UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers, Defendants.

Case No. 23-CV-2447 (RER) (LKE)

NON-PARTY INTERVENOR JAY LEWIS FARROW'S EX PARTE EMERGENCY MOTION TO INTERVENE PURSUANT TO FED. R. CIV. P. 24 AND/OR FOR RELIEF PURSUANT TO FED. R. CIV. P. 71
(Verified Intervenor Complaint Attached as Exhibit 1)

COMES NOW, Non-Party Jay Lewis Farrow ("Farrow"), (pro se), and hereby files this Ex Parte Emergency Motion for Intervention pursuant to Federal Rule of Civil Procedure 24 and/or for Relief pursuant to Rule 71, and in support thereof, states as follows:

Certification of Emergency: Emergency Relief Requested

Movant certifies that this Motion is brought on an emergency basis and here further states as evidence of the same as follows: Plaintiff Jay Farrow has been the target of a

sophisticated, years-long Advanced Persistent Threat (APT) campaign that infiltrated his law practice and related legal systems from 2019 through 2025. Every element of the attack on Farrow – the hijacked domains, forged emails, data theft, and orchestrated legal sabotage – corresponds to the pattern of the Conti/TrickBot APT for which a U.S. court has already granted broad injunctive relief (Coy Decl., ¶ 42; Lyons Decl., ¶ 7). **Each day that passes,** the ongoing harm to Farrow is irreparable and escalating, and the **only effective way to neutralize it is to enforce the existing injunction** and related remedies against these Defendants before they can cause further damage (Sept. 8 Final Judg., pp. 5–8; Farrow Dec., ¶ 191).

Most recently, the attackers escalated their campaign by "sinkholing" Farrow's new business websites via registrar-level interference. In early November 2025 – after Farrow slowly built a network of websites which sought to generally support businesses, law firms and attorneys with respect to teaching cyber-security habits and routines and supporting others in the business community to publish industry works. Farrow created these websites so he could work and generate income as the threat actors sabotaged his law firm so drastically that the firm went from a healthy ongoing business to being effectively closed in 5 weeks between June 2024 and July 2024. Farrow discovered on November 13, 2025, that numerous websites he owned (which had been live or in development as part of his planned December 2025 relaunch) were suddenly offline and unreachable. This concerted sinkholing event on or about November 2–3, 2025 mirrors the Defendants' prior tactics against Farrow and identified by Microsoft's Experts in this case. In other words, the same cloud-based name servers previously identified as part of the Conti botnet were used to take down Farrow's new websites.

This registrar-level "kill switch" effectively severed Farrow's ability to operate or even access his own web properties, echoing the campaign's broader goal of isolating him digitally. (*See* CNF Sinkhole Rpt., pp. 2–3).Forensic analysis indicates that the perpetrators of this campaign are a well-organized group who are in fact the same group as some or all of the named Defendants in this case. The overlap is striking: the malicious infrastructure that Microsoft and Google sought to dismantle in prior actions is materially and in some cases, precisely, the same as the infrastructure still attacking Farrow today (CNF Supp. Rpt., p. 15).

Indeed, numerous command-and-control nodes located in Queens County, New York – roughly 15 to 20 distinct IP addresses – have been identified as continuing to communicate with Farrow's compromised systems in 2024–2025. These Queens-based servers were part of the Defendants' APT toolkit and directly facilitated the hijacking of Plaintiff's court emails, e-filing accounts, and law firm domains. This threat group's structure and methods reflect a highly coordinated, persistent enterprise, not isolated hackers. Microsoft's Jason Lyons describes these Defendants as an interlinked set of ransomware and botnet operators who share malicious infrastructure and tools in a continuous, cooperative manner. In his sworn declaration, Lyons explains that the various sub-groups (e.g., Conti, LockBit, DEV-0193, DEV-0206, etc.) "3everage[e] each others' work" and often cooperate significantly – reusing cracked Cobalt Strike malware beacons and overlapping command-and-control servers – to further their joint cybercriminal objectives (Lyons Decl., ¶ 37).

This collaborative model has allowed the attackers to persist over multiple years, adapt to countermeasures, and strike at critical moments in Farrow's legal battles, all while obscuring their identities. (Finones Decl., ¶¶ 11–13). A hallmark of this APT campaign is the hijacking of core

internet infrastructure to intercept and manipulate communications. By manipulating DNS "on demand," the adversaries essentially held the *"keys to the internet's address book"* for Farrow's professional network. (Coy Decl., ¶ 22).

In Microsoft's 2023 action against these actors, investigators observed entire clusters of victim domains being repointed to Amazon's Route 53 cloud DNS servers in the 205.251.192.0/19 IP range –Farrow's Experts, including the CNF Team, observed that very pattern in Farrow's case: during key periods of the attack, dozens of Farrow's domains (including law firm email domains, court portal addresses, and even opposing counsel's domains) were abruptly redirected to Route 53 name servers in the 205.251.192.0/19 range – a one to one match of the infrastructure specifically identified in this Court's injunction Orders. The domain hijacking techniques used here are identical to those employed by the enjoined APT operators, further tying the Defendants to the prior known campaign (Coy Decl., ¶ 22; Finones Decl., ¶ 13).The near-term consequences of the domain takedowns of Farrow's websites and domains on November 2 and 3, 2025 have been dire.

As of November 17, 2025 (day 13 of the "clientHold" incident), search engines had ceased crawling Farrow's sites, previously indexed pages were being delisted, and external websites were removing links to Farrow's content. By November 20 or 21, 2025 (around the 17-day mark from the sinkholing), Farrow's web domains will be treated as abandoned by most Internet platforms – triggering mass purging of backlinks and a collapse of the online credibility he spent the past year rebuilding. Each hour that passes makes the harm more irreparable. In sum, Farrow's seeking to intervene in this case is more than about the domains which were recently sinkholed, it is about effectuating the September 8, 2025 Final Judgment's word, breath and reach to victims like him

who, after nearly 18 months of painstaking research, have identified precise matches of the banned infrastructure which continues to sabotage and cause immeasurable damages to their lives. Like Microsoft, Farrow or Farrow's Experts left a stone unturned as cyber-crime exists in the realm of requiring proof beyond and to the exclusion of any possible doubt. And, however that may sound or be challenging to digest, any doubt as to the veracity of that statement, or 'how they did it', and 'how the continue to do it' is dispelled through eg CNF's Expert Reports which span nearly five hundred pages of data analysis which determinations were only overlayed with Microsoft's DCU experts in this case after they made attribution determinations.

Again, what was discovered were one to one matches, Full Stop. Put plainly, if Farrow's domains are not promptly reinstated, his entire nascent business will vanish from the internet. Moreover, without a foothold for meaningfully timed judicial relief when Defendants decide to attack again, Farrow and others like him stand to lose everything. Here, the evidence of that reality is specifically reported by CNF, we are now at the last feasible moment to prevent permanent digital ruin Farrow's websites, and hence, the business foundation he built over the last year.

More specifically, if these domains and websites are not returned to being online within the next 24–72 hours, they will be worthless, and the threat actors would have succeeded in accomplishing the same in direct violation of this Court's September 8, 2025 Final Judgment. (CNF Sinkhole Rpt., pp. 4–6).

Statement of Facts

A. Background on APT Attack on Farrow Law

Farrow adopts the facts stated in his Emergency Certification as if recited herein and incorporates by reference his November 17, 2025 Declaration in Support of this Motion, and the

Expert Reports of Marlin Technologies, and Cyber-N.E.T. Forensics, as well as the November 17, 2025 Declaration of CNF as if fully set forth herein.

Non-Party Jay Lewis Farrow and his law firm were and are the targets of a prolonged, sophisticated cyberattack a/k/a an Advanced Persistent Cyber Attack ("APT") beginning as early as late 2020 and escalating dramatically in 2024 (Marlin Rpt., p. 3). By June 2024, Farrow observed clear signs of network intrusion—unauthorized email forwarding rules, unusual outbound network connections, and other anomalies indicating that confidential data was being exfiltrated (Marlin Rpt., p. 3). The attacks rapidly intensified: by July 2024 the threat actors had achieved full administrative access over Farrow Law's computer network, email domain DNS settings, and cloud storage, effectively crippling the firm's operations (Marlin Rpt., p. 3). Farrow's law practice was essentially shut down by this advanced persistent threat (APT) assault, as routine communication channels (email, phones, file systems) became unusable under the attackers' persistent control (CNF Rpt., p. 84).

Despite Farrow's remedial efforts—including replacing hardware and attempting secure communications—the cyberattacks continued unabated into 2025, forcing Farrow to devote full-time attention to incident response rather than his legal practice (Coy Decl., ¶ 8; Marlin Rpt., p. 4). In sum, Farrow has been the victim of a sustained, professionally orchestrated cyber-sabotage campaign intended to undermine his livelihood and his participation in legal proceedings (Marlin Rpt., p. 4).

B. Overlap with Microsoft-Targeted Infrastructure

Forensic investigations have revealed that the infrastructure used in the attack on Farrow overlaps significantly with the infrastructure previously targeted by federal court orders against

known cybercrime groups. Notably, Microsoft's 2023 investigation into a cracked *Cobalt Strike* malware network (associated with the Conti and LockBit ransomware gangs) identified two IP address ranges – 172.93.0.0/16 and 146.20.0.0/16 – as core command-and-control hubs for the adversaries (Coy Decl., ¶ 15).

Farrow's network logs have recorded multiple malicious IP addresses squarely within those exact ranges (CNF Rpt., p. 233). For example, IP addresses 172.93.148.174 (hosted by Nexeon Technologies) and 146.20.161.105 (Rackspace Cloud) were observed communicating with Farrow's systems – the same ASN networks that Microsoft's experts pinpointed as supporting the Conti/TrickBot malware infrastructure (CNF Rpt., pp. 269–270; Coy Decl., ¶ 8).

The overlaps span multiple technical vectors. Microsoft's 2023 operation documented that Defendants' C2 (command-and-control) servers were hosted on platforms like Alibaba Cloud, Linode, DigitalOcean, and OVH (Coy Decl., ¶ 12).

Critically, the infrastructure associated with the Glupteba botnet (the subject of *Google LLC v. Starovikov*, S.D.N.Y. 2021) also intersects with Farrow's case. During the period of attack, an IP address 185.198.57.110 (registered to HostSailor) was detected making illicit access attempts to Florida's statewide e-filing portal for attorneys (CNF Rpt., p. 270). Google's 2021 evidence identified that exact IP as a command-and-control proxy within the Glupteba malware network (Finones Decl., ¶ 3).

Moreover, multiple Google-owned IP addresses – specifically, Gmail SMTP servers 209.85.128.170 and 209.85.219.180 – appeared in the headers of compromised emails from Farrow's accounts (CNF Rpt., p. 270). These are the same Gmail server IPs that the Glupteba operators hijacked to covertly send control signals and exfiltrate data under the guise of legitimate traffic (Finones Decl., ¶ 4). In both Google's case and Farrow's case, the threat actors abused

Google's mail infrastructure to blend malicious communications into normal network noise – a known APT tradecraft for evading detection (CNF Rpt., p. 270).

Industry enforcement actions in 2020–2023 achieved roughly an 80–90% takedown of that malicious infrastructure, but the perpetrators preserved or rebuilt the remaining 10–20% to continue their operations (CNF Rpt., p. 257). Farrow's case exhibits so many identical Indicators of Compromise (IoCs) precisely because the adversaries are leveraging the "leftover" servers and tools from the prior botnets – along with some fresh additions – to strike again (CNF Rpt., p. 257).

C. Sinkholing of Domains – Nov. 2–3, 2025 (Emergency Grounds)

On November 2–3, 2025, the threat actors escalated their campaign by effectively sinkholing several of Farrow's new business domain names. Without warning or consent, Farrow's domains in ncluding were suddenly subjected to registrar-level holds ("clientHold" status), which disabled their DNS resolution and shut down related email and website services (Farrow Aff., ¶¶ 14–19; CNF Dec., Nov. 17, 2025, ¶¶ 15–22). This coordinated takedown closely mirrors tactics that Defendants had used in the past against other victims' infrastructure. Specifically, the adversaries leveraged unauthorized access—or influence—at the domain registrar level to hijack DNS settings, redirect traffic, and ultimately null-route the domains.

In Farrow's case, the sinkholing was accompanied by telltale signs of the same enjoined infrastructure being involved: the domains' DNS records were found pointing to malicious name servers in Amazon's Route 53 cloud service (within the 205.251.192.0/19 IP range), exactly the kind of configuration that the Final Judgment identified and prohibited (CNF Dec., Nov. 17, 2025, ¶ 17; Sept. 8 Final Judg., pp. 6–7). In other words, Defendants have repurposed the very DNS

infrastructure that this Court already froze via injunction and turned it against Farrow's new ventures (CNF Dec., Nov. 17, 2025, ¶¶ 33–34).

This recent attack not only cut off Farrow's ongoing business communications but also set in motion an irreversible degradation of the business operation he was building. Industry experts note that if a domain remains in a sinkholed state (unresolved in DNS) for more than about two weeks, it risks being dropped from email trust lists and search engine indices permanently, even if later restored (CNF Dec., Nov. 17, 2025, ¶¶ 20–24). At the time of this filing, that critical threshold is imminent. Thus, the November 2–3 incident presents an extraordinary circumstance: Farrow faces imminent irreparable harm to his professional reputation, client outreach, and digital operations if this Court does not act immediately to lift the unauthorized holds and enforce its judgment against those responsible.

The use of previously enjoined infrastructure in this sinkholing attack underscores the brazenness of Defendants' contempt and the direct violation of the Final Judgment's mandate. Farrow brings this emergency motion as soon as practicable after discovering the overlap and impact of the attack, and the facts around the November 2–3 sinkholing form a central basis for the urgent relief requested herein.

Disclosure of Prior Related Proceedings (Local Civil Rule 1.6).

Pursuant to Local Civil Rule 1.6, Movant respectfully discloses that he previously filed a separate action in this District on **October 27, 2025**, *Farrow v. John Does 1–20*, Case No. 25-cv-6033 (AMD) (PK). That matter resulted in a November 4, 2025 Memorandum and Order, which Movant later received in two separate mailings containing differing page sequences and without the exhibits and supporting materials he had filed. The November 4 Order reflects that the Court had access only to Movant's complaint, motion, and declarations, and did **not** have access to the

exhibits, forensic materials, or the September 8, 2025 Permanent Injunction entered in *Microsoft Corp. v. Does 1–16*.

Although Movant expressly requested that judicial notice be taken of that September 8 Final Judgment, the November 4 Order indicates the Court did not have the injunction before it and thus understood the *Microsoft* matter as involving **o**nly a trademark/copyright dispute, rather than the broad anti-botnet, anti-malware, and command-and-control infrastructure takedown that the September 8 Judgment actually ordered. Movant further notes that he received the November 4 Order **after** the deadline for responding to the venue show-cause requirement had already passed, leaving him no meaningful opportunity to reply.

In addition, the November 4 Order was entered **before** Movant discovered, on November 2–3, 2025, that his business domains had been sinkholed using the same command-and-control infrastructure that this Court had permanently enjoined in *Microsoft v. Does 1–16*. Once that evidence emerged, immediate action was necessary, as the domains faced irreversible de-indexing within days. In light of these circumstances—specifically that the November 4 Order was issued without the September 8 Permanent Injunction, without Movant's exhibits, and **before** the sinkhole evidence definitively tied the ongoing attacks to infrastructure already banned by this Court—Movant prepared this Emergency Motion, traveled to New York to ensure secure physical filing, and now seeks only the limited relief available under **Rule 24** and **Rule 71** to enforce this Court's own Final Judgment. This disclosure is made respectfully and solely to provide the Court with a complete and accurate procedural history.

Argument

I. Intervention as of Right Under Rule 24(a)(2)

The Second Circuit has long held that where a nonparty is directly harmed by conduct regulated by an injunction, the nonparty may intervene to protect its interests and may enforce the injunction as though it were a party. *ASCAP v. Showtime/The Movie Channel*, 912 F.2d 563, 565–66 (2d Cir. 1990); *United States v. Pitney Bowes, Inc.*, 25 F.3d 66, 70 (2d Cir. 1994).

Movant satisfies all four requirements for intervention as of right under Rule 24(a)(2): **(1)** timeliness; **(2)** an interest relating to the subject of the action; **(3)** a potential impairment of that interest absent intervention; and **(4)** inadequate representation by existing parties. In evaluating these factors, the Second Circuit instructs courts to consider the totality of the circumstances, noting that failure to meet any one factor is fatal to the application. Here, all factors strongly support granting Farrow intervention in the Microsoft action.

Timeliness: Farrow's application is timely in light of the ongoing nature of the harm and the posture of this case. Although the Microsoft case has already reached a Final Judgment, the "timeliness" requirement is flexible and context-dependent, not measured strictly by the calendar. Courts consider **(1)** how long the applicant knew of their interest; **(2)** the prejudice to existing parties from any delay; **(3)** the prejudice to the applicant if intervention is denied; and **(4)** any other unusual circumstances. All of these factors favor Farrow.

First, Farrow prepared this motion to enforce the injunction at the earliest opportunity and traveled to New York to ensure it was delivered securely to this Court. Notably, it was only after receiving a comprehensive CNF forensic report on October 22, 2025 (detailing the IP overlaps) that Farrow could be certain his attackers were the same enjoined actors; prior to that report, he

had no practical way of knowing that intervention would be necessary. Thus, Farrow has acted diligently once his stake and the Defendants' breach of the injunction became evident.

Second, there is no prejudice to the existing parties by intervening now. The original plaintiff (Microsoft) has already achieved its judgment and is not actively litigating the case further, so intervention will not disrupt any ongoing proceedings. In fact, Microsoft is likely to benefit from Farrow's involvement, as he brings additional evidence of Defendants' non-compliance and can help effectuate the judgment's purpose. The Doe Defendants, for their part, cannot claim any unfair prejudice – they had notice of the injunction and chose not to appear, and Farrow's intervention imposes no surprise on them. If anything, allowing Farrow to enforce the order promotes the injunction's intent without reopening any adjudication on the merits.

Third, the prejudice to Movant if intervention is denied would be severe. Farrow would be left exposed to ongoing cyber-attacks with no direct means to invoke this Court's protection. The Final Judgment was a critical tool intended to stop these very hackers; excluding Farrow from using it leaves him effectively unprotected and the injunction under-enforced in the face of new violations. Meanwhile, the hackers would face no immediate consequences for flouting the Court's order, emboldening them to continue harming Farrow (and others). Farrow's entire law practice—and the rights of his clients—are at stake. He has already suffered case dismissals, service disruptions, and immense costs due to these intrusions. Each day without enforcement worsens his prejudice. This factor strongly favors intervention.

Finally, unusual circumstances weigh in favor of intervention. This is not a typical post-judgment scenario: here we have an ongoing emergency, where a non-party victim is pleading for the Court's assistance to enforce an injunction *because the enjoined Defendants have resumed their illicit conduct*. The ordinary concern for finality is outweighed by the extraordinary situation

at hand—a continuing cybercrime spree that directly attacks the integrity of court proceedings. Indeed, the Court anticipated that ongoing jurisdiction might be needed to "adapt to attempts by Defendants to circumvent" the relief, and Plaintiff Microsoft explicitly asked the Court to "retain jurisdiction to modify or clarify" its orders to respond to new misconduct (Sept. 8 Final Judg., p. 8). Farrow's motion falls squarely within that retained authority: Defendants' brazen circumvention of the injunction now warrants the Court's intervention. Given these circumstances, Farrow's timing is eminently reasonable and justified. In sum, the application is timely under the totality of the circumstances—a standard to be liberally construed in favor of intervention when it serves the interests of justice.

Protectable Interest: Farrow unquestionably has a "direct, substantial, and legally protectable" interest in the subject matter of the Microsoft litigation. The purpose of that action was to thwart a specific malicious cyber infrastructure – an infrastructure that (as shown above) is also the cause of Farrow's injuries. Farrow's interest is direct: the injunction was intended to protect anyone victimized by Defendants' hacking enterprise, and Farrow is exactly such a victim. He is not an unrelated third party; he is in the bull's-eye of the enjoined scheme, suffering the very harm the injunction seeks to prevent (ongoing illicit network intrusions, data theft, and interference with legal processes). This interest is far from "academic" or contingent; it is concrete and immediate.

Moreover, Farrow's interest is legally protectable because the Final Judgment and applicable law give him the right to be free from Defendants' unlawful cyber-attacks. Courts have recognized interests sufficient for intervention where, as here, the movant "stands to gain or lose by the direct legal operation of the judgment" – or its lack of enforcement – in the case at hand. If the injunction is enforced, Farrow gains security; if it is not, he loses that protection. This aligns

with the very rationale for the injunction: to confer a benefit (freedom from attack) on those affected by Defendants' conduct. In sum, Farrow's stake in ensuring the injunction is carried out is precisely the kind of interest Rule 24(a)(2) is designed to protect.

By contrast, denying intervention would treat Farrow as a mere bystander to a case that profoundly affects him. The Federal Rules do not require such a result. To the contrary, Rule 24 broadly protects "anyone" with a meaningful interest in the litigation's outcome. Here, the outcome (the Final Judgment) was explicitly intended to shut down infrastructure that is *currently* tormenting Farrow. He thus has a legally cognizable interest in seeing that outcome realized in practice.

Impairment of Interest: Absent intervention, Movant's ability to protect his interest "may as a practical matter be impaired or impeded" by the disposition of the action (or lack thereof). This factor is plainly met because if Farrow is not permitted to invoke or enforce the Final Judgment, then that Judgment – a critical tool for his protection – lies dormant while the attacks continue. In effect, without Farrow's involvement, the Doe Defendants can violate the injunction with little fear of repercussions, since the original plaintiff (Microsoft) is not presently monitoring or addressing these post-judgment violations. Thus, Farrow's interest in stopping the ongoing hacks would be significantly impaired if he cannot act in this case.

Courts routinely find impairment where a proposed intervenor's rights might be adversely affected if intervention is denied. Here, Farrow has already experienced adverse effects: the Defendants' continued hacking has derailed his litigation efforts and forced him to expend tremendous resources to trace the source. The Final Judgment is meant to avert exactly such harm. If Farrow cannot directly ask this Court to enforce its injunction, he is left to essentially fend for

himself against a crew of international cybercriminals – an untenable position given that the very power of a federal injunction is needed to neutralize them.

No alternative forum or remedy exists that would comparably protect Farrow's interest. His own separate lawsuits have been stymied by the hackers' interference, and law enforcement investigations (while ongoing) have not yet halted the attacks. The EDNY injunction is uniquely suited to deliver immediate relief by binding the actors and infrastructure in question. Furthermore, the relief Farrow seeks (enforcement of the existing injunction) can realistically be obtained *only* in this Court, which issued the Final Judgment. If he is not allowed to intervene here, he effectively cannot obtain the benefit of that Judgment at all – a classic example of impairment. Rule 24(a)(2) does not require absolute certainty of impairment, only that the disposition of the action *may* impede the movant's ability to protect his interest. Here, the risk is not theoretical; it is happening in real time – every day without enforcement brings more harm to Farrow. This factor strongly supports intervention.

Inadequate Representation: Farrow's interests are not adequately represented by the existing parties in the Microsoft case. At this stage, the only plaintiffs of record are Microsoft and its co-plaintiffs, and the Defendants have defaulted. Microsoft's interest, while aligned generally in stopping the hackers, is *not identical* to Farrow's specific interest and is no longer being actively pursued in court. The Second Circuit imposes only a "minimal" burden on a proposed intervenor to show inadequacy of representation – it is enough to demonstrate that the representation of the movant's interest **"may be"** inadequate. Farrow clears that low bar easily.

Microsoft's case was primarily focused on protecting its own customers and infrastructure; it obtained relief and has not indicated any intent to seek contempt or further action against the Does for new violations affecting others. In fact, Microsoft may believe it has done its part by

securing the injunction and could be content that the matter is closed. It is not actively monitoring whether *other* victims like Farrow are being targeted anew. By contrast, Farrow has a personal, **pressing stake** in enforcement that Microsoft does not share to the same extent. This divergence in perspective means Microsoft cannot be relied upon to champion Farrow's interests at this juncture. As courts recognize, even a well-intentioned party cannot adequately represent an intervenor when the intervenor's interests are narrower or more focused or require emphasis on issues that the existing party is not motivated to raise. Here, only Farrow will underscore the ongoing harms and the need for immediate contempt proceedings – matters that, from Microsoft's vantage point, might not be a priority.

Moreover, there is effectively **no one** in the litigation currently protecting the interests of victims like Farrow. The Defendants surely do not represent Farrow's interests; they are his adversaries. And with the plaintiffs having obtained their judgment, there is a vacuum as to who will ensure compliance with that judgment going forward. This void is precisely what Rule 24 is meant to fill: permitting an affected non-party to step in when the existing parties cannot or will not pursue the necessary relief. Farrow's situation is analogous to that of class members or third-party beneficiaries in other cases who intervene post-judgment to enforce a decree – courts have found representation inadequate in such instances because the original parties have "moved on," leaving the beneficiaries' interests unguarded (or even in conflict).

In summary, Microsoft's understandable focus on its own remedies, and its lack of ongoing action, leaves Farrow's distinct interests insufficiently protected. Farrow has easily made the required "minimal showing" of possible inadequacy. Therefore, this fourth factor is satisfied. Having met all elements – timely application, a compelling interest, a threat of impairment, and inadequate representation – Movant Farrow is entitled to intervene as of right under Rule 24(a)(2).

The Court should grant intervention to allow Farrow to enforce the Final Judgment and shield himself under its provisions.

II. Permissive Intervention Under Rule 24(b) (Alternative)

Even if the Court had any doubt about intervention as of right, it should in the alternative grant **permissive intervention** under Rule 24(b). Rule 24(b)(1)(B) allows intervention, at the Court's discretion, when a movant "has a claim or defense that shares with the main action a common question of law or fact." Farrow easily meets this standard, and permissive intervention here would cause no delay or prejudice to any party. Farrow's claims share common questions of law and fact with the Microsoft action, including the identity, operation, and continuing use of the same malicious C2 infrastructure. Courts routinely grant permissive intervention where the movant's claims and the injunction's scope overlap, especially where enforcement is sought. *ASCAP*, 341 F.2d at 1007.

Common Questions of Law and Fact: Farrow's requested intervention and relief undoubtedly share common questions with the original action – indeed, they are virtually identical. The Microsoft case determined as a matter of law that the Doe Defendants' cyber activities were illegal and should be enjoined. Farrow now raises the question of whether those **same Doe Defendants** (or those in privity with them) are violating that same injunction through the same factual conduct.

This involves overlapping facts (e.g., the identity of the command-and-control servers, domains, and malware signatures — all of which were part of the evidentiary foundation of the original case) and overlapping law (the scope and effect of the Court's injunction, and the legal consequences for those bound by it). In essence, Farrow seeks to apply the law and facts already established in *Microsoft v. Does* to a new instance of non-compliance. At a minimum, there are

common factual issues about the linkage between Farrow's hackers and the enjoined enterprise, and common legal issues about enforcement and scope of the injunction (including principles of privity and Rule 65's binding effect on those "in active concert or participation" with the enjoined parties).

Allowing Farrow to intervene will thus "fast-track" the resolution of these issues within the existing case, rather than require a separate full-blown lawsuit to prove what has essentially already been decided. This promotes judicial efficiency. The Second Circuit has noted that permissive intervention is appropriate where it will avoid duplicative litigation and the intervenor's claims overlap significantly with the main action's claims. Here, a separate enforcement action by Farrow would cover much of the same ground – proving the link between Defendants and the prior judgment, and seeking injunctive relief that this Court has already crafted. It is far more efficient to handle enforcement of the existing injunction in the original case, with this Court's familiarity and authority, than to start anew in a different forum.

No Undue Prejudice or Delay: Rule 24(b) also directs courts to consider whether intervention will "unduly delay or prejudice the adjudication of the original parties' rights." In this case, there are no ongoing proceedings to delay – the original case has concluded on the merits. Permissive intervention for the purpose of enforcement will not reopen any issues between Microsoft and the Defendants; it will simply ensure that **the Court's judgment is given effect**. Farrow is not trying to relitigate liability or inject unrelated claims – he accepts the Final Judgment as-is and seeks only to enforce it. Thus, there is no risk of transforming or complicating the case; this is a post-judgment enforcement matter that courts routinely entertain under their ancillary jurisdiction.

Likewise, there is no prejudice to Microsoft (the original plaintiff) – if anything, Microsoft's victory is bolstered by ensuring the injunction it obtained is honored. Nor is there prejudice to the Defendants beyond having to finally face the consequences of an order that has long bound them. The Doe Defendants had full notice of the injunction and of the possibility that those acting in concert with them or benefiting from the judgment could be held to account. Indeed, Rule 65(d) already binds them and anyone aiding them to the terms of the injunction. Permitting Farrow to step in simply provides the Court a vehicle to address what the Defendants should already be doing (complying with the Order). Since the Defendants never appeared, there is no litigation position of theirs to protect – and since they are actively violating the injunction, they can hardly argue they relied on any expectation of finality.

Finally, **equity favors intervention**. Farrow's presence will help the Court supervise and enforce its Judgment, which was clearly intended to have broad protective reach. The Second Circuit has observed that where non-parties are intended beneficiaries of an injunctive order, it may be appropriate to allow them to participate in enforcement rather than require each to file separate suits. In *Berger v. Heckler*, for example, the court permitted intervention by non-parties to enforce a consent decree, noting that "judicial economy virtually requires that appropriate persons be permitted to intervene" to effectuate the judgment. The same reasoning applies here. Farrow's intervention will streamline enforcement and prevent irreparable harm that would occur if the injunction's breach goes unchecked. This is precisely the type of scenario where a court should exercise its broad discretion to allow permissive intervention in service of justice.

In sum, Farrow meets the threshold for permissive intervention (common issues abound), and granting it will cause no undue delay or prejudice. On the contrary, it will serve the public interest and uphold the integrity of the Court's orders. Therefore, if for any reason the Court finds

intervention as of right inapplicable or unavailing, Movant respectfully requests that the Court nevertheless grant leave to intervene under Rule 24(b) to pursue the enforcement relief described herein. The Court has **broad discretion** in this area, and that discretion should be used to allow Farrow a day in court to secure the benefits of an injunction that was, in part, designed for his protection.

III. Enforcement of the Final Judgment Under Rule 71

Separately, Federal Rule of Civil Procedure 71 provides an independent mechanism for relief. Rule 71 states: "When an order grants relief for a nonparty or may be enforced against a nonparty, the procedure for enforcing the order is the same as for a party." In other words, if a court's judgment is intended to benefit a person who was not a formal party, that person has the right to enforce the judgment as though they were a party to the case. Likewise, if an injunction can bind a nonparty (as Rule 65(d) often contemplates), that nonparty can be held to account under the order. Here, both prongs of Rule 71 are satisfied: the Final Judgment confers relief for the benefit of nonparties (i.e. all those victimized by Defendants' cybercriminal infrastructure), and it may be enforced against certain nonparties (those in active concert or participation with the enjoined actors, as well as any successor infrastructure).

Rule 71 exists to prevent the injustice of a court's order benefiting someone but then denying that person the ability to enforce it. Courts have applied Rule 71 in similar contexts – for example, to allow members of the public or a class (who weren't named plaintiffs) to invoke a consent decree that was meant to benefit them. The Second Circuit's decision in Berger v. Heckler, 771 F.2d 1556 (2d Cir. 1985), is directly on point. There, a consent judgment against a federal agency provided for the restoration of certain Social Security benefits to nonparty claimants. When

the agency failed to fully comply, those nonparties sought to enforce the decree. The government argued that nonparties had no standing to enforce a decree to which they were not formal parties.

The Second Circuit disagreed, holding that Rule 71 entitled the nonparty beneficiaries to enforce the decree, and that they could do so by intervening in the action. The Court noted that although normally a consent decree is not enforceable by those not party to it (citing Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 750 (1975)), that general rule "was not intended to preclude nonparties from intervening to enforce [a] consent decree where otherwise authorized by the federal rules." The Second Circuit emphasized that since the decree explicitly extended benefits to a broader class of persons, it would undermine the decree's purpose to bar those persons from enforcement. Indeed, "judicial economy and fairness" required allowing them to enforce the order rather than insisting on separate actions.

The parallels here are strong. The Final Judgment in the Microsoft case provides broad injunctive relief aimed at protecting anyone who might be victimized by Defendants' malicious infrastructure. By its terms, the Judgment permanently shut down domains and IP addresses used for the hacking, forbade Defendants from engaging in those attacks, and thus extended protection to every would-be target of the enjoined operation. Farrow falls squarely within that protected group – he is exactly the kind of victim the injunction anticipated. In fact, as discussed above, the Judgment explicitly authorizes nonparties like Farrow to leverage the injunction in cooperation with law enforcement efforts.

Under Rule 71, Farrow can "enforce obedience" to that injunction by the same process as if he had been a named plaintiff all along. That means he can come before this Court and seek orders of enforcement, contempt, or other appropriate relief to ensure the Defendants cease violating the injunction.

To be clear, Rule 71 does not magically transform Farrow into a party for all purposes; rather, it grants him the procedural right to enforce the Court's order. Here, Farrow has chosen to exercise that right through this motion (and via intervention, out of an abundance of caution). The Court can treat this filing, in the alternative, as a nonparty motion to enforce the Final Judgment pursuant to Rule 71. The relief sought – an order finding that Defendants' continued hacking violates the injunction and enforcing the injunction against them with coercive measures – is relief that the Court has full authority to grant to a nonparty beneficiary under Rule 71.

One might question whether Farrow has Article III standing to enforce the injunction. The answer is yes. Article III standing requires (1) an injury in fact, (2) causation, and (3) redressability. Farrow's injuries (cyber intrusions, case sabotage, etc.) are concrete and directly caused by Defendants' conduct that the injunction prohibits. These injuries are ongoing and actual, not speculative – satisfying the injury and causation elements. As for redressability: a court order directing Defendants (and those in concert with them) to comply – for example, through contempt sanctions, further disabling of servers, or other measures – would likely mitigate or halt the attacks on Farrow, thereby redressing his injuries. In Berger, the Second Circuit held that the original plaintiff's claim to enforce a consent decree was not moot and was ripe, even though he was still receiving benefits at that moment, because the agency's non-compliance with the decree threatened his future benefits.

Likewise, here, Farrow need not wait until he is completely ruined by the hackers to seek relief; the ongoing threat is sufficiently real and immediate to warrant judicial intervention. There is no contention that Farrow falls outside the "zone of interests" of the injunction – quite the opposite, he is front and center among those the injunction was designed to protect. Accordingly,

Farrow meets any standing test that could apply to a Rule 71 motion (to the extent such a test is distinct from the Rule's express requirements).

Moreover, under basic principles of equity and contract law, Farrow can be seen as a third-party beneficiary of the Final Judgment (which, after all, was in part a court-approved stipulation with the effect of a consent decree). The decree was essentially a "contract" between Microsoft and the Doe Defendants, enforceable by the Court, and it conferred a benefit on victims like Farrow (namely, the benefit of injunctive protection). In general, a third-party beneficiary to a promise has the right to enforce that promise. The Second Circuit noted this analogy in Berger, citing contract law principles that a third-party beneficiary can sue to enforce a contract. By the same token, Farrow, as an intended third-party beneficiary of the injunction, can ask this Court to enforce the Defendants' promise (imposed by the Court's Order) not to engage in the enjoined conduct.

Therefore, independent of Rule 24, Rule 71 provides that the Court should hear Farrow's plea and grant appropriate enforcement relief. The Court need not engage in any metaphysical inquiry about whether Farrow was "intended" as a beneficiary; the record of the Microsoft case makes it abundantly clear that the injunction's aim was to protect the public (including attorneys like Farrow) from the Defendants' cyber-attacks. To effectuate that aim, the Court can simply apply its Order to the situation at hand and hold Defendants accountable to it upon Farrow's motion.

In practical terms, Movant requests that the Court enforce the Final Judgment by: (1) declaring that the individuals who have been targeting Farrow's systems are bound by and in violation of the Final Judgment's permanent injunction (as they are either the same Doe Defendants named therein or acting in concert with them); (2) issuing appropriate orders to compel immediate compliance with the injunction – for example, an order directing any domain registries, hosting providers, or internet services referenced in the Judgment (or newly identified in Farrow's

evidence) to take down or transfer the malicious infrastructure being used against Farrow, consistent with the injunctive relief previously granted; and (3) requiring the Doe Defendants to show cause why they should not be held in contempt for violating the Court's decree. Through such measures, the Court will give full effect to its prior Judgment and halt the ongoing irreparable harm.

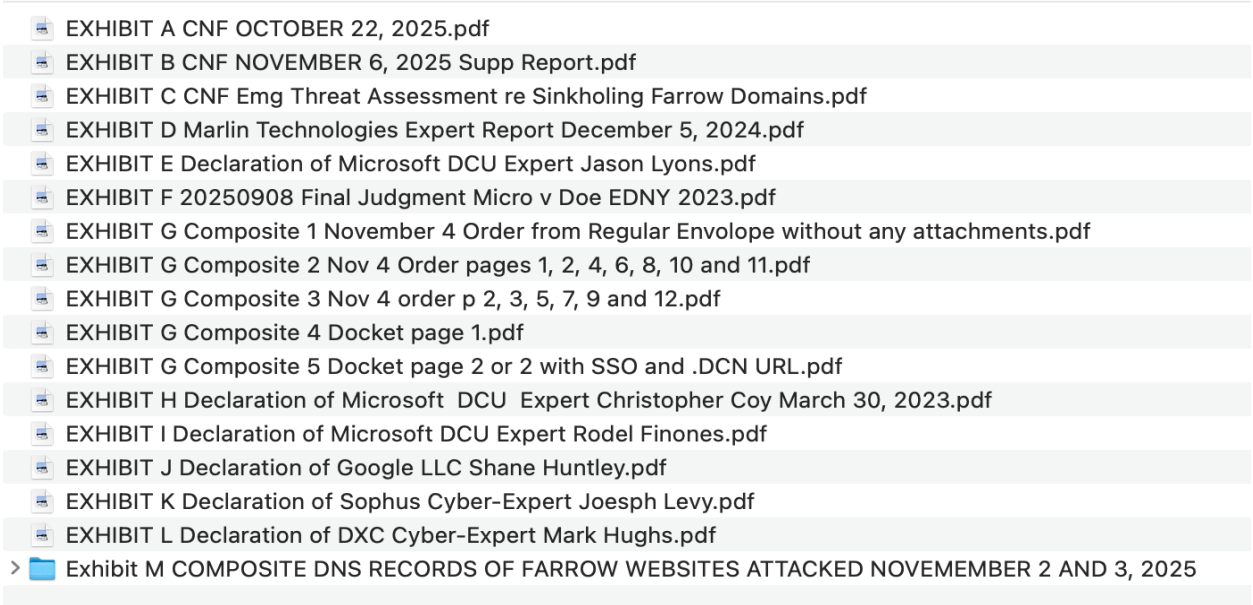
The Court unquestionably has the power to do so. District courts retain inherent jurisdiction to enforce their orders and may use contempt sanctions to coerce compliance or punish disobedience. Here, a finding of contempt would be warranted given the prima facie evidence that Defendants have violated a clear and unambiguous term of the injunction (namely, the prohibition on continuing their illicit cyber activities) and that they had actual notice of the injunction (by virtue of the default proceedings and the public nature of the relief, which was well-publicized in cybersecurity channels). Even if the particular individuals hacking Farrow were not themselves named in the case, if they are acting as part of the same collective or in concert with those who were named, they are bound under Rule 65(d)(2) and subject to contempt all the same.

The Court might direct, for example, that any new IP addresses or domains Defendants have switched to (which were not already covered by the original injunction and seizure order) be immediately seized or disabled under the All Writs Act authority invoked in the original case, given that such action is necessary to prevent evasion of the Judgment. The local U.S. Attorney or appropriate law enforcement officials could be enlisted to execute such technical enforcement measures, as was done when the original injunction was implemented. The specific mechanics can be addressed in the Proposed Order Movant will submit, but the key point for this Motion is that the Court should now exercise its enforcement powers on Farrow's behalf.

In sum, Rule 71 provides a straightforward path: treat Farrow as if he were a party beneficiary of the Judgment (because, in effect, he is) and grant him the relief the Judgment entitles him to – namely, an end to Defendants' illegal cyberattacks. This Court's injunction "established the illegality of Defendants' infrastructure and obtained a permanent injunction dismantling it." Recognizing and enforcing that Judgment's binding effect here will "fast-track the neutralization" of Defendants' operation against Farrow, since "the heavy lifting of technical findings and injunctive crafting has been done." Movant respectfully urges the Court to follow the letter and spirit of Rule 71 and exercise its authority to enforce the Final Judgment now, in order to prevent further harm and to uphold the Court's mandate.

Incorporation and Designation of Exhibits

Farrow incorporates by reference his November 17, 2025 Declaration, and the November 17,2025 Declaration of Cyber-N.E.T. Forensics dated November 17, 2025. In sequential Order, the following are the Exhibits which have been cited herein and within the CNF Declaration in sequential order, all of which are incorporated herein in their entirety.



Conclusion and Emergency Relief Requested

For the foregoing reasons, Movant Jay Lewis Farrow respectfully requests that the Court **GRANT** this Emergency Motion and enter an Order providing the following relief:

1. **Grant of Intervention and/or Rule 71 Enforcement Authority:** That Movant be permitted to intervene in this action pursuant to Fed. R. Civ. P. 24(a)(2) or, in the alternative, that the Court recognize Movant's status as a nonparty beneficiary entitled to enforce the Final Judgment entered on September 8, 2025, under Fed. R. Civ. P. 71.
2. **Emergency Restoration of Sinkholed Digital Property:** That the Court direct that Farrow's lawfully owned domain names—including but not limited to *legalweeklynews.com*, *privatestocknews.com*, *usnewshour.com*, and *jtrnews.com*—be immediately restored to functioning DNS and removed from any registrar-imposed "clientHold" (or equivalent) restrictions, which have caused irreparable business harm and which threaten permanent de-indexing from the global internet infrastructure if not reversed within hours **(CNF Dec., Nov. 17, 2025, ¶¶ 12–24; Farrow Aff., ¶¶ 10–21; Sept. 8 Final Judg., pp. 6–7)**.
3. **Finding of Active Concert Violation and Contempt Proceedings:** That the Court find that the individuals operating the command-and-control infrastructure used to sinkhole Farrow's domains and compromise his network are either the same Doe Defendants or their affiliates/successors bound by the Court's Final Judgment, and that such persons are in active violation of that injunction **(CNF Dec., Nov. 17, 2025, ¶¶ 16–20, 25–28; Coy Decl., ¶ 22; Sept. 8 Final Judg., pp. 5–8)**.
4. **Order to Show Cause and Interim Protective Measures:** That the Court issue an immediate **Order to Show Cause** directing any persons in active concert or participation with the enjoined Doe Defendants to cease all use of infrastructure previously enjoined by the Final Judgment—including, but not limited to, any Amazon Route 53 name servers in the **205.251.192.0/19** range and any registrar-level DNS manipulation—and to show cause why contempt sanctions and additional enforcement measures should not issue **(CNF Dec., Nov. 17, 2025, ¶¶ 14–17; Farrow Aff., ¶¶ 25–29; Sept. 8 Final Judg., pp. 6–7)**.

5. **Relief Tailored to Imminent Digital-Reputation Collapse:** That the Court recognize the urgency of the situation and issue appropriate interim relief—whether injunctive, restorative, or supervisory—in no more than 24 to 48 hours, given that Farrow's domain infrastructure will cross the 14-day DNS failure threshold by November 20, 2025, triggering potentially irreversible loss of domain trust, email deliverability, and search engine indexing **(CNF Dec., Nov. 17, 2025, ¶¶ 20–24)**.
6. **Mandatory Meet-and-Confer with Microsoft DCU and Counsel:** That the Court direct Microsoft's Digital Crimes Unit and its counsel to meet in person with Movant within 48 hours of the Order (as contemplated in Microsoft's enforcement framework) to coordinate containment efforts, restoration of services, and evidentiary sharing **(Farrow Aff., ¶ 31; CNF Dec., Nov. 17, 2025, ¶ 26)**.
7. **Retention of Jurisdiction and Follow-On Enforcement:** That this Court retain jurisdiction to modify, clarify, or extend its prior injunctive orders as needed, consistent with its continuing supervisory authority under the Final Judgment and the All Writs Act, and to ensure that the September 8, 2025 Final Judgment is not evaded by successor infrastructure or actors **(Sept. 8 Final Judg., pp. 7–8)**.

Respectfully submitted,

November 17, 2025

Jay Lewis Farrow
[redacted]
Tel: [redacted]
Email: [redacted]