying the initial warrantless seizure.

In this action, the Government nevertheless persists with an attempt to forfeit the remaining "frozen" assets targeted in that original illegal seizure. The Complaint should be dismissed on multiple grounds. The Complaint fails to state a claim for relief under Supplemental Rule G(2)(f), which requires that a complaint in a civil forfeiture action "state sufficiently detailed facts to support a reasonable belief that the Government will be able to meet its burden of proof at trial." Supp. R. G(2)(f). The Complaint fails under this standard because it fails to plead facts that would support any valid theory of forfeiture tied to any of the underlying predicate offenses (wire fraud, money laundering, and accessory theories of liability tied to those offenses). *First,* its claims far exceed the extraterritorial reach of the wire fraud statute because the Complaint fails to describe any domestic conduct, conflating effects on U.S. citizens with prohibited activity targeting the United States. *Second*, the Complaint likewise fails to adequately allege any underlying federal money laundering offense, *i.e.*, the other predicate for forfeiture in this case, both because it pleads no domestic money laundering conduct and because it fails to allege facts supporting a reasonable

belief that the any alleged money laundering transactions touching the seized wallets were committed with knowledge of wrongdoing or intent to conceal, as required by the money laundering statute. Because the Complaint fails to adequately plead wire fraud or money laundering, the Government is not entitled to forfeit the Defendant Property. *Third*, the Complaint does not support a reasonable belief that the Government will be able to meet its burden at trial of tracing the assets to any forfeitable offense, because evidence the Government would need to be able to use to trace the Defendant Property to the alleged forfeitable offenses must be suppressed (as discussed below). *Fourth*, to the extent it espouses a theory of forfeiture predicated on identification of proceeds derived from "aiding and abetting" or "accessory after the fact" liability, the Complaint exceeds the scope of 18 U.S.C. § 981, the civil forfeiture statute on which the Complaint is premised and which excludes either form of accomplice liability as a basis for forfeiture.

The Complaint also fails to adequately plead *in rem* jurisdiction. To plead *in rem* jurisdiction, a civil asset forfeiture complaint must "state the grounds for . . . in rem jurisdiction over the defendant property." Supp. R. G(2)(b). Here, the Complaint alleges that the "Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)." While the Complaint alleges that the Defendant Property is currently in the District of Columbia in the custody of the United States Marshals Service, the Government will not be able to prove that the Defendant Property was brought into the District of Columbia (if indeed that is true), because all of the evidence it could conceivably use to prove its location is suppressible. Moreover, despite request for confirmation, the Government has not provided a simple confirmation as to the actual location of the seized assets. Given that the Marshals Service has publicly announced an agreement with Coinbase Global, Inc., for the custody of digital assets, and given that Coinbase is a Delaware

company operating principally outside of the District of Columbia, the Government's bald assertion that these digital assets are actually located in the District of Columbia should be viewed with significant skepticism.

Finally, paragraphs 239 and 240 of the Complaint should be stricken pursuant to Federal Rule of Civil Procedure 12(f), because they contain allegations based on inadmissible confidential settlement communications between counsel for Infiniweb and the Government. To the extent those allegations could be considered material to any assessment of the sufficiency of the Complaint—and they cannot—they must be disregarded insofar as the Government has no basis to expect the admissibility of the protected statements recited therein.

I. Infiniweb

Infiniweb is an online gaming and wagering company that is registered in the British Virgin Islands. The company operates multiple online gaming platforms, including both websites and mobile applications, primarily servicing Chinese-language speakers in Asia. Verified Claim of Infiniweb Technology Inc., ECF No. 23 at 2. Infiniweb operates outside of the United States, and U.S. users are blocked from accessing the Company's various websites that host its gaming platforms. *Id.*[1]

[1] At various times, Infiniweb has sponsored football clubs in Europe, in partnership with particular Infiniweb gaming platforms such as Baobo.com, to enhance brand awareness for these platforms, but it has at all times focused on serving customers in Asia. *See, e.g.*, Ex. 1, Press Release, Racing Club de Strasbourg Alsace, *Baobo Sports Devient Sponsor Officiel du Racing Club de Strasbourg Alsace sur le Territore Asie-Chine* (Oct. 15, 2021), https://www.rcstrasbourgalsace.fr/baobo-sports-devient-sponsor-officiel-du-racing-club-de-strasbourg-alsace-sur-le-territoire-asie-chine/; Ex. 2, *HEAD Sports | VfL Bochum 1848* (Oct. 14, 2021), https://www.youtube.com/watch?v=r3PdkUTlC48; Ex. 3, Press Release, Levante U.D., *Levante UD and ROR Sports join forces* (Aug. 24, 2021), https://www.levanteud.com/en/news/levante-ud-and-ror-sports-join-forces; Ex. 4, Press Release, *FCA Augsburg*, TVT Sports becomes Official Regional Partner of FC Augsburg in Asia (Aug. 23, 2021), https://www.fcaugsburg.de/en/article/tvt-sports-becomes-official-regional-partner-of-fc-augsburg-in-asia-14387.

The Government does not allege that Infiniweb operates in the United States. Indeed, the Government apparently has no independent knowledge whatsoever of Infiniweb, and the only references to Infiniweb in the Complaint are partial representations of post-seizure outreach to the Government by counsel for Infiniweb. Compl. ¶¶ 239-40. The Complaint alleges that after being informed by counsel that Infiniweb owns the funds associated with the Subject Virtual Currency Addresses, the Government conducted "[o]pen-source research regarding Infiniweb." *Id.* ¶ 240. The Government's "[o]pen-source research" revealed that Infiniweb had held a gaming license from the Philippine Amusement and Gaming Corporation. *Id.*

Infiniweb's customers may transact using fiat currency or certain digital assets. One digital asset commonly used to transact on Infiniweb's platform is USDT, a stablecoin that is pegged to the U.S. dollar and that is designed to operate digital cash. Verified Claim of Infiniweb Technology Inc., ECF No. 23 at 2; Compl. ¶ 28.[2] USDT, like other digital assets and "cryptocurrency," is a medium of exchange over "blockchain" technology, a publicly available ledger of digital transactions. Compl. ¶¶ 17-19. USDT transacts over various blockchains.[3] In effect, the blockchain records which online addresses, or "wallets," are sending, holding, or receiving digital assets. *Id.* ¶ 18. A recipient of USDT may be able to view the history of transactions of various wallets that interact with a particular blockchain. *Id.* However, unless an independent public statement exists claiming ownership of a particular wallet, public blockchains

[2] *See also* Ex. 5, Tether, *What are Tether tokens and how do they work?*, https://tether.to/en/how-it-works ("Tether tokens are assets that move across the blockchain just as easily as other digital currencies but that are pegged to real-world currencies on a 1-to-1 basis. . . . All Tether tokens are pegged at 1-to-1 with a matching fiat currency (e.g., 1 USD₮ = 1 USD) and are backed 100% by Tether's reserves.").

[3] *See* Ex. 5, Tether, *How it works*, https://tether.to/en/how-it-works ("Tether tokens exist as digital tokens built on various blockchains including Algorand, Avalanche, Celo, Cosmos, Ethereum, EOS, Liquid Network, Near, Polkadot, Solana, Tezos, Ton, and Tron.").

do not reflect the ownership of any individual wallet or the purpose of any particular transaction. *See United States v. Chastain*, No. 23-7038, 2022 WL 13833637, at *1 (S.D.N.Y. Oct. 21, 2022) (discussing the "transfer[of] funds through anonymous Ethereum blockchain accounts and new Ethereum accounts without any prior history"). Just as with the cash in one's physical wallet, it is not possible for a recipient to know the full provenance or origin of the USDT represented in any particular transfer into one's digital wallet, unless one has access to independent information regarding that provenance. *See id.*

USDT is widely known to be subject to freeze and seizure by U.S. authorities; indeed, Paolo Ardoino, CEO of Tether, which issues USDT, has explained, "Unlike traditional financial systems, where illicit flows often go unseen, USDT is traceable, transparent, and accountable. We remain fully committed to continue working with law enforcement around the world to disrupt financial crime, as demonstrated by our ongoing support of investigations in the U.S. and beyond."[4] USDT is also widely listed on global cryptocurrency exchanges, including those directly regulated by U.S. authorities.[5] As such it is far from an asset exclusively or even primarily used to facilitate fraud or money laundering.

[4] Ex. 6, Press Release, Tether, *Tether Acknowledged by U.S. Authorities for Freezing $1.6M Connected to Terrorism Financing* (Jul. 24, 2025), https://tether.io/news/tether-acknowledged-by-u-s-authorities-for-freezing-1-6m-connected-to-terrorism-financing/.

[5] *See, e.g.*, Ex. 7, Kraken, *Tether*, https://www.kraken.com/prices/tether (Kraken listing for USDT); Ex. 8, Kraken, *Where is Kraken licensed or regulated* (detailing Kraken's registration with FinCEN, registration of a subsidiary offering digital asset custody services as a Wyoming-chartered Special Purpose Depository Institution, and registration of a subsidiary offering equities trading services with the SEC, FINRA, and SIPC); Ex. 9, Coinbase, *Tether*, https://www.coinbase.com/price/tether (Coinbase listing for USDT); Ex. 10, Coinbase, *Enhancing Trust with Regulatory Compliance* (detailing Coinbase's "licensure in nearly every US state," "approval from international regulatory bodies," and compliance with laws and regulations administered by OFAC and other federal authorities).

The Defendant Property identified by the Complaint consists of USDT held in seven virtual currency addresses (the "Subject Virtual Currency Addresses"), amounting to 225,364,961 USDT. Compl. at ¶ 48. These assets are revenues belonging to Infiniweb, generated in the normal course of its business operations, through Infiniweb's provision of gaming and wagering services. Verified Claim of Infiniweb Technology Inc., ECF No. 23 at 3.

The Complaint contains no allegation that Infiniweb's gaming and wagering services, which are not available to users in the United States, constitute illegal or forfeitable activity under the laws of the United States. Nor could there be, as the provision of such services abroad by a company incorporated and operating outside of the United States is perfectly legal under U.S. law.[6]

II. The Government's Warrantless Seizure

This matter first came to Infiniweb's attention through a warrantless seizure by the Government. On November 20, 2023, the Government demanded that Tether "freeze" the USDT held at the Subject Virtual Currency Addresses. Compl. ¶ 172. "Freeze," of course, is a euphemism for "warrantless seizure." Unmentioned by the Complaint is the fact that the Government's initial freeze covered not only the wallets at the seven Subject Virtual Currency Addresses, but rather a total of thirty-five wallets belonging to Infiniweb, the contents of twenty-eight of which are not named as defendants-in-rem in this litigation. The freeze rendered the contents of Infiniweb's operating accounts inaccessible to Infiniweb, and by the Government's own admission, the seizure was conducted without any effort to obtain a warrant. Indeed, the

[6] Should this matter proceed beyond the motion-to-dismiss stage, Infiniweb will show that to the extent the allegedly illegal activity described in this matter occurred at the time or after Infiniweb obtained the Claimed Assets, Infiniweb is an innocent owner, as described in 18 U.S.C. § 983(d); and that, to the extent the alleged illegal activity occurred prior to Infiniweb's receipt of the Claimed Assets, Infiniweb is a bona fide purchaser or seller for value, reasonably without cause to believe that the Claimed Assets were subject to forfeiture, as described in 18 U.S.C. § 983(d). *See* Verified Claim of Infiniweb Technology Inc., ECF No. 23 at 3.

Government did not obtain a "clean up" warrant permitting seizure of the Defendant Property until almost a year and a half later, on May 1, 2025. *Id.* ¶ 48. The Government never obtained a seizure warrant as to the remaining twenty-eight wallets, and it has since asked Tether to unfreeze those wallets, essentially conceding that this portion of its warrantless seizure was also baseless.

In connection with the Government's long-delayed, post-hoc execution of its warrant, the USDT contents of those target wallets were "burned" (that is, destroyed by being sent at the Government's direction to an unrecoverable address) and "reissued" (that is, new tokens of equal value were issued by Tether and directed to a wallet controlled by the Government). *Id.* ¶¶ 209, 213, 216, 220, 224, 227, 230. Accordingly, the tokens the Government currently seeks to forfeit are not the same tokens that were originally in Infiniweb's wallets at the Subject Virtual Currency Addresses, but rather are tokens of equivalent value issued to the Government by Tether following a prolonged period during which Infiniweb's wallets and its property were subject to a remote, extraterritorial seizure by the United States. The constitutional violation at the outset of the Government's ill-conceived investigation taints the downstream transfer, and evidence of that transfer, such that the current assets in the Government's control cannot be demonstrated to be traceable to any of the alleged offenses giving rise to forfeiture.

III. The Complaint

The Complaint bases its claim of forfeiture on two alleged offenses: (1) a wire fraud scheme involving theft of funds from various, disconnected victims, involving a total of $19 million in identifiable proceeds that have been traced to the Subject Virtual Currency Addresses (*see, e.g.*, Compl. ¶¶ 1, 68); and (2) a purported money laundering scheme centered on alleged attempts to conceal the nature, source, or origin of the proceeds of that wire fraud scheme (*see, e.g.*, Compl. ¶ 1). The Government alleges that unspecified persons caused other unspecified

individuals in the Philippines with Vietnamese identification documents to perpetuate these schemes. *See, e.g.*, Compl. ¶ 63.

The Complaint alleges that certain of the victims of the $19 million wire fraud scheme resided in the United States (*see, e.g.*, Compl. ¶ 86) and that others did not. *See* Compl. ¶ 68 (identifying some victims whose funds are part of the $19 million as being from the United Kingdom, Australia, and Germany). Beyond the allegation that a portion of the $19 million (itself less than 10% of the funds seized in this case) originated in the United States, there are no allegations of domestic conduct in the Complaint. The Complaint does not allege that the remainder of the Defendant Property originated in the United States, or that that *any funds* passed through the United States at any point in connection with a supposed laundering transaction. Nor does the Complaint allege that any of the persons responsible for the disconnected "schemes" were United States persons or were located in the United States. The vast majority of the Defendant Property, therefore, is concededly *not* the proceeds of any identified fraud, and even the $19 million identified as fraud proceeds is divided between U.S. and non-U.S. origins. Moreover, at no point does the Government so much as attempt to link any of these alleged thefts through an overarching fraud "scheme," such that minimal U.S.-contacts as to one purported victim might suffice to extend the reach of the federal wire fraud statute to the totality of the funds described in the Complaint. Rather, the vast majority of the funds named as defendants-in-rem appear to be seized exclusively on the basis that those undescribed funds were purportedly "involved in" purported "money laundering" transactions that are not themselves alleged to have occurred in or through the United States. *See* 18 U.S.C. § 981(a)(1)(A).

With respect to the alleged money laundering, the Complaint is short on specifics as to intent or the purpose of any particular transaction and simply fails to identify any *money*

laundering transaction occurring in or through the United States. The Complaint sets forth details about transfers among various digital wallet addresses, with approximately 8% of the assets (about $19 million out of about $225 million) alleged to have been proceeds of the alleged wire fraud "scheme." In support of the supposed intent of the persons responsible for the transactions at issue to conceal those transactions, the Government alleges that the transactions that it has selected, based on an alleged "tracing" of fungible digital assets, is complicated and involves reciprocal payments at various points along its selected tracing route. For instance, the Complaint alleges that "frequent transfers to or from the same transaction counterparties by more than one person from the same IP address is a red flag indicator of money laundering." Compl. ¶ 56. The Complaint does not explain how these same transactions are also inconsistent with innocent, legitimate arms' length transactions among counterparties engaging in repeat business, or with transactions by potentially *multiple* individuals or institutions through shared or "bridge" wallets that facilitate commerce in the digital asset ecosystem.[7] Critically, the Government makes no specific allegation as any actual intent to conceal as to any of these transactions—unsurprising in that the digital assets and exchanges at issue appear to involve well-known issuers (such as Tether) and exchanges (such as OKX). Each transaction the Government references in the Complaint was conducted on a public blockchain, using cryptocurrencies, such as USDT, that are widely known to be, and even touted by their creators as being, traceable by law enforcement. *See supra* notes

[7] *See* Ex. 11, Transak, *What is Cryptocurrency Bridging? An Explainer on Crypto Bridges* (Jan. 29, 2024), https://transak.com/blog/what-is-cryptocurrency-bridging-an-explainer-on-crypto-bridges ("Crypto bridging is a potential solution to the problem of blockchain interoperability. It allows effortless transmission of assets between blockchains. From a technical standpoint, crypto bridging involves locking up assets on the source blockchain using smart contracts and producing their "clones" on the destination chain.").

4-5; Compl. ¶ 19 ("Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency.").

The Complaint's only allegations concerning Infiniweb are in paragraphs 239 and 240. These allegations are products of (but, to be clear, do not accurately reflect) confidential settlement communications between counsel for Infiniweb and the Government. The Complaint says nothing else about Infiniweb, its ownership of the Subject Virtual Currency Addresses, or its business. Because these allegations are based on inadmissible statements, they should be stricken without regard to the Government's inaccurate recounting of those protected statements.

ARGUMENT

I. THE GOVERNMENT'S COMPLAINT FAILS TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED

The Court should dismiss this action because the Complaint fails, in numerous ways, to state a claim upon which relief can be granted. *First*, the Government's claims far exceed the extraterritorial reach of the wire fraud and money laundering statutes, the two pleaded forfeitable offenses. *Second*, the Complaint does not support a reasonable belief that the Government will be able to meet its tracing burden at trial, particularly due to suppression of information required in response to the Government's unlawful warrantless seizure. *Third*, the Government's theory of forfeiture is not viable to the extent it is predicated on aiding and abetting and accessory after the fact liability.

A. The Government's Heightened Pleading Burden

A civil asset forfeiture complaint is subject to a "higher standard of pleading" than a typical civil action. *United States v. All Assets Held at Bank Julius Baer & Co., Ltd.*, 571 F. Supp. 2d 1, 16 (D.D.C. 2008). Most civil actions are subject to the familiar "notice pleading" standard embodied by Federal Rule of Civil Procedure 8(a), under which "a complaint must contain

sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). But the pleading requirements for civil asset forfeiture actions are set forth in the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (the "Supplemental Rules"). 18 U.S.C. § 983(a)(3)(A). And under Supplemental Rule G(2)(f), the complaint in a civil forfeiture action must "state sufficiently detailed facts to support a reasonable belief that the Government will be able to meet its burden of proof at trial." Supp. R. G(2)(f).

Whereas *Iqbal* requires mere facial plausibility and does not impose a "probability requirement," *Iqbal*, 556 U.S. at 678, Supplemental Rule G(2)(f) does, requiring that the Government plead facts giving rise to a "reasonable belief" that the Government will prevail. This is a "heightened particularity requirement . . . designed to guard against the improper use of seizure proceedings and to protect property owners against the threat of seizure upon conclusory allegations." *United States v. One Gulfstream G-V Jet Aircraft*, 941 F. Supp. 2d 1, 14 (D.D.C. 2013) (granting motion to dismiss asset forfeiture complaint where government failed to substantiate allegation that defendant property is derived from or traceable to illicit activity). Greater detail is required in the civil asset forfeiture context "because of the drastic nature of th[e] remedies" available. *Id.* (quoting 12 Wright & Miller, Fed. Prac. & Proc. § 3242 (2d ed. 1997)).

In a civil asset forfeiture action, the Government ultimately bears the burden of establishing, by a preponderance of the evidence, that the property is subject to forfeiture. *See United States v. Funds From Prudential Sec.*, 362 F. Supp. 2d 75, 80-81 (D.D.C. 2005) (citing 18 U.S.C. § 983(c)). Specifically, the Government must sufficiently allege that *every USDT token that it seeks to forfeit* is either traceable to a forfeitable offense or was "involved in" a money laundering transaction. 18 U.S.C. § 981(a)(1)(A).

B. The Government's Forfeiture Theories

The Complaint alleges that the Defendant Property is forfeitable based on two interrelated theories:

1. The Defendant Property constitutes "proceeds of wire fraud and wire fraud conspiracy offenses, committed in violation of 18 U.S.C. §§ 1343, 1349, 2, and 3," where 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud or conspiracy to commit wire fraud. Compl. ¶¶ 6, 9.
2. The Defendant Property was "involved in money laundering and money laundering offenses, committed in violation of 18 U.S.C. 1956(a)(1)(B)(i) [*i.e.*, concealment money laundering], 1956(h), and 2, and 3," where 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956. Compl. ¶¶ 6, 8.

With respect to each of these theories, the Complaint fails at both steps of the analysis: it fails to adequately allege an underlying criminal offense, and it fails to adequately allege that the Defendant Property will be traceable to those alleged underlying offenses.

C. The Complaint Fails to Adequately Plead Wire Fraud Because It Does Not Allege Sufficient Domestic Conduct

The Complaint alleges that the Defendant Property constitutes or is derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud. Compl. ¶ 242. The wire fraud statute does not apply extraterritorially, however, and the Complaint fails to plead conduct giving rise to a domestic application of the statute. The Complaint does not describe any overarching "scheme" sufficient to connect the disparate alleged frauds described therein. Even were the subset of alleged U.S.-based victims described in discrete portions of the Complaint sufficiently connected to constitute an overarching "scheme," the Government cannot rely solely on the place in which the

effects of the wrongdoing were felt to plead a domestic scheme, but rather it must plead domestic fraudulent conduct underlying an overarching scheme, which it has failed to do here. Here, the Complaint attempts to use a subset of allegations regarding U.S. persons (but not necessarily U.S.-based conduct) to extend the U.S. wire fraud statute to activity occurring outside of U.S. borders without any allegations suggesting that the various, individual frauds alleged somehow converge into a global "scheme" by any actor or set of collaborative conspirators.

The Supreme Court has articulated a two-step test for determining the extent of a criminal statute's extraterritorial reach. *See RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325, 337 (2016). *RJR Nabisco* reaffirmed the established "presumption against extraterritoriality," under which "federal laws will be construed to have only domestic application" in the absence of "clearly expressed congressional intent to the contrary." *Id.* at 335. When faced with allegations of conduct that occurred abroad, either in whole or in part, courts must determine whether "Congress has affirmatively and unmistakably" stated that the offense applies extraterritorially. *Id.* If not, the statute has no extraterritorial application. *Id.* This inquiry into "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially"—constitutes the first step of the extraterritoriality analysis. *Id.* at 337.

The second step, which is reached if the statute is not extraterritorial, requires the court to "determine whether the case involves a domestic application of the statute," by "looking to the statute's 'focus.'" *Id.* "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S.

territory." *Id.* Thus, it is not the case that *any* domestic conduct or effects are sufficient to give rise to a domestic application of a statute. *See Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 266 (2010) ("[T]he presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case.").

The Supreme Court's recent ruling in *Abitron Austria GmbH v. Hetronic Int'l Inc.*, 600 U.S. 412 (2023), sheds further light on the application of the second step of the test. There, the Court held that in determining whether a case involves a permissible domestic application of a statute (there, the Lanham Act), a court should look to the location of the defendant's alleged conduct (in that case, trademark-infringing sales of products that did not end up in the United States) rather than the effects of that conduct (consumer confusion in the United States). *Id.* at 415-16, 421-22.

Applied here, the *RJR Nabisco* test reveals that the Complaint fails to plead an underlying violation of the wire fraud statute sufficient to give rise to federal forfeiture. As to step one of the test, the wire fraud statute does not apply extraterritorially. *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 101-102 (D.D.C. 2017) ("[N]othing in the text, legislative history, or context of the wire fraud statute expressly rebuts the presumption against extraterritoriality."); *see also European Cmty. v. RJR Nabisco, Inc.*, 764 F.3d 129, 141 (2d Cir. 2014), *rev'd on other grounds*, 579 U.S. 325; *United States v. Sidorenko*, 102 F. Supp. 3d 1124, 1129 (N.D. Cal. 2015). The Government therefore must plead an adequate nexus to the United States under step two.

In *All Assets Held at Bank Julius*, the court held that for the purposes of step two of the *RJR Nabisco* test, the focus of the wire fraud statute is "a scheme to defraud that involves the use of U.S. wires," and *not* "the use of U.S. wires no matter where th[e] scheme is conceived,

developed, or executed." 251 F. Supp. 3d at 102. The court then concluded that "the United States has failed to allege sufficient domestic conduct to support a domestic claim for wire fraud," even though the Government had alleged in that case, among other things, that:

- in connection with a foreign extortion and bribery scheme, funds were transferred through bank accounts in the United States;
- in connection with a scheme to defraud a foreign government of at least $23.4 million, fraud proceeds were acquired through transactions that passed through U.S. financial institutions;
- in connection with another foreign extortion and bribery scheme, "there were financial transactions through the United States and . . . two U.S. corporations allegedly made payments"; and
- in connection with a scheme to cause a foreign government to overpay for prefabricated homes, the homes were first purchased from a company in the United States and were shipped from the United States (no domestic wire was specifically alleged, though).

Id. at 105-09.

The Complaint in the instant matter contains no allegations as to who is responsible for the alleged wire fraud scheme, or from where those persons were operating, except that persons apparently in the Philippines, with Vietnamese identification documents, were involved with certain of the many disparate frauds described in the Complaint (though not with respect to any of the alleged U.S.-based victims of certain disconnected fraudulent activity). *See, e.g.*, Compl. ¶ 63. With respect to the handful of alleged U.S.-based victims, the Government alleges nothing about the locations involved with the actual events that led to their alleged loss of funds, merely asserting their residency as an apparent stand-in for relevant facts. In other words, the Government has failed to plead any facts concerning the location of the alleged conduct underlying the wire fraud scheme.

Even assuming that some small subset of alleged victims are residents of U.S. states, under *All Assets Held at Bank Julius*, the mere use of domestic wires (which are not actually alleged

here) does not give rise to a permissible domestic application of the wire fraud statute. *Abitron Austria* speaks directly to the Government's deficiency in this case: the Court may not look only to the place in which the effects of the wrongdoing are felt, assuming that residency of some victims in fact represents such a place.

To tie proceeds to a wire fraud scheme, the Government is required to allege that the proceeds stemmed from a unified scheme to defraud. *See* 18 U.S.C. § 1343 (wire communications must be transmitted "for the purpose of executing [the] scheme or artifice"); *see, e.g.*, *United States v. Chinchic*, 655 F.2d 547, 551 (4th Cir. 1981) (holding that the government failed to offer any evidence to support the "alleged common scheme" where there was no evidence to support that "two . . . separate and unrelated transactions" were "so interconnected in time, place and manner (that they) constitute[d] a common scheme or plan"); *United States v. Whitehead*, 539 F.2d 1023, 1025 (4th Cir. 1976) (holding that "the government did not meet its burden of proving that there was any connection between" two offenses where the only thing they had in common was the involvement of a common third party); *United States v. Gengler*, No. 1:08CR12, 2009 WL 5549225, at *16 (E.D. Va. Oct. 23, 2009) (holding that the government was required to prove that "Defendants devised or culpably participated in the alleged single, overarching scheme to defraud and that "the evidence is not sufficient for that purpose since the evidence did not sufficiently connect the two Defendants to a single criminal enterprise or undertaking"). But the Complaint fails to allege that any of the assets beyond the $19 million the Government purports to trace were part of *any* alleged fraud, let alone a unified scheme, and it also does not allege that those assets are products of some other unlawful and sufficiently domestic scheme. Thus, even if there were a sufficiently domestic wire fraud scheme alleged with respect to part of the $19 million in purportedly traced Defendant Property, the remainder of the Defendant Property is simply not part

of any sort of "overarching scheme" to defraud alongside any portion of the purportedly traced $19 million. In short, no wire fraud scheme has been pleaded with respect to these assets, which comprise all but the purportedly traced $19 million of the Defendant Property.

D. The Complaint Fails to Adequately Plead Money Laundering

The money laundering allegations in the Complaint are legally insufficient in two ways. *First*, like the pleaded wire fraud scheme, the pleaded money laundering scheme does not allege sufficient domestic conduct. *Second*, the Complaint fails to support a reasonable belief that the money laundering transactions were conducted by anyone with the requisite knowledge of wrongdoing and intent to conceal.

1. The Government's Money Laundering Allegations Lack Sufficient Domestic Conduct

The Government's money-laundering theory is even less tethered to any U.S. activity than its wire fraud theory. Unlike the wire fraud statute, the concealment money laundering statute has an extraterritoriality provision, but by its express terms it applies to *laundering* conduct by a non-U.S. citizen only if that laundering conduct—*distinct from any underlying fraud that might have generated proceeds subsequently laundered*—occurs in part in the United States. In other words, the Government cannot meet the money laundering statute's extraterritorial jurisdiction requirements by relying on conduct (such as an allegedly domestic payment made by a victim) that was part and parcel of the wire fraud scheme that necessarily preceded a subsequent transaction to launder the proceeds of that fraud. Instead, the Government must plead domestic *money-laundering conduct* involving transfers of funds that are already the proceeds of a completed "specified unlawful activity." 18 U.S.C. § 1956(a). The Complaint simply fails to plead any domestic money-laundering conduct, and thus cannot support forfeiture of any funds purportedly "involved in" non-existent money laundering transactions.

The Complaint alleges that the Defendant Property is forfeitable because it was the subject of concealment money laundering under 18 U.S.C. § 1956(a)(1)(B)(i) and conspiracy to commit the same under § 1956(h). Compl. ¶ 6. Under § 1956(f), there is extraterritorial jurisdiction over concealment money laundering by a non-U.S. citizen (and here, there are no allegations of laundering activity by any U.S. citizen) only if "the conduct"—meaning "the conduct prohibited by [§ 1956]"—"occurs in part in the United States," and the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000. *Id.*

The conducted prohibited by § 1956 is, of course, money laundering, rather than wire fraud or other violations not prohibited by § 1956. The D.C. Circuit has held that the "offense of money laundering [under § 1956(a)(1)] must be separate and distinct from the underlying offense that generated the money to be laundered." *United States v. Hall*, 613 F.3d 249, 254 (D.C. Cir. 2010) (citing a string of circuit-court cases reaching the same holding), *amended*, No. 07-3036, 2019 WL 6794225 (D.C. Cir. Dec. 12, 2019). That is, the "provision requires first that the proceeds of specified unlawful activity be generated, and second that the defendant, knowing the proceeds to be tainted, conduct or attempt to conduct a financial transaction with these proceeds with the intent to promote specified unlawful activity." *United States v. Piervinanzi*, 23 F.3d 670, 679–80 (2d Cir. 1994); *see also United States v. Santos*, 553 U.S. 507, 513 (2008) (interpretating "proceeds" in the context of § 1956 to mean "profits," rather than "receipts," because treating all receipts of a crime as proceeds would cause a "merger" between the underlying unlawful activity and money laundering). Accordingly, in *Hall*, the D.C. Circuit held that "the evidence was insufficient to support [a] money laundering conviction because the alleged money laundering activity was part and parcel of the underlying bank fraud." *Hall*, 613 F.3d at 254.

The Complaint makes no allegation that any money laundering conduct occurred in the United States, with respect to any of the assets at issue. The only payments alleged to have taken place in the United States are the initial payments made by disparate victims of scams that, as discussed above, fail to cohere as a "scheme." But even assuming those victim payments amount to proceeds of a federal wire fraud (and they do not, as pled), those payments were not money laundering transactions by definition. They were not made to conceal the proceeds of wire fraud, but rather were alleged to have been made by victims as "part and parcel of the underlying . . . fraud." *Hall*, 613 F.3d at 254. As such, even assuming those transactions involved the use of U.S. wires, those transactions were not money laundering transactions themselves prohibited by § 1956. Because the Complaint alleges *zero* domestic money laundering payments and no U.S. citizen money launderers—in fact, no domestic activity money laundering activity whatsoever—the Complaint must, at a minimum, be dismissed to the extent it relies on a theory of forfeitability based in the money laundering statutes.

2. The Complaint Alleges No Facts Regarding an Intent to Conceal as Required by the Concealment Money Laundering Statute

Concealment money laundering requires a pleading of one or more financial transactions conducted by someone who: (1) "know[s] that the property involved in a financial transaction represents the proceeds of some form of unlawful activity," and (2) "know[s] that the transaction is designed in whole or part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity." 18 U.S.C. § 1956(a)(1).

The Complaint makes no allegations concerning the knowledge of the person(s) conducting any of the alleged transactions following the generation of "proceeds" of a fraud. It makes no allegations about who they are, or whether they had any involvement in, or even knowledge of, the alleged underlying confidence scams. Indeed, as discussed above, the Complaint does not

allege a single, coherent wire fraud scheme for someone to have had the requisite intent to conceal. In all, the Complaint:

- Connects IP addresses in the Philippines with various accounts associated with "Vietnamese identification documents and KYC photos." *See, e.g.*, Compl. ¶¶ 55, 63.
- Points to a variety of transactions and, to a limited degree, purports to "trace" funds using a self-selected accounting methodology between various accounts. *Id. passim*.
- Makes conclusory assertions – not factual allegations – that the transfers constitute "suspicious transaction behavior" and a "series of hops for no legitimate purpose." *Id.* ¶¶ 107, 140.

The Government makes *no* allegations about Infiniweb, the rightful owner of the assets, except a handful of assertions based on confidential and inadmissible settlement communications (see below) and, apparently, a Google search. None of the allegations in the Complaint, taken separately or together, gives rise to a "reasonable belief" that Infiniweb or anyone else knew that the property being transferred was (allegedly) proceeds of unlawful activity, or that the contents of the wallets illegally seized by the Government came to be in those wallets through an intent to conceal. The Complaint does not, and cannot, explain how these transactions are inconsistent with innocent, legitimate arms' length transactions among business counterparties or, further "upstream" in the Government's purported tracing, among friends, family members, or others who may exchange funds for any number of reasons. As the Complaint makes clear, each transaction the Government references in the Complaint was conducted on a public blockchain, using cryptocurrencies, such as USDT, that are widely known to be, and even touted by their creators as being, traceable by law enforcement. *See* Compl. ¶ 19. The Government's assertion of a baseless conclusion simply does not rise to the level of a well-pleaded fact. *See Lee v. N.E.C.A.*, No. 19-

7012, 2019 WL 2563223, *1 (D.C. Cir. June 11, 2019) (per curiam) (explaining that courts are not required to accept in a complaint "a legal conclusion couched as a factual allegation," or "naked assertions devoid of further factual enhancement" (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009))).

E. Because the Complaint Fails to Adequately Plead Wire Fraud or Money Laundering, the Government Is Not Entitled to Forfeit the Defendant Property

The Complaint fails to allege domestic conduct sufficient to plead either wire fraud or money laundering. Because the Government has adequately alleged no forfeitable offense, the Complaint should be dismissed.

In the alternative, if the Court were to conclude that the Complaint adequately pleaded wire fraud but not money laundering, the Complaint must be dismissed with respect to the 92% of the Defendant Property not traced, or traceable, to the alleged underlying wire fraud scheme. *See United States v. $8,221,877.16 in U.S. Currency*, 330 F.3d 141, 158 (3d Cir. 2003) ("In forfeitures under section 981, the Government is required to trace the seized property directly to the offense giving rise to the forfeiture."); *United States v. $125,938.62*, 537 F.3d 1287, 1294 (11th Cir. 2008) (reversing the district court's order of forfeiture with respect to certain assets "because the Government failed as a matter of law to meet its burden of proving by a preponderance of the evidence that [those assets] were derived from funds" obtained through the commission of a forfeitable offense). The Complaint candidly admits that only a small portion of the funds at issue here are traceable to alleged wire fraud, as opposed to funds that are forfeitable as having been "involved in" money laundering because they were later identified in the same wallets as wire fraud proceeds allegedly "traced" by the Government:

> The launderers' use of sophisticated money laundering techniques presents numerous complex challenges to investigators when tracing victim funds from their initial deposit addresses all the way to the SUBJECT VIRTUAL CURRENCY

> ADDRESSES. These challenges include the sheer volume of transactions involved in the network of 144 OKX Accounts (hundreds of thousands), the use of consolidation addresses used to accumulate hundreds of millions of dollars that redirects the LIFO order, and the use of countless intermediary addresses that serve to both add additional difficulty to the tracing efforts and also redirect the LIFO order. Nevertheless, using LIFO, investigators were able to trace some victim funds in initial deposit addresses to some of the SUBJECT VIRTUAL CURRENCY ADDRESSES.

Complaint ¶ 196. Ultimately, the Complaint purports to trace only $19 million—about 8% of the Defendant Property—from victims to the Subject Virtual Currency Addresses. Because the Government has failed to plead any domestic conduct, as required by the money laundering statute, the only funds it could even conceivably forfeit are the 8% that are allegedly traceable to the alleged wire fraud scheme. The other 92% of the Defendant Property should be immediately returned to Infiniweb's wallets. Those wallets, in turn, should be relieved of the Government's warrantless "freeze" order directed to Tether.[8]

F. Because the Defendant Property, the Burned Tokens Seized by the Government, and All Related Evidence Is Subject to Suppression, the Complaint Fails to Support a Reasonable Belief that the Government Will Be Able to Meet Its Tracing Burden at Trial

To plead a claim for forfeiture, the Complaint must "state sufficiently detailed facts to support a reasonable belief that the Government will meet its burden." Supp. R. G(2)(f). As relevant to the instant case, the Government may forfeit only property that "constitutes or is derived from proceeds traceable to" money laundering under § 1956, or wire fraud, or conspiracy to commit either, or property that is "involved in a transaction or attempted transaction in violation of section 1956." *See* 18 U.S.C. § 1981(a)(1)(A), (C).

[8] As noted above, the Complaint fails to allege a basis for forfeiture under the wire fraud statute, as well. Taken together, these failures require the return of all funds, not merely that portion expressly targeted solely on the basis of an extraterritorial laundering theory.

The Government seized the assets previously held at the Subject Virtual Currency Addresses illegally, without a warrant and in blatant violation of the DOJ's own policies designed to safeguard due process for property owners, as discussed *infra* § III.A. As a result, those assets and all evidence derived from this illegal seizure must be suppressed. Without that evidence—including evidence of the transfer of the illegally seized funds into the Government-controlled wallet where the Defendant Property now sits—the Government is unable to trace any of the Defendant Property, now held by the Government in its own digital asset wallets, to a forfeitable offense.

The Government illegally seized hundreds of millions of USDT from thirty-five wallets, including the approximately 225 million USDT at the seven Subject Virtual Currency Addresses that is the subject of this action, by requesting that Tether freeze those assets without first obtaining a warrant. *See* Compl. ¶¶ 48, 172. Over a year and a half later, the Government obtained a warrant, only for the portion of the frozen assets residing in the seven Subject Virtual Currency Addresses. *Id.* ¶ 172. This portion of the assets was "burned" by Tether, at the Government's request, and then reissued. *Id.* ¶¶ 209, 213, 216, 220, 224, 227, 230. These reissued tokens, which constitute the Defendant Property, are the assets the Government now seeks to forfeit. Yet all of this evidence—the illegally seized (and now burned) tokens, the reissued tokens, and any data and information created as the result of this burning and transfer that provides the critical connection between the burned tokens and the reissued tokens—is the fruit of a poisonous tree. As discussed in § III, *infra*, it must all be suppressed.

Accordingly, and even assuming the Government were able to adequately trace funds from the alleged victims to the illegally seized Subject Virtual Currency Addresses, the Government will not be able to trace the Defendant Property sitting in its own wallets back to the Subject Virtual

Currency Addresses and, therefore, to a forfeitable offense. As a result, the Complaint must be dismissed.

G. The Government's Theory of Forfeiture Is Not Viable to the Extent It Is Predicated on Aiding and Abetting and Accessory After the Fact Liability

The Government's forfeiture theory expressly relies on theories of accessory liability that do not in fact constitute bases for forfeiture. The Complaint asserts:

1. The Government is entitled to forfeit (1) proceeds of aiding and abetting wire fraud under 18 U.S.C. § 2 and (2) proceeds of the offense of being an accessory after the fact to wire fraud under 18 U.S.C. § 3. *See* Compl. ¶¶ 6, 9.
2. The Government is entitled to forfeit (1) funds "involved in" aiding and abetting money laundering under 18 U.S.C. § 2 and (2) funds involved in the offense of being an accessory after the fact to money laundering under 18 U.S.C. § 3, or proceeds traceable to such funds. *See* Compl. ¶¶ 6, 8.

Neither of these positions is tenable. Even the Complaint argues, in summarizing the Government's forfeiture authorities, only that "18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957, or 1960, or any property traceable to such property" and that "18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting 'specified unlawful activity' as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense." Compl. ¶¶ 8-9. While both 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C) encompass violations of substantive offenses and conspiracies to commit the same, they exclude aiding and abetting or accessory after the fact liability. *See* 18 U.S.C. § 981(a)(1) (stating that conspiracy to commit an enumerated offense is itself a forfeitable offense, but making no mention of aiding and

abetting, or accessory after the fact).[9] In this circumstance, the Court should apply the well-established *expressio unius est exclusion alterius* interpretive canon, which applies when the "draftsmen's mention of one thing, like a grant of authority, does really necessarily, or at least reasonably, imply the preclusion of alternatives." *Indep. Ins. Agents of Am., Inc. v. Hawke*, 211 F.3d 638, 644 (D.C. Cir. 2000). Here, the forfeiture statutes painstakingly list a specific set of federal crimes as the basis for forfeiture, and expressly includes conspiracy theory liability as part of that statutory scheme. The forfeiture statutes do not incorporate violations of § 2 or § 3 of Title 18 as a basis for forfeiture. This exclusion is important in cases where, as here, the Government's case rests on a purported "tracing" effort that refers to less than 10% of the funds that it has seized and makes no reference to any criminal intent by any identifiable individual at any point. The Court should dismiss the Government's claims to the extent that they plead a forfeiture theory that relies on after the fact or aiding and abetting liability.

II. THE COMPLAINT FAILS TO ADEQUATELY PLEAD THAT THE GOVERNMENT WILL BE ABLE TO ESTABLISH *IN REM* JURISDICTION

In a civil asset forfeiture case, the property the Government seeks to forfeit is a party to the litigation. The Court therefore must have *in rem* jurisdiction—analogous to *in personam* jurisdiction in a typical case—over that property. *Luan v. United States,* 722 F.3d 388, 397, 399 & n.15 (D.C. Cir. 2013). *In rem* jurisdiction is established through the valid seizure of the *res*. *Ventura Packers, Inc. v. F/V Kathleen*, 424 F.3d 852, 853 (9th Cir. 2025); *see also Republic Nat'l Bank of Miami v. United States*, 506 U.S. 80, 84 (1992) ("[A] valid seizure of the *res* is a prerequisite to the initiation of an *in rem* civil forfeiture proceeding."). Even at the pleading stage,

[9] This is unsurprising as a construction of the forfeiture statutes: it is unclear what the "proceeds of" or funds "involved in " the offenses of aiding and abetting another offense, or being an accessory after the fact to an offense, could be.

a civil asset forfeiture complaint must "state the grounds for . . . in rem jurisdiction over the defendant property." Supp. R. G(2)(b).

The Complaint alleges only one basis for the Court's *in rem* jurisdiction: "The Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)." Compl. ¶ 4. Section 1355(b), and 28 U.S.C. § 1395 that is cross-referenced in § 1355(b), provide, in relevant part, that a forfeiture action or proceeding may be brought in "the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred," in "any district where such property is found," "in any district into which the property [is] brought," or "[w]henever property subject to forfeiture . . . is located in a foreign country, . . . in the United States District [C]ourt for the District of Columbia." 28 U.S.C. § 1355(b); 28 U.S.C. § 1395.[10]

The Complaint, however, makes only one allegation about the location of the Defendant Property: "The Defendant Property is currently in the custody of the United States Marshals Service in the District of Columbia." Compl. ¶ 16. Nowhere is it alleged that "any of the acts or omissions giving rise to the forfeiture occurred" in the District of Columbia or that the Defendant Property "is located in a foreign country." Accordingly, the only theory of this Court's *in rem* jurisdiction pleaded in the Complaint necessarily is that the Defendant Property was "brought" into the District of Columbia.

As noted above, the United States Marshals Service has publicly announced an arrangement with Coinbase, a company not located in the District of Columbia, to custody digital assets. Therefore, the bald assertion appears to be in contradiction of the USMS's own public

[10] The D.C. Circuit has held that § 1355(b) grants district courts *in rem* jurisdiction over property and is not merely a venue statute. *See United States v. All Funds in Acct. Nos. 747.034/278, 747.009/278, & 747.714/278 in Banco Espanol de Credito, Spain*, 295 F.3d 23, 27 (D.C. Cir. 2002).

statements regarding the location of cryptocurrencies such as those at issue here. In any event, the Government will not be able to prove that the Defendant Property was "brought" into the District of Columbia, because all of the evidence it could conceivably use to prove its location is suppressible. As discussed in greater detail below, *see* § III, *infra*, because the Government unlawfully seized the assets at the Subject Virtual Currency Addresses, those assets and all other evidence derived from them—including any evidence that Tether allegedly burned those unlawfully seized tokens and then reissued them (with the reissued tokens constituting the Defendant Property)—must be suppressed as the fruit of a poisonous tree.

Without the ability to point to the originally seized USDT tokens, or evidence of the subsequent history of those tokens, including their burning and reissuance in the form of different USDT tokens by Tether (which new USDT tokens constitute the Defendant Property), the Government has no means of establishing that it has seized the Defendant Property, or that the Defendant Property was at any point "brought" to the District of Columbia. Accordingly, the Government will not be able to establish that the Court has *in rem* jurisdiction over the Defendant Property, and certainly not under § 1355(b), and the case must be dismissed.

III. THE COURT SHOULD SUPPRESS THE DEFENDANT PROPERTY AND ALL RELATED EVIDENCE

This Court should suppress the Defendant Property and evidence obtained as the fruits of that illegal seizure, including any evidence that Tether allegedly burned and reissued the unlawfully seized tokens as the Defendant Property. The Government illegally seized the Defendant Property without a warrant in violation of the Fourth Amendment, and no exception to the warrant requirement applied. The Government's subsequent seizure of the Defendant Property pursuant to a warrant does not cure the initial warrantless seizure. The Court should thus preclude

the Government from using the Defendant Property and evidence derived from the unlawful seizure in this case.

A. The Defendant Property Was Seized Without a Warrant, and No Exception to the Warrant Requirement Applied

Consistent with the Fourth Amendment, the civil forfeiture statute generally requires that seizures "be made pursuant to a warrant." 18 U.S.C. § 981(b)(2); U.S. Const. amend. IV (prohibiting unreasonable seizures); *United States v. Proctor*, 489 F.3d 1348, 1353 (D.C. Cir. 2007) ("A seizure … conducted without a search warrant is per se unreasonable under the Fourth Amendment."). Under Section 981(b)(2)(B)(ii), the Government may seize property without a warrant where an "exception to the Fourth Amendment warrant requirement would apply." Thus, the forfeiture statute itself does not "create a new exception to the fourth amendment's warrant requirement." *United States v. Cosme*, 796 F.3d 226, 235 (2d Cir. 2015) (citation omitted). Rather, a warrantless seizure must meet one of "few specifically established and well delineated exceptions" to the Fourth Amendment warrant requirement. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); *see also Proctor*, 489 F.3d at 1353 (warrantless seizures are "per se unreasonable" subject "only to a few specifically established and well delineated exceptions").

The Government concededly seized the Defendant Property without a warrant. The Complaint alleges that in November 2023, the Government instructed Tether to "freeze" the Defendant Property (and other digital assets), Compl. ¶ 172, to facilitate the Government's then-ongoing investigation into alleged crypto confidence scams. This "freeze"—which completely cut off Infiniweb's access to and use of the subject funds in the digital wallets—constituted a seizure for which the Government lacked a warrant. See *Cosme*, 796 F.3d at 235 (characterizing a bank account freeze as a seizure for Fourth Amendment purposes); *see also Salmo v. United States*, No. 06-12909, 2006 WL 2975503, at *2 (E.D. Mich. Oct. 17, 2006) (explaining that "a seizure of

property occurs when there is some meaningful interference with an individual's possessory interest in that property") (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1983)).

The Government has offered no justification for its warrantless seizure of the Defendant Property. Nor could it. None of the traditional exceptions to the warrant requirement are applicable in this case.

The Government may claim—based on its allegation that it requested to freeze the assets after a failed law enforcement operation "appear[ed] to have triggered a substantial movement of illicit funds from some of the Subject Virtual Currency Addresses," Compl. ¶¶ 170, 172—that exigent circumstances justified the seizure of the Defendant Property. The Government's own actions in this case, however, reflect the vacuity of any such assertion. First, the Government *had no probable cause* to effect a seizure, with or without a warrant, in November 2023 and makes no attempt to describe any such basis. *Barham v. Ramsey*, 434 F.3d 565, 573 (D.C. Cir. 2006) ("It is firmly established that, to comport with the Fourth Amendment, a warrantless search or seizure must be predicated on particularized probable cause."). Second, the Government's Complaint asserts that the Seized Virtual Currency Addresses were essentially static, acting as pools for funds that did not move beyond those wallets (that is, of course, because the Government was misguidedly targeting a subset of treasury wallets of a legitimate company, rather than transient laundering wallets).

Even if an immediate freeze was justified (it was not), the Government's continued retention of the Defendant Property for nearly a year and a half without a warrant was an egregious violation of the Fourth Amendment. Exigent circumstances do not "immunize . . . lengthy, warrantless seizure[s]" of allegedly forfeitable property. *Cosme*, 796 F.3d at 235. Rather, a warrantless seizure "must be strictly circumscribed by the exigencies which justify its initiation,"

Mincey v. Arizona, 437 U.S. 385, 393 (1978), and the Government is required to obtain a warrant as soon as practicable after a warrantless seizure. *Cf. Zweibon v. Mitchell*, 516 F.2d 594, 631 (D.C. Cir. 1975) (explaining the presumption that a warrant should be obtained "whenever practicable, and exceptions to the warrant requirement have been based on exigent or other circumstances where delay would frustrate legitimate police activity"); U.S. Dep't of Justice, *Asset Forfeiture Policy Manual* at 6-10 (2025) (encouraging prosecutors to commence a judicial forfeiture action within 90 days of receiving a request by a potential claimant for the release of property that is not subject to administrative forfeiture in order to avoid an eventual adverse ruling by a court on Due Process grounds, *i.e.*, because "courts have applied the Due Process Clause to set limits on how long the government may retain seized property absent the initiation of forfeiture proceedings").

Here, the Government did not obtain a warrant to seize the Defendant Property until May 2015, almost *a year and a half after* the November 2023 warrantless freeze and seizure of the assets. The Government's extended, warrantless seizure of the Defendant Property violated the Fourth Amendment. *Accord Cosme*, 796 F.3d at 24-35 (holding that extended seizure of funds was not justified by exigent circumstances exception and thus violated the Fourth Amendment).

B. The Government's Subsequent Seizure of the Defendant Property Pursuant to a Warrant Does Not Render the Property Admissible

Nor does the Government's subsequent seizure of the Defendant Property pursuant to a warrant render the property admissible. Where the Government obtains a warrant after an unlawful seizure has occurred, it is nevertheless barred from using the unlawfully obtained evidence unless it can show that the evidence would have been obtained through an independent source absent the Government's misconduct. *See United States v. Dawkins*, 17 F.3d 399, 408 (D.C. Cir. 1994) (citing *Murray v. United States*, 487 U.S. 533 (1988)).

The Government cannot make that showing here. Nothing in the Complaint suggests that the Government could have or would have seized the precise digital assets that are the subject of this case without unlawfully freezing the property in the first place. Nor has the Government made any effort to provide an independent legal basis for retaining the Defendant Property. Rather, the Complaint suggests that the Government initially seized the property without a warrant in violation of the Fourth Amendment, and only obtained a warrant to retain the property without committing a continuing constitutional violation. Because the Government has not identified a basis for treating the subsequent seizure pursuant to a warrant as "independent" of the unlawful warrantless seizure, the Court should suppress the Defendant Property.

C. The Court Should Also Suppress Other Evidence Related to the Defendant Property

Finally, the Court should suppress all other evidence related to the Defendant Property—including any evidence that Tether allegedly burned and reissued the unlawfully seized tokens as the Defendant Property—as the unlawful fruit of the warrantless seizure of the Defendant Property. Evidence obtained as a result of an unconstitutional seizure is "fruit of the poisonous tree," *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963), and may be excluded under the exclusionary rule. *Dawkins*, 17 F.3d at 408 (explaining that the exclusionary rule "encompasses all indirectly derivative evidence of an unlawful search or seizure). Evidence stemming from the Government's freeze of the subject assets, including evidence that Tether burned and reissued some of the assets as the Defendant Property pursuant to a warrant, is inadmissible fruit of the unlawful seizure of the Defendant Property.

The Defendant Property and related evidence should be suppressed. As discussed above, *see* § II, *supra*, without this evidence, the Government will likely be unable to prove the allegedly illicit source of the property in its possession, and thus unable to articulate facts that justify its *in*

rem jurisdiction or meet its tracing burden. *See One 1958 Plymouth Sedan v. Pennsylvania*, 380 U.S. 693, 698 (1965) (explaining that evidence derived from a violation of the Fourth Amendment cannot be used in a forfeiture proceeding); *accord United States v. $639,558*, 955 F.2d 712, 715 & n.5 (D.C. Cir. 1992) (where "defendant" property is obtained illegally, *that property* is admissible in a forfeiture proceeding for the limited purpose of proving its existence and to establish in rem jurisdiction, whereas fruits of an illegal seizure remain subject to suppression for all other purposes).

IV. THE COURT SHOULD STRIKE PARAGRAPHS 239 AND 240 OF THE COMPLAINT, WHICH (INACCURATELY) RECOUNT CONFIDENTIAL SETTLEMENT COMMUNICATIONS THAT ARE INADMISSIBLE UNDER FEDERAL RULE OF EVIDENCE 408

Paragraphs 239 and 240 of the Complaint contain allegations based on inadmissible confidential settlement communications. The allegations are immaterial and prejudicial to Infiniweb, and they should be stricken from the Complaint pursuant to Federal Rule of Civil Procedure 12(f).

Under Federal Rule of Civil Procedure 12(f), the Court may strike from a pleading "any redundant, immaterial, impertinent, or scandalous matter." Fed. R. Civ. P. 12(f). A motion to strike a pleading on the grounds that it is impertinent and immaterial should be granted when "it can be shown that no evidence in support of the allegations would be admissible," *Cobell v. Norton*, 224 F.R.D. 266, 282 (D.D.C. 2004) (quoting *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887, 893 (2d Cir. 1976)), or where the allegations at issue are prejudicial to the moving party. *See, e.g. United States v. Trie*, 21 F. Supp. 2d 7, 20 (D.D.C. 1998); *Wiggins v. Philip Morris, Inc.*, 853 F. Supp. 457, 457–58 (D.D.C. 1994). For example, in *Lipsky*, the Court granted the defendant's motion to strike portions of the complaint because the allegations at issue were based on information that was inadmissible under Federal Rule of Evidence 410. *Lipsky*, 551 F.2d at 893.

Under *Lipsky*, allegations in a complaint that rely on clearly inadmissible evidence should be stricken as impertinent and immaterial.

Confidential settlement communications are protected by Federal Rule of Evidence 408. Rule 408 states that "conduct or a statement made during compromise negotiations about [a] claim" is "not admissible . . . to prove or disprove the validity or amount of a disputed claim." Fed. R. Evid. 408.

It is clear from the face of the Complaint that the allegations in paragraphs 239 and 240 purport to be based on compromise negotiations between the Government and counsel for Infiniweb in or around June 2024 and February 2025. Paragraph 239 begins, "In or around June 2024, an attorney from an international law firm claimed that their client owned the funds" associated with the virtual currency addresses at issue in the Complaint. Compl. ¶ 239. Paragraph 239 then goes on to describe the nature of the attorney's communications with the Government over a six-month period, casting the attorney—and ultimately, Infiniweb—in a negative light by stating that "counsel never provided answers to simple ownership questions." *Id.* Similarly, paragraph 240 begins, "In or around February 2025, an attorney from another law firm contacted the United States on behalf of a client claiming that they owned the funds" associated with the virtual currency addresses at issue in the Complaint. Compl. ¶ 240. Paragraph 240 then continues in the same manner as paragraph 239 by describing the nature of the communications between the Government and Defendant's counsel, then disparagingly stating that "[t]he law firm representing Infiniweb has not provided the United States with any additional information showing that the funds associated with the **SUBJECT VIRTUAL CURRENCY ADDRESSES** are derived from lawful sources." *Id.*

The communications referenced in paragraphs 239 AND 40 of the Complaint would be inadmissible at trial as confidential settlement communications under FRE 408, and their incorporation into the Complaint reeks of bad faith. Given that evidence concerning these communications will not be admissible if the case proceeds to trial, the Court should strike both paragraphs from the Complaint, and the allegations they contain should not be weighed by the Court in considering the sufficiency of the Complaint.[11]

CONCLUSION

For the foregoing reasons, Claimant Infiniweb Technology Inc. respectfully submits that the Government's Complaint must be dismissed; that the seized property and all evidence derived

[11] Beyond flagrantly violating Rule 408, the descriptions of the parties' confidential settlement communications in paragraphs 239 and 240 profoundly misrepresent the conversations that took place and the nature of the information provided to the Government by Infiniweb. The nature of counsel's outreach to the Government on behalf of Infiniweb is irrelevant to this action, and the paragraphs' inaccuracy—specifically their false depiction of Infiniweb and its counsel as unresponsive and unwilling to provide the Government with information—makes their inclusion in the Complaint prejudicial, another ground for striking them. *See Wiggins*, 853 F. Supp. at 457–58 (granting motion to strike complaint where allegations were irrelevant and prejudiced defendant by casting defendant in a negative light); *Trie*, 21 F. Supp. 2d at 20 (holding the same).

therefrom, including the Defendant Property, must be suppressed as fruits of an unlawful warrantless seizure; and that paragraphs 239 and 240 of the Complaint must be stricken.

Respectfully submitted,

/s/ Andrew C. Adams
Andrew C. Adams (*pro hac vice*)
Drew C. Harris (*pro hac vice*)
Steptoe LLP
1114 Avenue of the Americas
New York, NY 10036
(212) 957-3081
acadams@steptoe.com
dcharris@steptoe.com

Steven H. Levin (DC Bar No. 985290)
Steptoe LLP
1330 Connecticut Avenue, NW
Washington, DC 20036
(202) 429-8169
slevin@steptoe.com

Attorneys for Claimant Infiniweb Technology Inc.