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

STATUS REPORT OF CLAIMANT NIVEDITA KAUL

TO THE HONORABLE COURT:

Claimant Nivedita Kaul respectfully submits this individual status report pursuant to the August 7, 2026 Minute Order, requiring reports every thirty days after September 4, "until the stay is lifted." The thirtieth day fell on Sunday, October 4, so the period ran to Monday, October 5 (Fed. R. Civ. P. 6(a)(1)(C)); this report is timely. Claimant remains a party of record through her Verified Claim and Answer (Docs. 53, 54), which have not been stricken (see Tr. 54:3-5). The Court directed, for the prior round of reports, that a party outside the joint group "can file your own status report" (Tr. 60:8-9; see Minute Order of July 24, 2026). "Doc." identifies ECF entries; page citations identify ECF-stamped pages. "Tr." identifies the official transcript of the July 23, 2026 hearing (Doc. 84).

This report identifies developments material to the preservation and proposed disposition of the Defendant Property: the Court's September 30 orders; the continuing Turkish prosecution and newly assembled reporting concerning Grand Bazaar laundering infrastructure; unresolved questions concerning Infiniweb's competing claim; and a sworn, first-hand account of what the

United States Attorney said about where the seized funds should go. Each is cited to its source: the Government's own filings and statements, the judicial record in this action and in Türkiye, sworn evidence, or identified public reporting. Claimant will present the supporting evidence in her forthcoming filings. Claimant is the investigative originator of the proceedings and enforcement actions this report describes: the Turkish prosecution, the seizure of Wallet 0x82e, and the September 2026 enforcement operation all trace to the criminal complaint and forensic mapping she filed in Türkiye in February 2023 (Doc. 79-1 at 9-11).

An Exhibit Index is included with this filing and appears after the signature block. Nothing in this report waives or narrows any position Claimant has taken in Docs. 53, 54, 79, 94, 97, or 98.

I. COMPLIANCE WITH THE COURT'S SEPTEMBER 30, 2026 MINUTE ORDER

1. On September 30, the Court directed Claimant to file her motion for leave to amend her claim by October 14, 2026. Claimant had asked the Court to set such a date before any decision on Doc. 91 (Doc. 97 ¶ 8). She will file by October 14. She also intends to seek leave to amend her Answer to conform to the proposed amended claim, as previously noticed in Doc. 94 at 26-27.

2. The amendment will restate the documentary basis and nature of Claimant's asserted interest, the perfected Turkish judicial custody she relies upon, her investigative and asset-preservation contributions, and the continuing Turkish proceedings. Claimant preserves her objection to the exercise of in rem jurisdiction over Wallet 0x82e, stated in her original Answer (Doc. 54 at 33, Affirmative Defenses 2-3) and raised in her emergency motion (Doc. 79). Supplemental Rule G(5)(b) provides that a claimant waives such an objection "if the objection is not made by motion or stated in the answer." Claimant's objection was both stated in her Answer and made by motion; nothing has been waived. Seeking leave to amend is not consent to the United States' asserted custody or disposition of that property, and waives none of Claimant's objections.

3. The Government's motion to strike (Doc. 91) is directed at Claimant's Verified Claim (Doc. 53), Answer (Doc. 54) and emergency motion (Doc. 79). Doc. 91 should not be decided before the Court resolves her motion for leave to amend, which the Court has directed her to file by October 14, 2026, so that the Court considers the claim as it will stand. The Advisory Committee's note to Supplemental Rule G(8)(c) states that, "[a]s with other pleadings, the court should strike a claim or answer only if satisfied that an opportunity should not be afforded to cure the defects under Rule 15" (see Doc. 97 ¶ 8). Doc. 91 also relied on "the tentative settlement," which the Government put before the Court under seal "[f]or the sole purpose of proving DDG's assertion about the settlement false" (Doc. 91 at 17). The sealed filings that accompanied it (Docs. 92, 93) have since been struck (Minute Order of Sept. 30, 2026). To the extent Doc. 91 depends on that struck material, it now rests on nothing properly before the Court.

II. THE SEALED FILINGS (DOCS. 92, 93)

4. On September 30, 2026, the Court struck the Government's sealed filings (Docs. 92, 93) for non-compliance with Local Civil Rule 5.1(h)(1) and the Court's Standing Order, and directed that "Plaintiff shall file a motion to seal that complies with Local Civil Rule 5.1(h)(1) and the court's standing order." Claimant had raised both defects, the absence of a motion to seal and of any Hubbard analysis, before that order (Doc. 97 ¶ 4; Doc. 98 at 3-4). Five days later, as of the date of this report, the Government has not filed the motion to seal the Court directed.

5. Doc. 91 nevertheless invokes "the tentative settlement," described as "attached under seal," against Claimant (Doc. 91 at 17). Those materials have never been served on her (Doc. 97 ¶ 4). Any material offered against her must be properly filed and served, subject to lawful protective measures, before she can be required to answer its substance. See Fed. R. Civ. P. 5(a)(1)(D); Doc. 4 at 4, §§ 5.D-E; Doc. 88 ¶ 15. No compliant motion to seal, and no properly filed settlement

exhibit, is on the docket. The Government has not conferred with Claimant as the Standing Order requires (Doc. 4 at 4), and Claimant will oppose any motion to seal material that is used against her without being served on her.

III. THE PUBLIC RECORD AND SWORN ACCOUNTS BEARING ON THE DEFENDANT PROPERTY

6. Claimant brings the following items to the Court's attention. Mr. Welte's declaration (Exhibit E) is his sworn, first-hand account of his exchange with the United States Attorney, and Exhibit C is the email in which he recorded that exchange and sent it to her office (Ex. E ¶ 14). The statements he attributes to the United States Attorney are statements of a party opponent. See Fed. R. Evid. 801(d)(2)(D). Exhibits A, B, D and F to H are public reports and statements. They are offered to show what has been publicly reported and stated, and what has long been available to the Government, on matters Claimant will prove with admissible evidence in her forthcoming filings. The Government's own filings and statements in this action are cited by docket and transcript reference and speak for themselves.

A. Financial Times video report concerning Infiniweb Technology Inc. (Exhibit A)

7. On September 8, 2023, the Financial Times published a video report, "Premier League betting sponsors: closed doors and companies within companies."[1] The report was public more than two months before the Secret Service asked Tether, on or around November 20, 2023, to freeze the subject addresses (Doc. 1 ¶ 172); seventeen months before counsel for Infiniweb approached the Government in February 2025 (id. ¶ 240); and before the Government filed this action on June 18, 2025 (Doc. 1) and Infiniweb filed its Verified Claim on October 17, 2025 (Doc.

[1] "Premier League betting sponsors: closed doors and companies within companies," reported by James Sandy and Taro Yokosawa. It is available at https://www.ft.com/video/4bf67319-ce1e-4d13-a49d-120e12cc7d3d

23). The Financial Times published a transcript of the report on the same page. A copy, with Claimant's declaration identifying it, is attached as Exhibit A.

8. The report examines the ownership of betting brands that sponsored Premier League and other European football clubs.

(a) It reports that the registrants of several of those brands "weren't in fact gambling operators" but "service providers for gambling operators." Asking "whose money are they actually using?", the reporters "found that it was another company sitting on top called Infiniweb" (Ex. A at 14-15).

(b) It then states: "Infiniweb Technology, Inc. seemed like a ghost. The Manila address they gave to the Philippines gaming regulator turned out to be false. Their website could only be accessed with the help of an agent." The reporters add that "none of those receiving the donations" Infiniweb representatives made to police stations across the Philippines "were able to offer any contact information for the company itself." (Id.)

(c) The reporters "couldn't find" company documents for Infiniweb Technology, Inc. "anywhere in the Philippines." They found them instead in "[t]he British Virgin Islands," which the report describes as "the end of the line in our various searches for brand owners." (Id.)

(d) The report concludes that "we still don't know who's behind . . . Infiniweb and a host of brands still operating under BOE United Technology." (Id.)

9. These reported findings are consistent with matters already in the record:

(a) Infiniweb's Verified Claim describes it as "an online gaming and wagering company that is registered in the British Virgin Islands." It states that it "operates outside of the United States," and that U.S. users are blocked (Doc. 23 ¶¶ 2-3). It claims all seven subject

addresses, including Wallet 0x82e (id. ¶ 1), as "revenues belonging to Infiniweb, generated through the provision of Infiniweb's gaming and wagering services" (id. ¶ 5). It asserts only that none of those services "constitutes illegal activity under the laws of the United States" (id.); it does not assert that they are lawful where, by its own account, it operates. It is verified by "Zeng Youzong" as "Chief Executive Officer" (Doc. 23 at 4). It does not state who owns or controls Infiniweb.

(b) The Verified Complaint states that "[o]pen-source research regarding Infiniweb revealed minimal information about the company." It cites an article describing Infiniweb as "understood to have close links with Xionwei Technologies, which is accused of being involved in kidnapping and human trafficking" (Doc. 1 ¶ 240 & n.51).

(c) The Complaint further states that Infiniweb appeared on a "LIST OF CANCELLED OFFSHORE GAMING LICENSEES" posted by the Philippine Amusement and Gaming Corporation (id. ¶ 240 & n.52). The report, for its part, states that the Manila address Infiniweb gave "to the Philippines gaming regulator turned out to be false" (Ex. A at 15). Claimant's independent verification of the same Manila address confirmed it was not a genuine operating address (Doc. 79-15). The Complaint adds that Infiniweb's counsel "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. ¶ 240).

(d) Under the settlement the Government described at the July 23 hearing, "the government will send Infiniweb back a certain amount of those funds" (Tr. 39:22-25).

240. 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 five of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. The attorney stated that their client was an online gaming/gambling company named Infiniweb Technology, Inc. Open-source research regarding Infiniweb revealed minimal information about the company, including an article stating that the company "is understood to have close links with Xionwei Technologies, which is accused of being involved in kidnapping and human trafficking. The accusations of kidnapping and human trafficking were outlined in a 120-page report from 2023, submitted to the nineteenth congress of the Republic of the Philippines."[51] Inifiniweb was also listed on a "LIST OF CANCELLED OFFSHORE GAMING LICENSEES," appearing to be dated January 15, 2024, posted by the Philippine Amusement and Gaming Corporation.[52] The 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, unrelated to cryptocurrency confidence scams or other criminal activity.

[51] Philippe Auclair, Andy Brown, Jack Kerr, Samindra Kunti, Steve Menary, *Meet the hydras: tracing the illegal gambling operators that sponsor football* https://www.playthegame.org/news/meet-the-hydras-tracing-the-illegal-gambling-operators-that-sponsor-football/ (Jan. 30, 2024).

[52] Philippine Amusement and Gaming Corporation, *List Of Cancelled Offshore Gaming Licensees,* https://www.pagcor.ph/regulatory/pdf/offshore/list-of-cancelled-offshore-gaming-licensees.pdf (Jan. 15, 2024).

72

Figure 1 - Doc. 1 ¶ 240 & nn.51-52, at 72 (highlighting added).

10. Infiniweb is directly adverse to Claimant as to Wallet 0x82e. It claims the wallet's entire balance as its own "revenues" (Doc. 23 ¶¶ 1, 5), and that is the same property Claimant claims (Doc. 53).

(a) Before this action was filed, two claims were made to "five of the SUBJECT VIRTUAL CURRENCY ADDRESSES." The first was made in June 2024 by an international law firm for an unnamed client (Doc. 1 ¶ 239). The second was made in February 2025 by counsel for Infiniweb (id. ¶ 240).

(b) The Complaint does not identify which five.

(c) Infiniweb's own pre-suit claim, made through counsel in February 2025, was to five addresses (Doc. 1 ¶ 240). Its Verified Claim, filed eight months later, claims all seven, including Wallet 0x82e (Doc. 23 ¶ 1), and does not explain the difference (see Doc. 89 at 10).

(d) Infiniweb states that "[t]his matter first came to Infiniweb's attention through a warrantless seizure by the Government" on November 20, 2023, and that this "initial freeze" covered "a total of thirty-five wallets belonging to Infiniweb" (Doc. 28-1 at 14). Neither that motion nor its Verified Claim mentions Türkiye. Yet before November 20, 2023, a Turkish court had ordered Wallet 0x82e seized, listing it among wallets "themselves in the nature of items of the offence" (Doc. 79-5 at 2), and the Turkish prosecutor had asked Tether to block it, stating that "it has been established that members of the criminal organisation used the cold wallet" at that address "within the scope of their acts" (Doc. 79-6 at 2). Infiniweb now claims the same wallet's balance as its own gaming "revenues" (Doc. 23 ¶¶ 1, 5).

(e) The Government knows which five addresses were claimed in June 2024 and February 2025, and whether Wallet 0x82e was among them. Neither the Complaint nor any later Government filing identifies them. Claimant will seek that identification.

(f) The Government has described the settlement it is negotiating as one under which "we'll agree to a forfeiture of a certain amount of those funds, and . . . the government will send Infiniweb back a certain amount of those funds" (Tr. 39:22-25).

(g) The settling parties have stated that the settlement framework "would not address the motions filed by" Claimant (Doc. 85 at 2).

(h) The Government placed "the tentative settlement" before the Court as a sealed exhibit to its motion to strike Claimant's claim (Doc. 91 at 17). The Court has since struck the Government's sealed filings, Docs. 92 and 93 (Minute Order of Sept. 30, 2026).

After filing her motion for leave to amend, Claimant will challenge Infiniweb's claim to Token Group G, relying on Exhibit A and the record set out above.

Status Update and Notice of Settlement Agreement in Principle

Since the Court's order, the 2025 Parties have met and conferred and are pleased to report that they have been able to reach agreement on a settlement framework, subject to internal approval requirements at the Department of Justice and claimants' final review and execution.

Accordingly, the 2025 Parties respectfully request that that the Court reserve decision on the following motions: (1) Claimant Infiniweb Technology Inc.'s Motion to Dismiss Complaint for Forfeiture in rem, Motion to Suppress, and Motion to Strike (ECF No. 28); (2) Claimants 1-118's Motion to Transfer Venue (ECF No. 29); (3) the government's Motion to Strike Verified Claims of Claimants 1-118 (ECF No. 44); and (4) the government's Cross-Motion to Dismiss Potential Claimant Infiniweb's Motion to Dismiss (ECF No. 50) (collectively "the Motions").

The 2025 Parties propose to update the Court promptly once a decision on the proposed settlement framework is received, but in any event no later than 60 days from the date of this Status Report.

In the avoidance of doubt, the proposed settlement framework would not address the motions filed by putative claimant Nivie Kaul.

Figure 2 - Doc. 85 at 2 (highlighting added).

B. Public statements by Erin West concerning Türkiye (Exhibit B)

11. Erin West, formerly a Deputy District Attorney in Santa Clara County, is the person Claimant contacted on January 18, 2023, following Ms. West's public solicitation of

cryptocurrency crime victims. Ms. West referred her to Andrew Frey of the U.S. Secret Service (Doc. 53 ¶ 15; Doc. 94-1 ¶¶ 12-13; Doc. 94-3; Doc. 91-3).

(a) When Claimant told her that Mr. Frey had made contact, Ms. West replied: "Frey is the best in the nation" (Doc. 91-3).

(b) Claimant's earlier filings quote Ms. West, in a June 2025 LinkedIn video post, as crediting Mr. Frey as the "genius" who "devised a clever plan" and "figured out how to do a burn and reissue with Tether" (Doc. 79-1 at 16 & n.8; Doc. 79-2 ¶ 32). The text accompanying that video gave "[k]udos to Andrew Frey, Shawn Bradstreet at United States Secret Service and the rest of the team" (Doc. 79-18 at 2). The "burn and reissue" she credits took place on June 18, 2025 (Doc. 89 at 8). In the Government's own description, Tether "will destroy" the cryptocurrency held by the alleged perpetrators and "create separate cryptocurrency with the same value," which it sends to the government "representing a substitute asset" (Tr. 12:11-19). By then, Wallet 0x82e had been under the Turkish court's seizure order since August 11, 2023, and Tether had confirmed to the Turkish prosecutor that it was frozen (Docs. 79-5, 79-7).

(c) The Government filed correspondence between Mr. Frey and Claimant as exhibits to its motion to strike (Docs. 91-4 to 91-7).

(d) Press reporting cited in Claimant's filings attributes to Ms. West the statement that "whatever Turkey says doesn't have any bearing on US Secret Service" (Doc. 79-1 at 16 & n.9; Doc. 94 at 11).

12. On September 21, 2026, Ms. West published a LinkedIn post stating that "[i]n the last 90 days alone, law enforcement has raided scam operations in Pakistan, Timor-Leste, Laos, Turkey, and Madagascar," and that "Turkish authorities hit 286 locations and 42 call centers in a

single morning - with Israeli-linked ownership targeting victims across Europe, East Asia, and Africa"[2] (Exhibit B). The post thus cites, as an example of action against transnational scam operations, the very Turkish enforcement operation of September 18, 2026 described in Public statement of Akın Gürlek, Minister of Justice of the Republic of Türkiye[3] (¶ 22 below). The operation West's post cites is Claimant's own investigation's product: Claimant originated the Turkish proceedings that produced it (¶ 23 below). That stands in contrast to the statement attributed to her in the published report quoted in Docs. 79-1 and 94, that "whatever Turkey says doesn't have any bearing on US Secret Service" (Doc. 79-1 at 16 & n.9).

13. Exhibit B also contains a capture of comments on the post, taken on September 23, 2026 at 6:10 PM ET.

(a) It shows a comment by Roger Welte. Mr. Welte's LinkedIn headline describes him as a Principal Research Engineer at SRI (Ex. B; Ex. E ¶ 2). He also serves, as an unpaid volunteer, as Senior Policy Advocate and Director of Government Engagement of Digital Defenders Group ("DDG"), the nonprofit Claimant founded (Ex. E ¶ 5; Kaul Decl. ¶ 6; Ex. C at 3; Doc. 79-2 ¶ 5; Doc. 94-1 ¶ 24). His own family lost retirement and other funds to a cryptocurrency investment scam (Ex. E ¶ 4; Ex. C at 3). His comment reads: "Erin, why are you deleting the comments of actual victims? And never answering their questions? What are you hiding?" (Ex. B; Ex. E ¶ 21).

(b) Replying to that comment, the account of Operation Shamrock stated: "There were no questions in the deleted message, just unfounded accusations." It added: "We are not

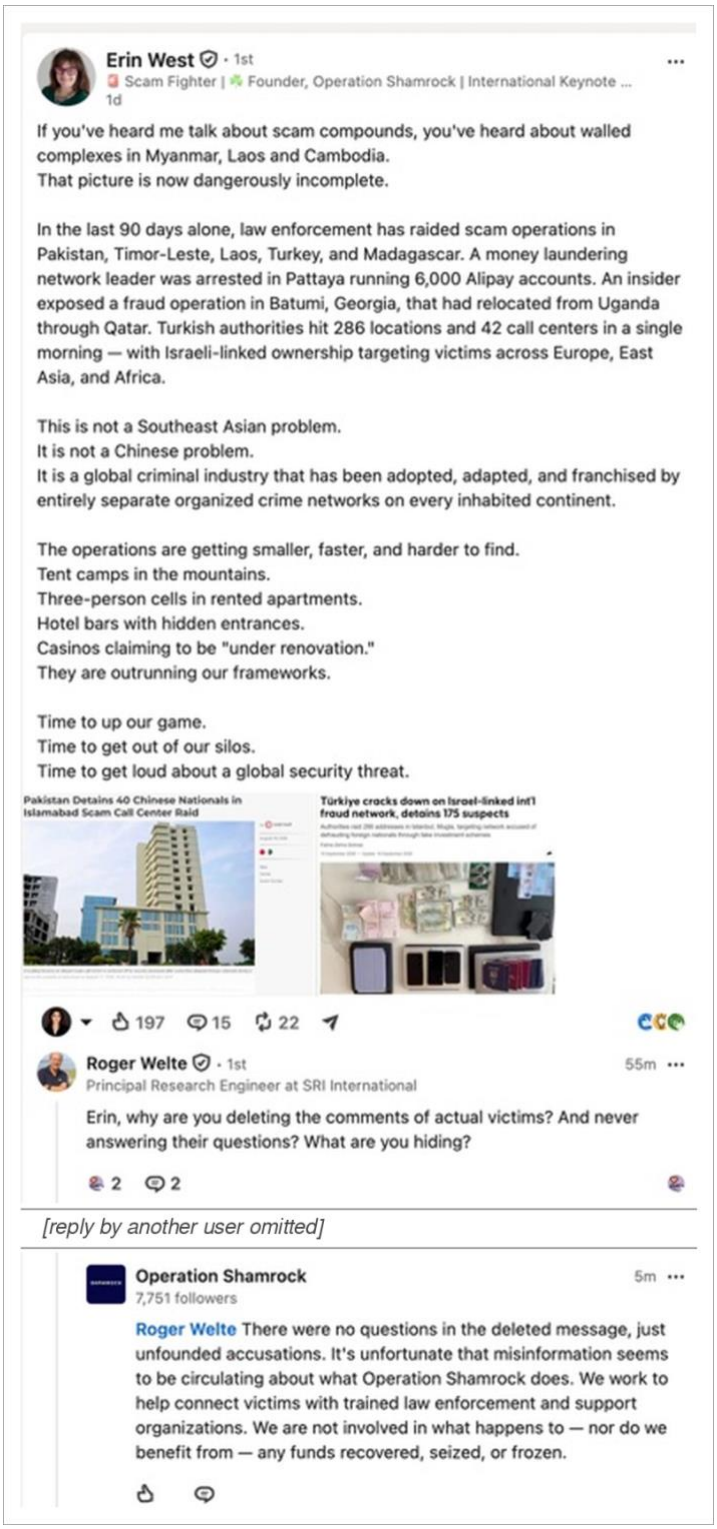
[2] "Turkish authorities hit 286 locations and 42 call centers in a single morning - with Israeli-linked ownership targeting victims across Europe, East Asia, and Africa" https://lnkd.in/p/gEEtgxfH

[3] Public statement of Akın Gürlek, Minister of Justice of the Republic of Türkiye, posted on X (September 18, 2026), https://x.com/abakingurlek/status/2100860597520752688, as accessed on October 5, 2026

involved in what happens to - nor do we benefit from - any funds recovered, seized, or frozen" (Ex. B). Ms. West's LinkedIn headline describes her as "Founder, Operation Shamrock."

(c) That reply, which itself refers to "the deleted message," was removed the same day, within three hours, before 9:00 p.m. ET, and Ms. West blocked Mr. Welte (Ex. E ¶¶ 21-22).

14. These statements matter because of the Turkish nexus. The laundering network was investigated in Türkiye (Investigation No. 2023/6371). A Turkish court ordered Wallet 0x82e seized, and Tether confirmed its freeze to the Turkish authorities, before any United States warrant was issued (Docs. 79-5, 79-6, 79-7; Doc. 53 ¶ 8). The court's order (August 11, 2023) and the prosecutor's request (October 11, 2023) also both preceded the Secret Service's own request, "[o]n or around November 20, 2023," that Tether "voluntarily freeze" the subject addresses (Doc. 1 ¶ 172), and came more than eighteen months before the United States obtained its seizure warrant "[o]n or about May 1, 2025" (Doc. 44 ¶ 5, at 2). The Government's own accounts of when its investigation began conflict: "[i]n November 2023," according to its Verified Complaint (Doc. 1 ¶ 50), but "January 9, 2023," according to its motion to strike (Doc. 91 at 5; Tr. 16:9). The Turkish nexus bears on issues Claimant will present with her Amended Verified Claim, including the Court's jurisdiction over Wallet 0x82e (Doc. 54, Aff. Def. 2; Doc. 79-1 § IV).



Erin West · 1st
Scam Fighter | Founder, Operation Shamrock | International Keynote ...
1d

If you've heard me talk about scam compounds, you've heard about walled complexes in Myanmar, Laos and Cambodia.
That picture is now dangerously incomplete.

In the last 90 days alone, law enforcement has raided scam operations in Pakistan, Timor-Leste, Laos, Turkey, and Madagascar. A money laundering network leader was arrested in Pattaya running 6,000 Alipay accounts. An insider exposed a fraud operation in Batumi, Georgia, that had relocated from Uganda through Qatar. Turkish authorities hit 286 locations and 42 call centers in a single morning — with Israeli-linked ownership targeting victims across Europe, East Asia, and Africa.

This is not a Southeast Asian problem.
It is not a Chinese problem.
It is a global criminal industry that has been adopted, adapted, and franchised by entirely separate organized crime networks on every inhabited continent.

The operations are getting smaller, faster, and harder to find.
Tent camps in the mountains.
Three-person cells in rented apartments.
Hotel bars with hidden entrances.
Casinos claiming to be "under renovation."
They are outrunning our frameworks.

Time to up our game.
Time to get out of our silos.
Time to get loud about a global security threat.

197 15 22

Roger Welte · 1st
Principal Research Engineer at SRI International
55m

Erin, why are you deleting the comments of actual victims? And never answering their questions? What are you hiding?

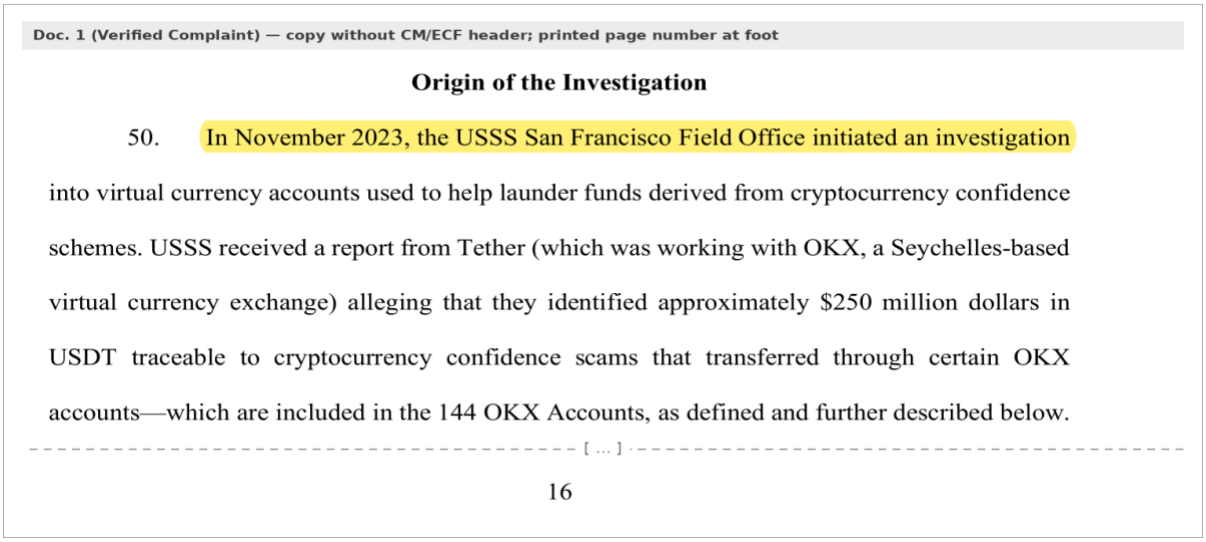
2 2

[reply by another user omitted]

Operation Shamrock
7,751 followers
5m

Roger Welte There were no questions in the deleted message, just unfounded accusations. It's unfortunate that misinformation seems to be circulating about what Operation Shamrock does. We work to help connect victims with trained law enforcement and support organizations. We are not involved in what happens to — nor do we benefit from — any funds recovered, seized, or frozen.

Figure 3 - Ex. B: LinkedIn post by Erin West, comment by Roger Welte and reply by the Operation Shamrock account, cropped as stated in the Declaration of Nivedita Kaul ¶ 2(e).



Doc. 1 (Verified Complaint) — copy without CM/ECF header; printed page number at foot

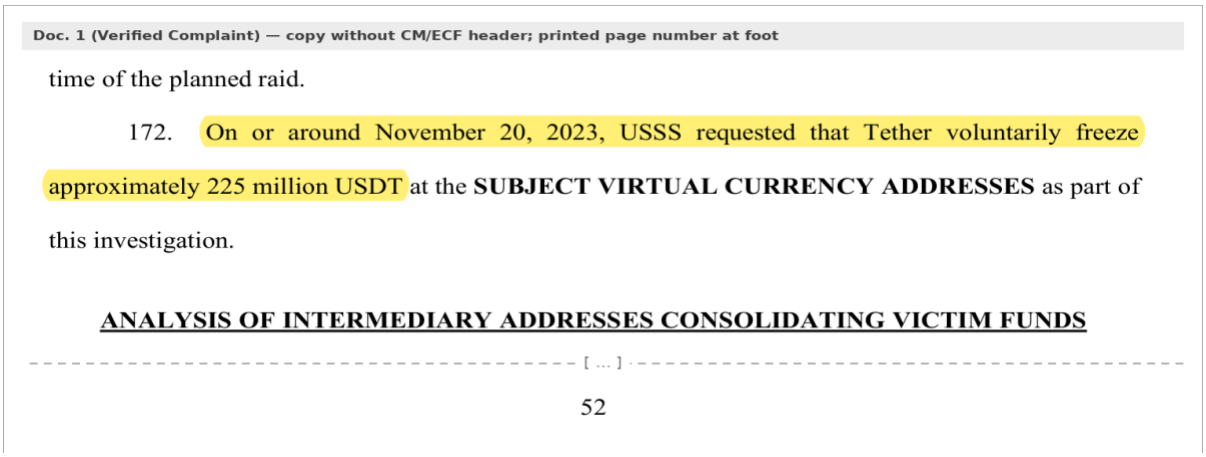
Origin of the Investigation

50. In November 2023, the USSS San Francisco Field Office initiated an investigation into virtual currency accounts used to help launder funds derived from cryptocurrency confidence schemes. USSS received a report from Tether (which was working with OKX, a Seychelles-based virtual currency exchange) alleging that they identified approximately $250 million dollars in USDT traceable to cryptocurrency confidence scams that transferred through certain OKX accounts—which are included in the 144 OKX Accounts, as defined and further described below.

[...]

16

Figure 4 - Doc. 1 ¶ 50, at 16 (highlighting added).



Doc. 1 (Verified Complaint) — copy without CM/ECF header; printed page number at foot

time of the planned raid.

172. On or around November 20, 2023, USSS requested that Tether voluntarily freeze approximately 225 million USDT at the **SUBJECT VIRTUAL CURRENCY ADDRESSES** as part of this investigation.

ANALYSIS OF INTERMEDIARY ADDRESSES CONSOLIDATING VICTIM FUNDS

[...]

52

Figure 5 - Doc. 1 ¶ 172, at 52 (highlighting added).

C. Sworn account of the United States Attorney's statement on the destination of the seized funds (Exhibits C and E)

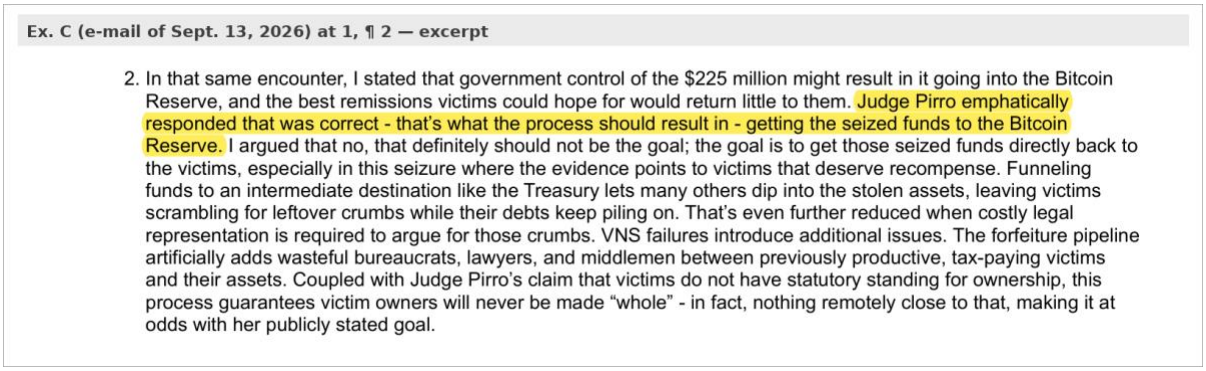
15. Mr. Welte attended the GASA Summit on September 2, 2026, representing DDG (Ex. C at 1; Ex. E ¶ 9). On September 13, 2026, he sent an account of his exchange there with the United States Attorney for the District of Columbia, Jeanine Ferris Pirro, to the Director of External Affairs of her office, who had been with her during the exchange and to whom she handed Mr. Welte off when she left, blind-copying Claimant (Ex. E ¶¶ 10-16). The Government's filings in this case are made in Ms. Pirro's name (e.g., Doc. 44 at 1; Doc. 91 at 23). Mr. Welte has

consented to the filing of his email (Kaul Decl. ¶ 6; Ex. E ¶ 23), and has made a declaration under 28 U.S.C. § 1746 describing the exchange (Ex. E ¶¶ 9-15).

(a) Mr. Welte states under penalty of perjury that he raised with her the Government's position that victims "voluntarily" gave up their funds, which he contrasted with her public statements about making victims "whole"; that she at first said she did not know what he was referring to; and that, once he identified the filing and the Assistant United States Attorney who prepared it, she appeared to recognize it (Ex. E ¶¶ 11-12; Ex. C at 1, ¶ 1). Doc. 44 was filed in the names of Ms. Pirro and AUSA Rick Blaylock, Jr. (Doc. 44 at 1). The "voluntarily" position is the one the Government took in moving to strike the claims of Claimants 1-118: their transfers, though "induced through misrepresentations," "were made voluntarily nonetheless" (Doc. 44 ¶ 6, at 2-3). In the same encounter, he "stated that government control of the $225 million might result in it going into the Bitcoin Reserve, and the best remissions victims could hope for would return little to them." His declaration confirms her answer and his email, written eleven days later, records it: "Judge Pirro emphatically responded that was correct - that's what the process should result in - getting the seized funds to the Bitcoin Reserve" (Ex. C at 1, ¶ 2). The remark concerned this case and "the $225 million."

(b) Mr. Welte has been a Principal Research Engineer at SRI International since November 2016. His earlier engineering career included GPS for military applications at Trimble Navigation (2005-2014). He holds a bachelor's degree in physics from the University of California, Berkeley, a master's degree in electrical engineering from the University of California, Davis, and a master's degree in applied mathematics from Santa Clara University (Ex. E ¶¶ 2-3). He states that he has "dedicated [his] life to DoD and national

security work" (Ex. C at 3; see Ex. E ¶ 2). He makes his declaration in his personal capacity, is not a party, and has received no payment or benefit for it (Ex. E ¶ 1).



Ex. C (e-mail of Sept. 13, 2026) at 1, ¶ 2 — excerpt

2. In that same encounter, I stated that government control of the $225 million might result in it going into the Bitcoin Reserve, and the best remissions victims could hope for would return little to them. Judge Pirro emphatically responded that was correct - that's what the process should result in - getting the seized funds to the Bitcoin Reserve. I argued that no, that definitely should not be the goal; the goal is to get those seized funds directly back to the victims, especially in this seizure where the evidence points to victims that deserve recompense. Funneling funds to an intermediate destination like the Treasury lets many others dip into the stolen assets, leaving victims scrambling for leftover crumbs while their debts keep piling on. That's even further reduced when costly legal representation is required to argue for those crumbs. VNS failures introduce additional issues. The forfeiture pipeline artificially adds wasteful bureaucrats, lawyers, and middlemen between previously productive, tax-paying victims and their assets. Coupled with Judge Pirro's claim that victims do not have statutory standing for ownership, this process guarantees victim owners will never be made "whole" - in fact, nothing remotely close to that, making it at odds with her publicly stated goal.

Figure 6 - Ex. C at 1, ¶ 2 (highlighting added).

16. Mr. Welte has given his account under penalty of perjury (Ex. E ¶¶ 10-12). Whether the remark reflects the Government's intentions for the defendant property is within the Government's own knowledge, and the Government has had the account since September 13, 2026: Mr. Welte sent it to a member of the U.S. Attorney's staff who was present for the exchange, writing "I hope you will share them with Judge Pirro" (Ex. C at 3; Ex. E ¶¶ 10, 14). He received no response (Ex. E ¶ 15). Claimant raises the account because it bears directly on matters before the Court.

(a) The Government has told the Court that Claimants 1-118, whose claims it moved to strike, "may still be made whole" through remission or mitigation (Doc. 44 ¶ 7, at 3). It has also told the Court that "[a] primary goal of the Department's Asset Forfeiture Program is to return forfeited funds to victims of crime" (id. ¶ 17, at 8), and that "[s]hould the government prevail in this forfeiture action, it intends to compensate victims through the routine process of remission" (id. ¶ 9, at 4). At the July 23 hearing, it said the settlement had been worked out "to make sure that victims are compensated in the way that we're describing" (Tr. 54:23-25). Its counsel wrote to Claimant on July 9, 2026: "Notwithstanding, we still intend to compensate victims" (Doc. 79-11 at 3). The Secret

Service's Special Agent in Charge in San Francisco publicly wrote that the analysts had worked on "this seizure, with the sole purpose of returning these stolen funds to the rightful victims" (Doc. 79-19 at 2; see Doc. 53 ¶ 17). When this action was filed, the Government announced that the U.S. Attorney's Office was working to "seize and forfeit stolen funds . . . all with the eye toward making victims whole" (Doc. 15 at 1-2 & n.2 (quoting Press Release, U.S. Dep't of Justice (June 18, 2025))).

(b) Under the settlement the Government has described, "the government will send Infiniweb back a certain amount of those funds" (Tr. 39:22-25). Victims, including the settling claimants and persons who are not parties, would go through a tiered remission process (Tr. 40:1-24), and "the government and parties are not agreeing to compensate any specific victim any specific amount of money" (Tr. 40:14-16).

(c) The Government has also told the Court that there are "many layers of government that have to approve" the settlement, including "the U.S. Attorney for our district" (Tr. 39:9-15). The official who, by Mr. Welte's sworn account, said the process should end in the Bitcoin Reserve is one of the officials who must approve the settlement. And the Government has told the Court that the forfeiture statutes "authorize victim compensation but do not mandate it as a matter of right" (Doc. 44 ¶ 17, at 8).

(d) Executive Order 14233 created a "Strategic Bitcoin Reserve" for forfeited bitcoin. It created a separate "United States Digital Asset Stockpile" for forfeited digital assets "other than BTC." Each is capitalized only with assets "finally forfeited" that are "not needed to satisfy requirements under 31 U.S.C. 9705 or released pursuant to subsection (d)." Subsection (d) permits their disposal where the Attorney General determines that they "can and should . . . be returned to identifiable and verifiable victims of crime." Exec. Order No.

14233, § 3(a), (b), (d)(i), 90 Fed. Reg. 11789 (Mar. 11, 2025). Forfeited USDT is a digital asset "other than BTC." Whichever vehicle would receive it, both are capitalized only with forfeited assets not released under subsection (d), the provision that permits their return to victims.

(e) The statement Mr. Welte attributes under oath to the United States Attorney, that the process should result in "getting the seized funds to the Bitcoin Reserve" (Ex. C at 1, ¶ 2; Ex. E ¶ 12), cannot be reconciled with those representations, and in particular with the Government's statement to this Court that "[s]hould the government prevail in this forfeiture action, it intends to compensate victims through the routine process of remission" (Doc. 44 ¶ 9, at 4). If the Government intends the defendant property, once forfeited, to go to a government reserve rather than to victims, that bears on:

(i) any settlement presented for approval;

(ii) the remission process to which the Government directs victims; and

(iii) Claimant's claim to Token Group G (see ¶ 26 below).

Claimant cites Exhibit C for Mr. Welte's written account of the exchange, sent to the United States Attorney's Office eleven days after the exchange, and for his role and background (Ex. C at 1, 3; Ex. E ¶ 14). The email is filed as sent; the opinions it expresses are Mr. Welte's own.

III. The proper mechanism for victim compensation is remission or mitigation, not contesting forfeiture.

17. A primary goal of the Department's Asset Forfeiture Program is to return forfeited funds to victims of crime.[27] The asset forfeiture statutes authorize victim compensation but do not mandate it as a matter of right. However, existing Attorney General guidance directs prosecutors to use asset forfeiture for the recovery of assets to compensate victims of crime, as permitted by law, whenever possible.[28]

Figure 7 - Doc. 44 ¶ 17, at 8 (highlighting added).

I. Background

On June 18, 2025, the United States filed a civil forfeiture complaint against more than $225 million in seized cryptocurrency alleged to be the proceeds of widespread cryptocurrency confidence scams. *See* Dkt. No. 1. This seizure froze the proceeds of an epidemic of fraud that is targeting American citizens from abroad, in order to reunite fraud victims with the funds stolen from them. As the United States Attorney for this District announced at the time this action was

[page break]

filed: "the U.S. Attorney's Office for the District of Columbia is taking a leading role in the fight against crypto-confidence scams, partnering with law enforcement throughout the country to seize and forfeit stolen funds and rip them from the hands of foreign criminals, *all with the eye toward making victims whole*." (emphasis added).[2]

[text omitted]

[2] Press Release, "United States Files Civil Forfeiture Complaint Against $225M in Funds Involved in Cryptocurrency Investment Fraud Money Laundering," U.S. Dep't of Justice (June 18, 2025), *available at* https://www.justice.gov/opa/pr/united-states-files-civil-forfeiture-complaint-against-225m-funds-involved-cryptocurrency (last visited Sept. 17, 2025).

Figure 8 - Doc. 15 at 1-2 & n.2 (Claimants 1-118's motion; italics and underlining in original; highlighting added).

D. Wall Street Journal report (Exhibit D)

17. On September 9, 2026, The Wall Street Journal published "They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It,"[4] . A copy is attached as Exhibit D. Among other things, it reports the following.

[4] "They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It," by Dylan Tokar (https://www.wsj.com/finance/currencies/crypto-investment-scam-victims-big-tuna-a489ece6)

(a) *Claimant's role in Türkiye.* The report states that Claimant "filed a legal claim in Turkey, where she had tracked some of her money. That sparked a probe into what Turkish prosecutors have described as a professional money-laundering ring, a tributary to the vast shadow economy underpinning the global scam industry." (Ex. D at 1.) It later describes Claimant as the victim "whose efforts kicked off a sprawling investigation in Turkey," and the wallet she seeks as "the wallet targeted by Turkish prosecutors." (Ex. D at 7.)

(b) *The Turkish seizure and the United States' later custody.* "A Turkish court in 2023 ordered the seizure of a digital wallet . . . from which Kaul says her losses would have been repaid." The report continues: "Before Turkey could move to distribute the money, U.S. law enforcement took custody of the wallet sought by Kaul, along with other crypto holdings totaling $225 million, in an operation dubbed Big Tuna that aimed to disrupt an alleged scam compound in the Philippines." (Ex. D at 1.)

(c) *The Turkish prosecution.* "Since Kaul took her legal crusade to Turkey, prosecutors there have filed a 1,548-page indictment describing a money-laundering operation they say operated out of Istanbul's Grand Bazaar . . . . As of July, the Turkish investigation, which is ongoing, had yielded more than 130 arrests." The report adds: "The U.S. hasn't filed any criminal charges connected to Big Tuna." (Ex. D at 7.)

(d) *The Government's position on Claimant.* The report states that "Justice Department attorneys have said Kaul's funds aren't traceable to the wallets seized in the Big Tuna case, though they have said she can still apply along with other victims when the case concludes." It also states that they "have dismissed the Turkish order as a basis for any claim over the wallet." (Ex. D at 7.) That position is wrong, for the reasons stated in Doc. 94, and the Government's own papers contradict it. The Secret Service tracing advice the

Government filed as Exhibit 7 to Doc. 91, which it captions "Funds Dissipated," replied to an email about a different address, which is not one of the seven subject addresses, and is dated June 6, 2023, five months before the investigation the Complaint says began in "November 2023" (Doc. 91-6 at 2; Doc. 91-7 at 1; Doc. 1 ¶¶ 15, 50). The Government's own motion describes what the Secret Service told her as being that "those funds unidentified by Kaul were not part of a current balance in the reported wallet address," and says that her funds "dissipated through a fast-moving money laundering network" (Doc. 91 at 12). Its Verified Complaint states that the Intermediary Groups, "along with the SUBJECT VIRTUAL CURRENCY ADDRESSES, also transferred hundreds of millions of dollars in virtual currency back and forth between each other in a manner that appears consistent with the repeated efforts to conceal the nature, location, source, ownership, and control of crime proceeds, and frustrate law enforcement's tracing efforts" (Doc. 1 ¶ 176).

(e) *Tether.* "El Salvador-based Tether initially declined a request to freeze the USDT held in two suspicious wallets, according to Justice Department attorneys. . . . By November, the company told the government it was ready to help." (Ex. D at 3.)

(f) *Infiniweb.* "Lawyers for the government have yet to respond to Infiniweb's claim, or explain how the alleged scam proceeds ended up in the company's possession." "Infiniweb declined to comment, citing the active litigation." (Ex. D at 6.) The Government has filed nothing since that answers the question. Its response to Infiniweb's motion to dismiss is procedural. It contends that Supplemental Rule G "Protects the United States from Responding to a Potential Claimant's Motion to Dismiss Until Standing Discovery is Complete" (Doc. 47 at 11, § I.D.; see Doc. 50), and it has told the Court that Infiniweb "has partially answered some of the 18 special interrogatories" (Doc. 47 at 7). Yet under the

settlement it describes, "the government will send Infiniweb back a certain amount of those funds" (Tr. 39:22-25).

(g) *The stated aim.* "U.S. Attorney Jeanine Pirro announced the $225 million seizure at a press conference in June 2025. The DC's attorney's office was taking a lead on fighting crypto scams with an 'eye toward making victims whole,' Pirro said in a press release at the time." (Ex. D at 6; see ¶ 16(a) above.)

18. The report is public independent reporting by a national newspaper on matters Claimant has raised. It reports:

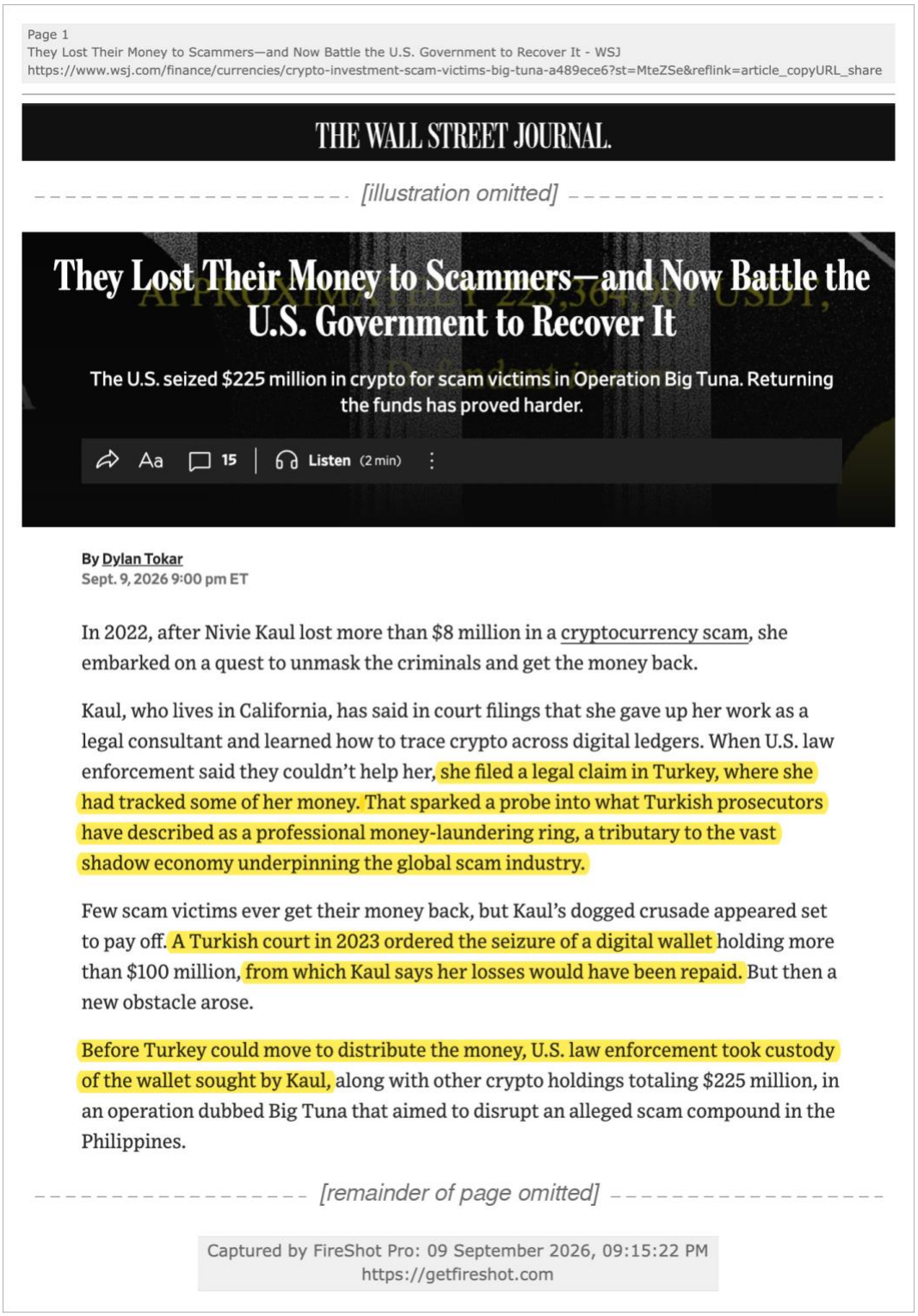
(a) that Claimant's legal claim in Türkiye "sparked a probe" by Turkish prosecutors;

(b) that a Turkish court ordered the seizure in 2023 of the wallet she sought;

(c) that United States law enforcement took custody of that wallet "[b]efore Turkey could move to distribute the money"; and

(d) that the Turkish prosecution has produced an indictment and arrests, while the United States "hasn't filed any criminal charges connected to Big Tuna."

It also reports that, when it was published, the Government had yet to "explain how the alleged scam proceeds ended up in [Infiniweb's] possession." The report bears on the Turkish nexus (¶¶ 14, 19-23), on Infiniweb's claim (¶¶ 9-10), and on Claimant's claim to Token Group G.



Page 1
They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It - WSJ
https://www.wsj.com/finance/currencies/crypto-investment-scam-victims-big-tuna-a489ece6?st=MteZSe&reflink=article_copyURL_share

THE WALL STREET JOURNAL.

[illustration omitted]

They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It

The U.S. seized $225 million in crypto for scam victims in Operation Big Tuna. Returning the funds has proved harder.

Aa 15 | Listen (2 min)

By Dylan Tokar
Sept. 9, 2026 9:00 pm ET

In 2022, after Nivie Kaul lost more than $8 million in a cryptocurrency scam, she embarked on a quest to unmask the criminals and get the money back.

Kaul, who lives in California, has said in court filings that she gave up her work as a legal consultant and learned how to trace crypto across digital ledgers. When U.S. law enforcement said they couldn't help her, she filed a legal claim in Turkey, where she had tracked some of her money. That sparked a probe into what Turkish prosecutors have described as a professional money-laundering ring, a tributary to the vast shadow economy underpinning the global scam industry.

Few scam victims ever get their money back, but Kaul's dogged crusade appeared set to pay off. A Turkish court in 2023 ordered the seizure of a digital wallet holding more than $100 million, from which Kaul says her losses would have been repaid. But then a new obstacle arose.

Before Turkey could move to distribute the money, U.S. law enforcement took custody of the wallet sought by Kaul, along with other crypto holdings totaling $225 million, in an operation dubbed Big Tuna that aimed to disrupt an alleged scam compound in the Philippines.

[remainder of page omitted]

Captured by FireShot Pro: 09 September 2026, 09:15:22 PM
https://getfireshot.com

Figure 9 - Ex. D at 1 (illustration and remainder of page omitted; highlighting added).

But last month a Justice Department attorney said the department was close to striking a deal with both Infiniweb and victims that could involve appointing an administrator to oversee claims and giving preference to victims who could trace their funds to the suspicious wallets identified in the Big Tuna case.

One victim whose claim to the seized funds remains in contention is Kaul, whose efforts kicked off a sprawling investigation in Turkey.

Justice Department attorneys have said Kaul's funds aren't traceable to the wallets seized in the Big Tuna case, though they have said she can still apply along with other victims when the case concludes.

Since Kaul took her legal crusade to Turkey, prosecutors there have filed a 1,548-page indictment describing a money-laundering operation they say operated out of Istanbul's Grand Bazaar—a 500-year-old shopping market stretching back to the Ottoman Empire. As of July, the Turkish investigation, which is ongoing, had yielded more than 130 arrests.

The U.S. hasn't filed any criminal charges connected to Big Tuna.

Kaul launched an organization called the Digital Defenders Group, aimed at helping other victims recover their funds, and has said she identified more than 200 other scam victims who were victims of the Turkish money laundering ring.

Kaul recently asked the judge overseeing the Justice Department's $225 million seizure to set aside the wallet targeted by Turkish prosecutors, arguing that the Turkish court's seizure order gave her special status over the funds. Justice Department attorneys have dismissed the Turkish order as a basis for any claim over the wallet.

"I have had no income for more than three years," Kaul wrote in a recent court filing. "I have funded my investigation, the Turkish proceedings, and DDG's work from my own savings."

– – – – – – – – – – *[remainder of page (related links, author note, "Up Next") omitted]* – – – – – – – – – –

Captured by FireShot Pro: 09 September 2026, 09:15:22 PM
https://getfireshot.com

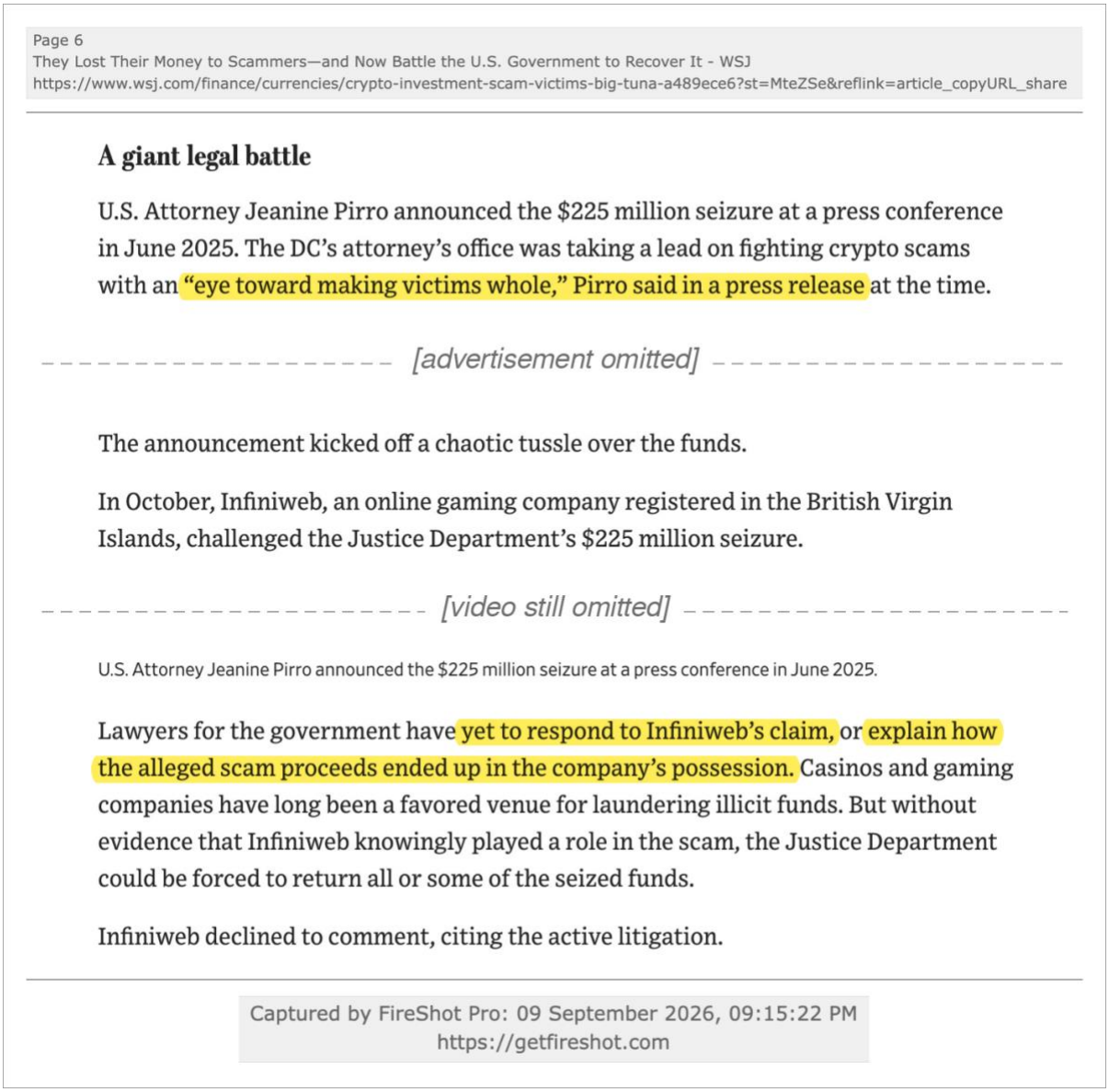
Figure 10 - Ex. D at 7 (remainder of page omitted; highlighting added).



Page 3
They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It - WSJ
https://www.wsj.com/finance/currencies/crypto-investment-scam-victims-big-tuna-a489ece6?st=MteZSe&reflink=article_copyURL_share

El Salvador-based Tether initially declined a request to freeze the USDT held in two suspicious wallets, according to Justice Department attorneys. Agents kept an eye on the funds. In the months that followed, with USDT's reputation as the crypto of choice for money launderers growing, pressure built on Tether to do more to police its digital currency. By November, the company told the government it was ready to help.

Figure 11 - Ex. D at 3 (highlighting added).



Page 6
They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It - WSJ
https://www.wsj.com/finance/currencies/crypto-investment-scam-victims-big-tuna-a489ece6?st=MteZSe&reflink=article_copyURL_share

A giant legal battle

U.S. Attorney Jeanine Pirro announced the $225 million seizure at a press conference in June 2025. The DC's attorney's office was taking a lead on fighting crypto scams with an "eye toward making victims whole," Pirro said in a press release at the time.

[advertisement omitted]

The announcement kicked off a chaotic tussle over the funds.

In October, Infiniweb, an online gaming company registered in the British Virgin Islands, challenged the Justice Department's $225 million seizure.

[video still omitted]

U.S. Attorney Jeanine Pirro announced the $225 million seizure at a press conference in June 2025.

Lawyers for the government have yet to respond to Infiniweb's claim, or explain how the alleged scam proceeds ended up in the company's possession. Casinos and gaming companies have long been a favored venue for laundering illicit funds. But without evidence that Infiniweb knowingly played a role in the scam, the Justice Department could be forced to return all or some of the seized funds.

Infiniweb declined to comment, citing the active litigation.

Captured by FireShot Pro: 09 September 2026, 09:15:22 PM
https://getfireshot.com

Figure 12 - Ex. D at 6 (advertisement and video still omitted; highlighting added).

E. Continuing Turkish prosecution and enforcement (Exhibits F to H)

19. The decision of the Ankara West 1st Criminal Judgeship of Peace of August 11, 2023 (Decision No. 2023/5986, Investigation No. 2023/6371) expressly lists Wallet 0x82e. The certified translation, already before the Court, records that "THE REQUEST IS GRANTED" and "THEIR SEIZURE IS ORDERED," and directs that the file and decision be returned to the prosecutor "for the necessary action," subject to a seven-day objection procedure (Doc. 79-5 at 2-3). The prosecutor's October 11, 2023 request that Tether block the wallet is Doc. 79-6, and Tether's confirmation that the address "is now frozen" is Doc. 79-7 (see Doc. 53 ¶ 8). The Government calls it "an inchoate order which never matured into a judgment or a perfected lien" and "preliminary inchoate orders" (Doc. 91 at 19, 20). It was neither (Doc. 94 at 13). The following public-record materials bear on that characterization.

20. On July 10, 2026, the Anadolu Agency reported that the Istanbul Chief Public Prosecutor's Office had prepared an indictment against 504 suspects in the Grand Bazaar (Kapalıçarşı) investigation, 134 of them in pretrial detention and 36 of them fugitives, and had sent it to the high criminal court. It further reported that, after a report by MASAK (Türkiye's Financial Crimes Investigation Board) established that criminal proceeds had been laundered through certain currency-exchange offices operating in the Grand Bazaar, an earlier decision of non-prosecution concerning certain exchange-office officials was lifted and the investigation against them continued (Anadolu Ajansı, "'Kapalıçarşı soruşturması'nda 504 şüpheliye iddianame,"[5]). This is the Grand Bazaar indictment reported by The Wall Street Journal: "[s]ince Kaul took her legal crusade to Turkey, prosecutors there have filed a 1,548-page indictment describing a money-

[5] Anadolu Ajansı, "'Kapalıçarşı soruşturması'nda 504 şüpheliye iddianame," as published by Habertürk (July 10, 2026), https://www.haberturk.com/son-dakika-haberi-kapalicarsi-sorusturmasinda-504-supheliye-iddianame-3897553, as accessed on October 5, 2026

laundering operation they say operated out of Istanbul's Grand Bazaar," and "the Turkish investigation, which is ongoing, had yielded more than 130 arrests" (Ex. D at 7).

21. A July 10, 2026 report in Türkiye Gazetesi describes a 1,548-page main indictment with a 138-page cover section; an internal accounting infrastructure, the "M80," used to track funds assigned to persons and companies and their onward transfer through exchange offices and cryptocurrency accounts; and 1,112 indictments prepared nationwide concerning the described fraud method and that proceeds were converted mainly into stablecoins such as USDT and sent to foreign-linked accounts. (Türkiye Gazetesi, "1112 iddianame, binlerce mağdur! Kapalıçarşı'da 'M80' ile 40 milyarlık para trafiği, kara para sistemi nasıl işledi?" [6]).

22. On September 18, 2026, Türkiye's Minister of Justice, Akın Gürlek, publicly announced that, in four investigations by the Istanbul Chief Public Prosecutor's Office into call centers defrauding foreign nationals through forex and cryptocurrency investment schemes, simultaneous operations had been carried out at 286 addresses in Istanbul and Muğla, targeting 42 call centers belonging to 28 companies and 239 suspects; that as of 10:00 that morning 175 suspects had been apprehended, with operations continuing; and that the investigation drew on MASAK analyses, intelligence and police findings, and hundreds of victim complaints obtained through Interpol (Public statement of Akın Gürlek, Minister of Justice of the Republic of Türkiye[7]). Those are the figures in Ms. West's own post: "Turkish authorities hit 286 locations and 42 call centers in a single morning" (Ex. B; ¶ 12 above).

---

[6] Türkiye Gazetesi, "1112 iddianame, binlerce mağdur! Kapalıçarşı'da 'M80' ile 40 milyarlık para trafiği, kara para sistemi nasıl işledi?" (July 10, 2026), https://www.turkiyegazetesi.com.tr/gundem/1112-iddianame-binlerce-magdur-kapalicarsida-m80-ile-40-milyarlik-para-trafigi-kara-p-1802427, as accessed on October 5, 2026

[7] Public statement of Akın Gürlek, Minister of Justice of the Republic of Türkiye, posted on X (September 18, 2026), https://x.com/abakingurlek/status/2100860597520752688, as accessed on October 5, 2026

23. Claimant's investigation shows that she is the investigative originator of these proceedings and of the September 18 operation concerning the same laundering infrastructure she identified in 2023. Her February 2023 criminal complaint and forensic work established the predicate for Investigation No. 2023/6371, the seizure of Wallet 0x82e, and the prosecutions that followed (Doc. 79-1 at 9-11). That is not her assertion alone: The Wall Street Journal reports that her claim in Türkiye "sparked a probe" and that her "efforts kicked off a sprawling investigation in Turkey," which has since produced the 1,548-page Grand Bazaar indictment (Ex. D at 1, 7). The points of continuity (the Grand Bazaar currency-exchange nexus, the internal accounting infrastructure and the actors under investigation), and the underlying actor, wallet and infrastructure links, will be set out in her forthcoming filings. These matters show a functioning prosecution and an implemented judicial measure, not "an inchoate order which never matured" (Doc. 91 at 19). The August 2023 order took effect when it was made: the prosecutor invoked it to have Tether block Wallet 0x82e, and Tether confirmed that the wallet was frozen (Docs. 79-6, 79-7; Doc. 53 ¶ 8). It did not need to "mature" into these later events, and the later events did not create it.

Claimant submits that they show the infrastructure the order addressed remained operational and under active prosecution in Türkiye, while the United States has filed no criminal charges (Ex. D at 7).

F. Statements in the record, side by side

24. Claimant sets out below, side by side and in the speakers' own words, statements that bear on matters she will address in her forthcoming filings. Each is quoted from the record or from the exhibits to this report.

Topic	Statement	Statement
When the United States investigation began	Verified Complaint: "In November 2023, the USSS San Francisco Field Office initiated an investigation into virtual currency accounts used to help launder funds derived from cryptocurrency confidence schemes." (Doc. 1 ¶ 50.)	Motion to strike: "The United States Secret Service ('USSS') began this investigation on January 9, 2023." (Doc. 91 at 5.) Hearing: "this investigation started on January 9, 2023" (Tr. 16:9).
The Secret Service's tracing advice to Claimant	Motion to strike: "The USSS undertook tracing using established accounting methods and advised Kaul that her property did not trace to the defendant property." (Doc. 91 at 19.) The same motion says her funds "dissipated through a fast-moving money laundering network," and that the Secret Service told her "those funds unidentified by Kaul were not part of a current balance in the reported wallet address" (Doc. 91 at 12).	The Government's exhibit: "your funds are not part of the current balance in this wallet address" (Doc. 91-7 at 1), in a reply dated June 6, 2023 and headed "RE: Good news - DBEX seizure" to an email naming "TARGET WALLET ADDRESS: 0x450195A34602FA0f8F1eaa82646ABeAd93641953" (Doc. 91-6 at 2). That address is not one of the seven subject addresses (Doc. 1 ¶ 15), and the reply predates by five months the investigation the Complaint says began in "November 2023" (Doc. 1 ¶ 50).
The stated aim, and the reported destination of the funds	"A primary goal of the Department's Asset Forfeiture Program is to return forfeited funds to victims of crime" (Doc. 44 ¶ 17, at 8); "Should the government prevail in this forfeiture action, it intends to compensate victims through the routine process of remission" (id. ¶ 9, at 4); "all with the eye toward making victims whole" (Doc. 15 at 1-2 & n.2).	As Mr. Welte recorded it, and has since sworn to it: "Judge Pirro emphatically responded that was correct - that's what the process should result in - getting the seized funds to the Bitcoin Reserve" (Ex. C at 1, ¶ 2; Ex. E ¶¶ 12, 15).

IV. OTHER MATTERS

25. *Pending motions.* Claimant's emergency motion (Doc. 79), the remaining reliefs in her interim motion (Doc. 94), and her request docketed as Doc. 99 remain pending. Claimant maintains every position stated in Docs. 79, 94, 97 and 98. The Government has filed no memorandum in opposition to Doc. 79 or Doc. 94; its Doc. 91 moves to strike Doc. 79 instead (its certificate of

service describes Doc. 91 as a "Motion to Strike Nivedita Kaul and Response," but it is captioned and docketed only as a motion to strike (Doc. 91 at 24)), and, apart from joining the 2025 Parties' joint status report of September 4, 2026 (Doc. 96), it has made no filing in this action since August 14, 2026. That is, although the 2025 Parties told the Court on August 6 that the Government "will continue to address any motion practice by all non-settling parties" (Doc. 85 at 1), described the stay they sought as a stay of "motion practice between the 2025 Parties" (Doc. 96 at 1), and stated on September 4 that they "are not seeking a stay of either" Doc. 79 or Doc. 91 (Doc. 96 at 2). The time for any opposition to Doc. 79 and Doc. 94 under Local Civil Rule 7(b) has run, and Claimant has asked that both be treated as conceded (Docs. 98, 99). The Government told Claimant at conferral that "[t]he government is opposed" to Doc. 94 (Doc. 98 at 3), but it has filed no opposition to either motion.

26. *Settlement.* None of the 2025 Parties has contacted Claimant about the settlement since her last report.

(a) The "2025 Parties" are the Government, Infiniweb, Claimants 1-118 and Claimants 119-266 (Doc. 85 at 1).

(b) Claimant has never been invited to take part in the settlement negotiations. The Government has told the Court that it "left open the possibility to invite Ms. Kaul to the tentative agreement once approved by the Deputy Attorney General," that is, only after approval, and that "that door is now closed" (Doc. 91 at 4).

(i) The June 12, 2026 joint status report says that "the government has reached out to claimant Kaul" (Doc. 70 at 5 n.1). What Claimant received was a request to join that report, made although she had not been invited to take part in the negotiations.

(ii) Apart from emailing her a courtesy copy of Doc. 91 (Doc. 91 at 24), counsel for the Government has written to Claimant only in reply to her emails. One of those replies, beginning "Confirming that we received your email, Ms. Kaul. We appreciate you reaching out," told her that the Government intended to move to strike her claim and invited her to withdraw it (Doc. 79-11 at 3).

(c) At the July 23 hearing, Claimant told the Court: "I haven't been invited to the settlement talks. I haven't been invited to any of the meetings. I have been conspicuously excluded." (Tr. 46:8-10).

(d) The Court then asked the Government "how do you propose we proceed in light of the fact that you have one claim that I think has been filed here that's outside of the scope of the settlement. Is the settlement going to somehow address that?" (Tr. 53:22-25), referring to "at least one claimant who I think has a filed claim here that's not been stricken" (Tr. 54:3-5). The Government answered that "their claims are untimely, so they aren't privy to the settlement negotiations" (Tr. 56:20-22). Asked "Was Ms. Kaul's claim objected to as untimely?", it answered: "Your Honor, we may strike her, and the government intends to strike her" (Tr. 56:23-57:1). No objection to Claimant's claim, on timeliness or any other ground, had then been filed. The Government's first came three weeks later, in Doc. 91, filed a week after the Court stayed the case. The Court stated: "I have got to make sure that I'm respecting everybody's rights who is before the Court as well. I assume the settlement is going to deal with that" (Tr. 59:24-60:2). The settling parties then told the Court that the framework "would not address the motions filed by" Claimant (Doc. 85 at 2).

(e) Claimant has not seen the terms of the settlement. The Government placed "the tentative settlement" before the Court only as a sealed exhibit to its motion to strike (Doc. 91 at 17).

The sealed filings were never served on her (Doc. 97 ¶ 4) and the Court has since struck them (Docs. 92, 93; Minute Order of Sept. 30, 2026). The further update the 2025 Parties proposed to file "no later than September 25, 2026" (Doc. 96 at 2) was not filed. Any proposed settlement, consent judgment or order of forfeiture that would dispose of Token Group G, including any portion filed under seal, must be served on Claimant and must not be entered until she has been heard (Doc. 97 ¶ 10(b)). Claimants 1-118 have themselves told the Court that "a court-approved settlement cannot dispose of Claimants' filed claims without their consent" (Doc. 65 at 9).

27. *Doc. 101.* On October 5, 2026, the settling parties filed a further joint status report (Doc. 101). It reports no development: the agreement in principle "remains under consideration by the 2025 Parties and subject to approval pursuant to Department of Justice policy" (Doc. 101 at 1) - the same terms reported on September 4 (Doc. 96 at 1-2). The further update the settling parties proposed on September 4, "no later than September 25, 2026" (Doc. 96 at 2), was not filed, and Doc. 101 does not mention it.

Doc. 101 states that the settling parties "are not seeking a stay of any of these motions, which would not be resolved by the pending agreement in principle" (Doc. 101 at 2). That is the third successive acknowledgment that the proposed settlement would not resolve the pending motions: on August 6, that the framework "would not address the motions filed by putative claimant Nivie Kaul" (Doc. 85 at 2); on September 4, that the settling parties were "not seeking a stay of either of these motions" - Docs. 79 and 91 - "which would not be resolved by the pending agreement in principle" (Doc. 96 at 2); and now, on October 5, "not seeking a stay of any of these motions," the list enlarged to include Doc. 94 (Doc. 101 at 2). Each acknowledgment was made by all of the 2025 Parties jointly, including the United States and Infiniweb (Doc. 101 at 2-5). The

report does not mention Docs. 98 or 99, which remain pending before the Court, or the Court's September 30 directive that Plaintiff file a compliant motion to seal, which, as of the date of this report, remains unfiled.

28. Claimant will file her next report within thirty days, as ordered.

Dated: October 5, 2026

Respectfully submitted,

/s/ Nivedita Kaul
Nivedita Kaul, Claimant, Pro Se
5001 Ramon Road, Building 3 #1005
Palm Springs, CA 92264
Tel: +1 724 413 8167
nivie@digitaldefendersgroup.org

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on October 5, 2026, the foregoing, with its exhibits, was filed electronically with the Clerk of Court using the CM/ECF system, which will send a notice of electronic filing to all counsel and parties of record.

Dated: October 5, 2026

Respectfully submitted,

/s/ Nivedita Kaul
Nivedita Kaul, Claimant, Pro Se
5001 Ramon Road, Building 3 #1005
Palm Springs, CA 92264
Tel: +1 724 413 8167
nivie@digitaldefendersgroup.org

EXHIBIT INDEX

Declaration of Nivedita Kaul as to Exhibits A to D and F to H (filed as the first attachment)

Exhibit A. Copy of the transcript, with the title, date and URL, of the Financial Times video report "Premier League betting sponsors: closed doors and companies within companies" (September 8, 2023), https://www.ft.com/video/4bf67319-ce1e-4d13-a49d-120e12cc7d3d, as accessed on October 5, 2026 with the Declaration of Nivedita Kaul identifying it.

Exhibit B. Screenshot of the LinkedIn post by Erin West published on or about September 21, 2026, https://lnkd.in/p/gEEtgxfH, and of comments on it, captured at the date and time stated in the Declaration of Nivedita Kaul.

Exhibit C. Email from Roger Welte to the Director of External Affairs, United States Attorney's Office for the District of Columbia, dated September 13, 2026, on which Claimant was blind-copied, printed October 2, 2026.

Exhibit D. Dylan Tokar, "They Lost Their Money to Scammers—and Now Battle the U.S. Government to Recover It," The Wall Street Journal (September 9, 2026), https://www.wsj.com/finance/currencies/crypto-investment-scam-victims-big-tuna-a489ece6, saved as a PDF (pages 1-7 of a 9-page capture; advertising, links to other articles and the author's note omitted).

Exhibit E. Declaration of Roger Welte (28 U.S.C. § 1746), executed October 5, 2026.