UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

JAY LEWIS FARROW, an individual, Plaintiffs, vs. JOHN DOES 1 through 15; unknown person(s)/corporation(s), Defendants.	

AMENDED VERIFIED COMPLAINT[1]

COMES NOW, Plaintiffs, JAY L. FARROW ("Farrow") ("Plaintiff"), by and through undersigned counsel, and hereby sue Defendants, and allege as follows:

VERIFIED COMPLAINT

COMES NOW Plaintiff JAY LEWIS FARROW ("Plaintiff" or "Farrow"), by and through undersigned counsel, and hereby sues Defendants JOHN DOES 1 through 15, and alleges as follows:

Introductory and Preliminary Allegations

1. Emergency – this Case involves the years-long and ongoing Advanced Persistent Threat Cyber-Attack ("APT") perpetrated upon Florida's Legal Industry. The Threat Actors have spent years using previously outlawed malicious command and control ("C2 Architecture" or "C2 Infrastructure") and repurposing, building upon and expanding the same as a templated APT which is easily tailored to target a single attorney or a larger legal institution to serve the interests of the group or groups as an enterprise for a sprawling array of criminal activity.

2. To date, the threat actors, named as John Doe Defendants here, some of whom were also named John Does in previously prosecuted cases by e.g. Microsoft Corporation and Google, LLC, have used advanced tactics and strategics which have achieved the infiltration into Florida's Legal Industry Ecosystem, with redundant lateral footholds, backdoors and failsafe mechanisms that they have been able to maintain persistence within micro and macro network environments while remaining undetected notwithstanding any instance which an IT team had believed they achieved 'containment' of a cyber-security breach.

3. In sum, the threat actors achieved their goals and milestones, in large part, through using previously known and outlawed C2 Infrastructure, repurposing, building upon and/or expanding upon the same, while employing specific Techniques, Tactics and Protocols ("TTPs") which have been researched and catalogued by federal agencies and APT researchers.

4. To date, the John Doe Defendants herein, and likely others, have successfully infiltrated Florida's judicial infrastructure, such as the network servers, email hosting servers, website domains, server domains, Florida's eFiling Authority and its central eFiling portal, the Florida Bar's network, scores of known law firms computer networks, individual computers belonging to attorneys, paralegals, legal staff and collateral supply chain digital environments within the Legal Industries' cyber-ecosystem.

5. For over a year, Plaintiff Farrow and his family have fought to find a means to stop, contain, and bring before a court of law the threat actors or their clients to end the nightmare they have experienced at the hands of cowardly keyboard-wielding cybercriminals.

6. In short, Plaintiff is one of the many victims of this templated APT, by certainly not the only victim.

7. Notwithstanding diligent efforts to get assistance from authorities through 'regular' channels and other means available to Plaintiff, and that an ongoing investigation is proceeding, Plaintiff notes that law enforcement's larger focus and a cyber-victims individual threshold for enduring more pain and trauma, creates a unique paradox. One, where the threat actors are very sophisticated and carrying out a well-planned and highly organized operation, a single victim's chances of obtaining the amount of forensic evidence necessary to procure injunctive relief is near zero. Two, law enforcement investigation into sophisticated cybercrimes seek to dismantle the operation while making meaningful arrests which will likely lead to convictions. Hence, the path to judicial relief for an individual who is a victim of an APT must employ a path to relief that is meaningfully-timed using the resources available without giving up, or in, thinking the Calvary will arrive 'soon.'

8. This lawsuit represents the discovery of one of those paths, and thus far, the only one which has proven to contain an attack that has otherwise devastated and forever changed Plaintiff's life and the lives of his family.

9. While Plaintiff would ordinarily detail the catastrophic emotional trauma caused by this ordeal, he limits this introduction to noting that the most recent threat to his child's life on July 11, 2025 – came almost a year to the day when he received the first threat to his child, then only 22 months by the threat actors. Why they targeted Plaintiff, and who ultimately benefited or caused him to be a target may be answered, but only after the threats and the daily consequences of threat actor activity against Farrow and his family are contained.

10. The APT at issue is highly adaptable and modifiable, employing nearly undetectable methods and tactics. By way of example, it targets the legal industry by stealing attorney e-filing

credentials, silently exfiltrating confidential information, redirecting email communications, sabotaging computer networks, and infiltrating electronic court filing systems.

11. Defendants leverage this templated APT to achieve various criminal objectives – such as ransom, information theft, network sabotage, and severing of communications – thereby depriving Plaintiff and others of access to courts and due process of law.

12. The legal pathway to stopping such cybercriminal activity has substantial precedent. It was not initially apparent to Plaintiff or his expert team until over a year's worth of evidence was compiled, pinpointing the locations where Defendants deploy their malicious scheme – i.e., the command-and-control computers and servers ("C2 Architecture" or "C2 Structure") distributed across the United States and internationally.

13. This legal path was charted by large technology companies like Microsoft Corporation and Google LLC, who employed a patchwork of federal statutes, and the All Writs Act to cut threat actors' malicious cyber-infrastructure off at its roots.

14. Critical to this approach is identifying the specific addresses or "neighborhoods" on the Internet used by the cybercriminals to send malware and orchestrate their attacks.

15. Once that attribution was obtained, Microsoft (for example) sought court orders to enjoin the use of those domains or IP address ranges by transferring administrative control over them. With such control, a plaintiff can effectively "pull the plug" on a malicious domain by redirecting it to safe servers or causing it to go dark, without harming the legitimate domain registrars or hosting providers.

16. After power is cut to the malicious infrastructure, notice is given to the domain owners, affording them an opportunity to appear and show cause why their domains or IPs are not, in fact, being used nefariously.

17. Here, Plaintiff has independently verified specific IP addresses and malicious domains used in the attack. Astonishingly, there is substantial overlap between the infrastructure attributable to Defendants here and the infrastructure already subject to active federal injunction orders or judicial orders obtained by large tech companies.

18. Many of those prior orders became moot when the tech company plaintiffs (e.g., Microsoft) were asked by the U.S. Department of Justice to stand down and dismiss without prejudice in deference to parallel criminal investigations. Nonetheless, the prior civil actions revealed the points of vulnerability.

19. Not only are there precise matches between Plaintiff's attribution evidence and the C2 infrastructure that was targeted in those prior cases (including infrastructure affecting Plaintiff as an end-user of Microsoft Windows), but Defendants here have employed techniques, tactics, and protocols ("TTPs") that are substantially identical to those used by the threat actors in at least five large-tech-company v. Doe cases.

20. The reuse of some of the exact same IP addresses and the replication of virtually identical TTPs gave Plaintiff a roadmap, as it has in over 15 known federal cases since 2017, to a civil remedy proven to work: cutting off the head of the proverbial snake by dismantling the malicious infrastructure.

21. An APT is by all accounts among the most intricate, sophisticated, tightly organized, well-financed, and harmful types of cyber-attack.

22. The APT at issue here is modifiable by design to target, and indeed has targeted, over 40 law firms and dozens of attorneys connected to Plaintiff's digital ecosystem, using cyber-architecture that has been enjoined by federal courts throughout the United States. In other words,

Defendants have been leveraging malicious cyber-infrastructure that was already identified and ordered to be disconnected in prior cases filed by Microsoft, Google, and others.

23. Thus, to the extent any remaining IP addresses or domains from those prior cases (or substantially similar ones) were found in the forensic artifacts on Plaintiff's devices, in unauthorized intrusions into the Florida Bar's network and Florida's eFiling Portal, or in email and document metadata, Plaintiff asks this Court to immediately order that such infrastructure be disconnected and dismantled.

24. Microsoft, Google and others reported achieving roughly 80–90% containment of the threat through their actions. However, Plaintiff's investigation has uncovered that Defendants – the cyber-criminals – have knowledge of, have used, and have built upon that very enjoined cyber-infrastructure, using the same resources and tools to continue their attacks. Without this Court's intervention, those malicious systems remain operational in part and continue to harm Plaintiff and others.

Jurisdiction and Venue

25. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962). Additionally, the Court has supplemental jurisdiction over Plaintiff's related state-law claims, including the Florida RICO count, under 28 U.S.C. § 1367, because those claims form part of the same case or controversy as the federal claims.

26. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and a substantial part of the property that is the subject of Plaintiff's claims is situated in this

District. Defendants have caused harm in this District and have availed themselves of the privilege of conducting activities in Florida by utilizing instrumentalities (computers, servers, email accounts, etc.) located in Florida and specifically within the Southern District of Florida.

27. Defendants have affirmatively directed actions at Florida, at this District, and at other federal districts (including the Eastern District of New York and the Eastern District of Virginia) as part of their scheme.

28. Defendants infiltrated computers located in this District, gained control of victim machines here, and moved laterally through networks to find additional victims and install malware. In doing so, they caused ransomware such as Conti, LockBit, Quantum Locker, Royal, Cuba, BlackBasta, BlackCat, and PlayCrypt to be deployed on systems of individuals and entities located in the Southern District of Florida, thereby directly harming persons and property in this District.

29. Pursuant to 28 U.S.C. § 1391(c), each Defendant is deemed to reside in this District because Defendants are all persons subject to personal jurisdiction here. Defendants are subject to personal jurisdiction in Florida under Fla. Stat. § 48.193(1)(a) because, inter alia, they committed tortious acts within Florida (via the internet and otherwise), caused injury to persons and property in Florida by acts outside Florida while engaging in persistent misconduct within Florida, and because they have used computers and networks located in Florida to carry out their scheme.

Parties

30. Plaintiff Farrow is an individual and resident of Miami-Dade County, Florida. Farrow is a licensed attorney and the principal of Farrow Law, P.A., a law firm based in Miami, Florida, which was among the targets of Defendants' cyberattack.

31. Defendant **John Does 1–3** are unknown persons who are part of the cyber threat group known to Microsoft threat intelligence as **DEV-0206**, or a group factually indistinguishable from

DEV-0206. DEV-0206 is an Evil Corp-affiliated threat group that develops malicious *Cobalt Strike Beacon* and other remote access malware loaders for use in multiple cybercrime campaigns. On information and belief, John Does 1–3 provided or operate the beacon malware used in the attacks on Plaintiff in furtherance of conduct designed to cause harm to Plaintiff and the public. Plaintiff is informed and believes, and thereupon alleges, that John Does 1–3 can likely be contacted (through their infrastructure providers or other intermediaries) using the information set forth in **Appendixes A, B and C** hereto. Appendixes A, B and C is a composite list incorporating by reference the Appendixes A, B and C attached to the Complaint in *Microsoft Corp., et al. v. John Does 1–16*, No. 1:23-cv-02447 (E.D.N.Y. 2023) (hereafter "Composite Appendixes A, B and C").

32. Defendant **John Does 4–6** are unknown persons who are part of threat group **DEV-0504** (a group identified by Microsoft) or a group factually indistinguishable from DEV-0504, or individuals operating with the same TTPs as DEV-0504. DEV-0504 is a team of ransomware affiliates and/or initial access brokers that relies on purchased network access to infiltrate victims. They use Cobalt Strike and similar remote monitoring and management (RMM) agents (indeed, an illicit RMM agent was found on Plaintiff's computers). DEV-0504 frequently disables antivirus products that lack tamper protection, all in furtherance of conduct designed to cause harm to Plaintiff and the public. Plaintiff is informed and believes, and thereupon alleges, that John Does 4–6 can likely be contacted through the information set forth in Composite Appendixes A, B and C.

33. Defendants **John Does 7–15** are individuals or members of threat groups, teams, or associations of cyber-threat actors that *repurpose and tailor* the specific malicious infrastructure and tools of groups such as DEV-0206 and DEV-0504 (among others). These John Doe Defendants took a pre-existing templated APT and directed it towards Plaintiff and other attorneys practicing

in the Southern District of Florida, with the intent to manipulate judicial outcomes and/or for other malicious purposes. Their actions caused irreparable harm and incalculable damage to Plaintiff (both personally and in his capacity as an attorney) and to members of the public. Plaintiff is informed and believes, and thereupon alleges, that John Does 7–15 can likely be contacted through the information set forth in Composite Appendixes A, B and C.

34. Plaintiff is informed and believes, and alleges, that each of the John Doe Defendants owns, operates, controls, and maintains portions of the malicious command-and-control infrastructure hosted at the IP addresses and domains identified in Composite Appendixes A, B and C. The C2 infrastructure at those IPs and domains is maintained by third-party hosting companies and domain registrars, as listed in Composite Appendixes A, B and C, which may provide avenues for notice and enforcement of any court orders.

35. Plaintiff will amend this Complaint to substitute the Doe Defendants' true names and capacities when ascertained. Plaintiff will exercise due diligence to determine their true identities, roles, and contact information, and will seek leave to effect service upon those individuals once identified.

36. Plaintiff is informed and believes, and alleges, that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that the injuries to Plaintiff (as well as to other attorneys in the Southern District of Florida, the Florida Bar, the Florida Courts' eFiling Authority, and members of the public) were proximately caused by Defendants' conduct.

37. On information and belief, the acts and omissions alleged to have been undertaken by John Does 1–15 were all authorized, controlled, directed, or ratified by each of the other Defendants, or each Defendant had the ability to authorize, control, or direct such acts. Furthermore, each

Defendant knowingly assisted, cooperated with, or encouraged the others in their wrongful actions, such that each Defendant is jointly and severally liable for the acts of the others. In acting as alleged, each Defendant was the agent, affiliate, officer, member, alter ego, or co-conspirator of each of the other Defendants, and was acting within the scope of such agency or relationship and in furtherance of the conspiracy and enterprise described herein.

38. Each Defendant aided and abetted the others in the commission of the unlawful acts. Each Defendant knew of the others' wrongful acts and provided knowing substantial assistance or encouragement, or otherwise ratified and adopted the acts, to accomplish the scheme. Each Defendant reaped profits and benefits from the scheme, and each was an integral part of the overall enterprise and conspiracy.

Factual Allegations

39. One of the earliest reported instances of attempting to manipulate a judicial outcome via hacking occurred in 2013, when a California company embroiled in litigation hired an operative who in turn enlisted a cyber-hacker to break into the emails of the opposing counsel.

40. The scheme was eventually discovered, leading to criminal convictions of those involved. Over the next decade, an underground market developed for "litigation hacking," and the tactics, techniques, and protocols of this dark endeavor evolved and grew more sophisticated.

41. By 2018, reports began surfacing of extremely sophisticated cyber-attacks targeting the legal system.

42. What had once been isolated incidents of "semi-pro" hackers accessing an opposing counsel's email had transformed into the kind of cyber-espionage and sabotage previously seen only in nation-state APT campaigns.

43. In essence, the tactics of long-term, persistent cyber-attacks were being repurposed for hire in civil disputes.

44. What materialized were tailor-made APT attacks using malicious cyber-infrastructure and architecture following a *template* designed by experienced threat actors.

45. These templates exploited ubiquitous platforms (for example, Microsoft's Windows operating system) by injecting malicious code that would blend in with normal system processes and network traffic, leaving little or no trace on disk. The injected malware would beacon out once the infected system was online, contacting the threat actors' C2 servers without tipping off the user.

46. In essence, an APT cyber-attack seeks to exploit a system vulnerability to gain a foothold in the victim's Windows OS. Once injected, the malware leaves virtually zero traces on the file system but is programmed to silently transmit a "beacon" when the machine connects to the Internet.

47. That beacon signal is received by the threat actor's C2 server. When the C2 server receives the beacon, the threat actors can remotely send further malicious instructions to the victim's computer (again disguised as normal, expected traffic).

48. These instructions enable the malware to propagate through the computer or network and escalate privileges – often seeking administrator, SYSTEM, or root access – which eventually gives the threat actors near-total control over the victim's systems and all data therein.

49. From 2018 through 2020, the illicit business of "hacking for hire" – often contracted by litigants' consultants or agents – grew in sophistication.

50. These operations leveraged tradecraft honed by years of training in national security and law enforcement agencies, now being used for private ends.

51. The hired hackers ("cyber-mercenaries") focused on high-stakes disputes (commercial, environmental, etc.), aiming to steal confidential information and sabotage the opposing parties' case preparation.

52. By 2022, *Reuters* documented numerous court cases in which cyber threat actors traced to India attempted to manipulate high-stakes litigation. Those groups targeted some 1,000 attorneys at 108 law firms, sending password-stealing emails cleverly disguised as client communications in an effort to gain access to attorneys' email and document systems.

53. This trend confirmed that such attacks were not isolated incidents but part of a broader pattern of organized, contract cybercrime aimed at undermining the judicial process.

54. In this case, Plaintiff alleges that the John Doe Defendants are part of that broader pattern. By 2021, these Defendants had tailored the templated APT to target Plaintiff and other attorneys within the Southern District of Florida, intending to manipulate judicial outcomes and/or achieve other malicious objectives to their benefit.

55. This included stealing confidential or privileged information, sabotaging computers and digital ecosystems, and interfering with court communications – all to gain unfair advantage in litigation or to extort and harass the victims.

56. One key characteristic of the scheme is *complete anonymity, for the John Does and their whiting or unwitting beneficiaries*: the threat actors conceal their identities behind layers of hacked infrastructure, false personas, and proxy servers.

57. They compromise third-party email and e-filing accounts (for example, stealing a lawyer's eFiling credentials and then filing fraudulent documents in a case) to hide their involvement. They silently intercept communications (such as by placing hidden forwarding rules on email accounts) so that neither courts nor opposing parties realize filings and orders are being diverted.

58. This anonymity gives the cyber-criminals tremendous power, while their employers (those who hire them) enjoy plausible deniability.

59. Without a direct means to attribute or stop the hackers, a small law firm like Farrow's had virtually no chance to fend off such sophisticated attacks in time to prevent harm.

60. Indeed, on or about June 3, 2024, Plaintiff's suspicions were confirmed when he first detected that his law firm's computers were compromised by an APT attack.

61. However, at that time, due to Defendants stealth, persistence and patience in the planning, stagging and execution of their APT from 2020 until Plaintiff believed his computers were being hacked, Plaintiff had no appreciation for how profound and serious the consequences were at that time for himself, his law practice, not to mention that other law firms, attorneys and even his family.

62. In fact, it would not be until July 2024, after his law practice had effectively been shut, did he and his wife call local and federal authorities, but even, still that was after he had attempted to obtain judicial relief from a court of law.

63. Moreover, due to the complete severance of his communications on July 2024 and moving forward, by the John Doe Defendants using various means to interfere with email and phone calls, he was not able to contact, meet with and retain his first expert team until November 2024.

64. As further alleged herein, ultimately, Farrow would work with several teams, two of them have global contacts and resources.

65. One of those teams, Team B, supported Farrow from January through June 2025 and Team C, from about late April 2025 through July 2025.

66. Each of these teams provided expert reports, and each of these teams forensically diagnosed that Farrow was the target of an Advanced Persistent Threat ("APT").

67. CNF is an international group of cybersecurity experts, cybercrime investigators, and APT analysts that collaborates with the U.S. Department of Homeland Security's Joint Cyber Defense Collaborative (JCDC).

68. Since mid-2024, Plaintiff has dedicated thousands of hours to extracting forensic artifacts from compromised devices, analyzing network logs and email metadata, and coordinating with law enforcement.

69. Over a year's worth of digital evidence was collected and analyzed, ultimately pinpointing Defendants' command-and-control infrastructure and tying it to known threat actor groups (as detailed below).

70. By way of illustration, Plaintiff's investigation revealed patterns in Florida court cases consistent with this scheme: attorneys of record would appear on behalf of parties for only a very short duration with minimal activity, and those same attorneys were later confirmed to have had their e-filing credentials compromised during that period.

71. In these cases, the pattern was strikingly consistent: filings were made in court dockets by persons impersonating attorneys (using real attorneys' names and bar numbers without authorization); the legitimate attorneys later provided sworn declarations that they had not drafted or authorized those filings and were unaware their names were being used. Defendants have also infiltrated official e-filing portals (e.g., the Florida E-Filing Portal) to redirect or suppress court notices.

72. They use clandestine PDF manipulation tools (e.g., PDF converters infamous for obfuscating metadata) to strip filing traces, and they deploy techniques outside the normal practices of the legal profession in order to conceal their involvement.

73. Such tactics amount to a direct attack on the justice system, causing immeasurable harm to courts, litigants, attorneys, and court staff – including Plaintiff.

Overlapping Infrastructure Between Farrow's Investigation and Prior Cases

74. Plaintiff's forensic investigation uncovered extensive overlaps between the infrastructure used against him and the infrastructure identified and targeted in prior federal cybercrime cases (2018–2025). See CNF eForensic Report attached hereto as Exhibit "A"

75. Plaintiff incorporates the Declarations of Microsoft v Does 2023 Ditgital Crime Unit Christopher Coy, Rodel Finoes, Jason Lyons (Microsoft v. Does 2023 E.D.N.Y.), Google's Cyber-Expert Shane Huntley (Google LLC v. Does, S.D.N.Y. 2020), Sophus Limited Cyber-Expert Joseph Levy (Sophus v Does, 2020 E.D.Va), and DXC Technology Corp Expert Mark Hughes DXC v Does (2020)(E.D.Va.) herein as Exhibits B, C, D, E, F and G.

76. Plaintiff also incorporates the December 5, 2024 Expert Report of Marlin Technologies herein as Exhibit H.

77. Plaintiff also incorporates herein as Exhibit H the March 30, 2023 Order Granting Microsoft Corporation [and partners] Ex Parte Motion for Temporary Restraining Order and Order to Show Cause as Exhibit I.

78. In particular, multiple Internet domains and IP addresses that appear in Plaintiff's network logs, malware configuration files, and other Indicators of Compromise (IoCs) also appear in the court filings and evidence of those prior cases. This strongly suggests that the same organized threat actors behind those earlier cases are involved here, or at least that Defendants are reusing the exact same malicious infrastructure.

79. For example, key components of the Trickbot botnet's C2 infrastructure (which Microsoft targeted via civil action in 2020) directly intersect with the infrastructure used against Farrow, especially beginning in 2021.

80. In the 2020 Microsoft case, investigators uncovered a global network of malicious servers and domains used to control infected machines. Hundreds of custom-generated domain names (often gibberish strings or innocuous-sounding names across various TLDs) and numerous IP addresses were identified. Microsoft listed these in an appendix to its complaint (filed under seal) as part of the botnet's callback infrastructure.

81. Microsoft's Digital Crimes Unit (DCU) experts, such as Jason Lyons, detailed how the defendants maintained illicit control through a shifting DNS infrastructure – employing *fast-flux* techniques and chains of proxy IPs to continuously rotate command endpoints and evade blocking.

82. Forensic analysis of one of Farrow's laptops (a Lenovo device that he used from late 2020 through August 2024) and another used from February 2025 through July 24, 2025 uncovered that several of the same domains and IP addresses from Microsoft's Trickbot investigation were communicating with Farrow's network.

83. For example, an IP address within a particular AS174 transit network range – flagged by Microsoft as a Trickbot C2 node – was also observed making connections to Farrow's network in 2021. This is a virtually irrefutable indicator that Farrow's computer had been forced to contact infrastructure that a federal court (the Eastern District of Virginia) had ordered be shut down in late 2020.

84. Stated plainly: Farrow's system became one node in the lingering remains of the Trickbot botnet. This directly connects the attack on Farrow to the same organized cybercriminal enterprise

that Microsoft disrupted, strongly supporting that the perpetrators are one and the same or closely affiliated.

85. Another significant overlap is in the abuse of DNS and Internet domains. In the Microsoft 2020 Trickbot case, the scale of domain usage was staggering – Microsoft ultimately worked with registries worldwide to sinkhole or seize over 500 malicious domains used by the hackers.

86. Those domains had no legitimate purpose; they were auto-generated to function as C2 beacons and phishing portals for the malware.

87. Plaintiff's investigators found that some of those *same domain names* – or slight variants of them – were queried or accessed in Farrow's network traffic in 2021–2022.

88. In other words, the John Doe Defendants repurposed parts of their old Trickbot infrastructure against new victims like Farrow, maintaining persistence in Farrow's computers by creating redundant backdoors and continuously using those C2 servers to send remote commands, escalate privileges, move laterally across devices, and exfiltrate confidential information.

89. Both Microsoft's 2020 evidence and Farrow's case also show the use of cloud services and dynamic DNS for resilience. Microsoft noted that Trickbot at times leveraged bulletproof hosting providers and even Tor/.onion services to hide its C2 servers.

90. In Farrow's case, Defendants similarly utilized cloud-based servers (for example, an Azure-hosted IP was seen exfiltrating data) and VPNs from foreign jurisdictions to make traceback difficult. This demonstrates a common modus operandi of using cloud or anonymization infrastructure to prolong the life of the enterprise.

Google LLC v. John Does (S.D.N.Y. 2021) – Parallels in Malware Behavior, DNS Spoofing, and Persistence:

91. In late 2020, Google initiated its own civil action against a major botnet, filing *Google LLC v. Starovikov, et al.* in the Southern District of New York (unsealed in 2021).

92. This case targeted the operators of the *Glupteba* malware botnet – a sophisticated criminal network that had infected over a million devices worldwide and notoriously leveraged blockchain technology to remain resilient to takedown. Google's complaint (which named two individual defendants and numerous Does) alleged violations including RICO, CFAA, the Electronic Communications Privacy Act, the Lanham Act (for trademark violations), and other causes. By invoking RICO, Google signaled that the Glupteba botnet was an ongoing criminal enterprise engaging in a pattern of cyber fraud and abuse.

93. The Glupteba malware was used for stealing user credentials, illicit cryptocurrency mining, and setting up proxy networks on victims' devices.

94. A hallmark of Glupteba was its *persistence*: when Google took steps to disrupt it, the malware would activate backup mechanisms – notably, querying specially encoded data on the Bitcoin blockchain – to locate new command servers and *revive* the botnet after takedown attempts.

95. Google's lawsuit mirrored Microsoft's strategy, seeking a TRO to freeze dozens of malicious domains and IPs, and to cut off the threat actors' access to Google services and the broader Internet.

96. A federal judge granted Google a preliminary injunction in December 2021, allowing Google to take down current and future domains tied to Glupteba's operation.

97. 40. Google's case is particularly relevant here because it dealt with an APT-like criminal operation employing stealthy malware, DNS/IP infrastructure abuse, phishing tactics, and even trademark infringement as part of its scheme – exactly the issues at the core of Farrow's incident.

98. The Glupteba malware's behavior closely parallels what has been observed in the Farrow attack (as well as in Microsoft's cases and others like DXC Technology's case). Glupteba essentially functioned as an APT toolkit wielded by criminals: once it infected a system (often via pirated

software laced with malware), it silently harvested sensitive data (credentials, cookies, personal files) and funneled that data back to its controllers.

99. This resonates with Farrow's experience – Defendants operated quietly within Farrow's and related systems for years, clearly aiming to collect sensitive legal information and intelligence.

100. Glupteba also co-opted victims' devices into a *proxy network* for illicit use. The botnet operators literally rented out access to infected "Internet of Things" (IoT) devices through services like AWMProxy, allowing paying criminals to route their traffic through unwitting victims' IP addresses.

101. This made tracing the true origin of attacks extremely difficult. By relaying malicious traffic through residential ISP IPs, the Glupteba enterprise masked itself.

102. The Farrow threat actors have shown a similar level of sophistication: evidence indicates that Defendants used residential VPN/proxy services and perhaps even infected third-party systems to proxy their traffic, in order to conceal their operational servers.

103. For instance, a C2 server IP address known to be tied to Defendants was observed attempting logins on a Florida Bar attorney's account – effectively using one victim's network to target another, a tactic pointing to central coordination by the same group.

104. The use of a previously enjoined *Nexeon* network IP to access a Florida Bar portal account is a glaring red flag showing the threat actors leveraging their arsenal across multiple facets of the legal system. It directly links the attack on Plaintiff's law practice to the broader enterprise's scheme against legal institutions.

105. **Shared Tactics and Infrastructure – Microsoft 2023 Ransomware Case:** In March 2023, Microsoft filed another landmark case in the Eastern District of New York against an array

of ransomware actors, again naming John Does 1–16 associated with various groups (Conti, LockBit, DEV-0193, DEV-0206, DEV-0237, DEV-0243, DEV-0504, etc.).

106. This case focused on an illicit Cobalt Strike-based C2 infrastructure being used to facilitate ransomware like Conti and LockBit across many victims. Microsoft's investigators, including Christopher Coy and Jason Lyons of the DCU, treated the interlinked cybercriminal actors as one collective *enterprise* due to their common use of cracked Cobalt Strike and shared infrastructure.

107. The complaint and supporting evidence in that case revealed that the defendants (spanning multiple threat groups) were not operating in isolation but were leveraging a common pool of malicious infrastructure and tools – essentially functioning as one RICO enterprise in practice.

108. A core observation in the Microsoft 2023 matter was the sheer number of disposable domains and IPs employed in the Conti/LockBit enterprise: hundreds of throwaway domains registered across various countries, with DNS records configured for very short TTLs to enable rapid IP switching.

109. Some of the specific domain naming patterns in that case (e.g., domains mimicking legitimate services or random-string subdomains) were found to overlap with patterns seen in the Farrow attack. In both instances, the actors favored certain registrars and hosting providers notorious for abuse tolerance, and both used similar tactics to rapidly rotate or obscure their infrastructure.

110. In Microsoft's sealed Appendixes A, B and C from the 2023 ransomware case, for example, over 100 IP addresses of C2 servers were listed; several of the IPs that communicated with Plaintiff's systems appear in that list or in the exact same network blocks.

111. Far from being deterred by prior court orders, the enterprise treated those enjoined servers as a blueprint, confidently continuing to use them (or slight variants) to target new victims once the original plaintiffs stood down.

112. Plaintiff's expert's report documents a "one-to-one overlap" between the evidence from *Microsoft v. Does 2023*and artifacts from Farrow's devices, showing that Defendants' C2 architecture remained operational (at least in part) through July 2025.

113. This brazen reuse of known malicious infrastructure highlights the enterprise's disregard for the law and underscores the need for coordinated judicial intervention to finally dismantle their network.

114. Notably, even after Plaintiff replaced his compromised devices, Defendants quickly infiltrated his new hardware. A Lenovo ThinkPad X1 Carbon Gen 3 laptop that Plaintiff deployed in early 2025 was compromised within weeks of setup.

115. Farrow's Team B and CNF's forensic testing confirmed that the threat actors maintained an active presence on the new laptop through at least June 2025.

116. In late June 2025, upon sensing imminent exposure, Defendants audaciously utilized their domain registrar privileges to alter a key command-and-control server's configuration—removing identifying registration data and adding subdomains—to evade tracing while preserving their foothold.

117. Marlin Technologies, Team B and CNF's investigation ultimately recorded nearly 400 distinct digital footprints of Defendants' activity between 2019 and July 31, 2025, each corresponding to malicious servers or domains that were also identified in prior cybercrime cases. CNF further determined that over 3,600 law firm files on Plaintiff's devices had been damaged,

exfiltrated, or sabotaged by Defendants through unauthorized modifications between 2021 and July 2025.

118. In short, Defendants' unlawful access to Plaintiff's and related systems did not cease—it is ongoing and persistent, demonstrably continuing even after prior infrastructure was exposed or enjoined.

119. In 2020, Sophos's Chief Technology Officer, Joseph Levy, declared under oath that advanced cybercriminal groups "will take steps to conceal their activities and move to new infrastructure" as soon as they become aware of any countermeasures (Levy Decl. (Sophos 2020)).

120. Similarly, in July 2020, Mark Hughes, President of Security for DXC Technology, observed that when such threat actors suspect an imminent takedown, they may "abandon or decrease use of [their] infrastructure and move to new infrastructure to continue" their attacks (Hughes Decl., ¶ 24).

121. These expert observations underscore that Defendants' racketeering conduct is part of a long-term ongoing pattern—one that necessitates decisive injunctive relief to disrupt.

The Cyber-Criminal Group or Groups Exploit Stolen Credentials, Infiltrations into Judicial Architecture and Institutions as Part of their Schemes to Serve their Ongoing Enterprise and Objectives

122. Evidence exists that the John Doe Defendants, acting in concert, harvested stolen attorney credentials to access electronic fling portals and infiltrated federal and state judicial infrastructure, such as servers, domains, websites, which Plaintiff used as an individual and as a practicing attorney. A copy of the Expert Spreadsheets related to infiltrations into the Florida Bar's Employee Portal and Membership Portal, and Florida's Electronic Filing Authority central portal, myflcourtaccess.com, are appended hereto and incorporated herewith as Exhibits J, K and L.

123. The Florida E-Filing Portal (myflcourtaccess.com) – through which attorneys file lawsuits, motions, and evidence electronically – was deeply infiltrated. Forensic data (including logs compiled by an independent "Team B" of experts) showed over a thousand unauthorized intrusions into the e-filing portal and related clerk-of-court systems (See CNF Expert Report, p. 5). With this access, the attackers could manipulate court filings in transit. In practice, they had the ability to *silently "kill" or delay critical filings*.

124. Documents submitted by the Plaintiff's firm victim's firm were at times held in a hidden "administrative hold" status and never reached the judges' dockets or were delayed so long that opposing parties gained advantage (See CNF Expert Report, p. 5).

125. By exploiting this backdoor, the threat actors effectively denied the victim access to justice – a motion might be filed on time on paper, but in reality it never arrived for the court's review, or an emergency petition would simply not show up in the judge's queue. One result was that emergency motions (even those filed under seal and meant to be decided ex parte) could be prevented from ever reaching a judge, thereby shielding the attackers from any immediate legal countermeasures.

126. This level of control over the court's own filing system allowed the adversaries to rig the legal process in subtle but powerful ways. As the CNF report describes, the attackers at one point were essentially able to *"block or manipulate [their opponent's] legal filings such that they could procure specific court outcomes"* in at least one Florida state case (See CNF Expert Report, p. 5). In effect, by ensuring the victim's important filings never made it onto the docket or were fatally delayed, the attackers guaranteed that court orders and judgments were issued in their favor by default.

127. State Judges, of course, had no idea that the record before them was incomplete or sabotaged – they were unwittingly signing off on outcomes orchestrated by the hackers' interference. This is a startling escalation from typical cybercrime into direct subversion of the judicial process. As well, in several cases, as is alleged hereinbelow, neither did the 'opposing law firm' or the 'attorney' purported in the position of opposing counsel.

Compromise of Federal Case Management Systems (CM/ECF)

128. Evidence suggests that the campaign did not stop at state-level systems.

129. The attackers also took advantage of vulnerabilities in the federal judiciary's electronic case management systems, which are known to be outdated in many districts.

130. The CNF investigation noted "redundant infiltrations and footholds within legacy Florida federal and state judicial systems" that allowed the threat actors to create or engineer judicial orders under false pretenses for their own benefit (See CNF Expert Report, p. 6).

131. In other words, by exploiting older, unsecure servers and databases in the court system, the hackers could potentially insert fraudulent court orders or case entries – effectively puppeteering the outcome of court cases by making it appear that a judge had duly signed an order, when in fact the process had been tampered with.

132. For example, the attackers, masquerading as attorneys using stolen e-filing credentials, were able to file motions and even secure dismissals or default judgments in certain federal cases *without the real parties' knowledge*. These actions would result in authentic-looking decrees (bearing a judge's signature or court seal) that furthered the attackers' interests, whether financial or strategic, while the victim's case was quietly derailed (See CNF Expert Report, p. 6).

133. Such compromises are not merely hypothetical as demonstrated by the discovery by Plaintiff of approximate 31 attorneys practicing within the Southern District of Florida, and using its CM/ECF Portal, in well over fifty cases filed between 2018 and 2025.

134. Aside from Plaintiff's evidence, in early 2021, the Administrative Office of the U.S. Courts acknowledged an "apparent compromise" of the confidentiality of the federal CM/ECF system, leading to emergency security measures for highly sensitive filings (they began requiring certain "HSD" documents to be filed only in paper or on secure, stand-alone systems)

135. By 2022, it emerged in a Congressional hearing that three hostile foreign actors had indeed breached the federal courts' document filing system in a hack of "startling breadth and scope." (House Judiciary Committee testimony, 2022; see Reuters, Aug. 7, 2025).

136. This startling disclosure implied that sealed indictments, warrants, and other confidential filings had been accessed by unauthorized parties. The federal case management system – containing some of the nation's most sensitive legal documents – has long been considered a prime target for nation-state espionage, and these fears were realized.

137. Most recently, in July 2025, a major new breach of the CM/ECF system was discovered, affecting multiple U.S. federal courts. According to reports by Politico and The New York Times, this attack potentially exposed sealed court records (including secret indictments and witness information) across at least a dozen federal districts, raising severe national security concerns. Investigators cited evidence that Russian state-sponsored hackers were at least partly responsible for the intrusion (See New York Times, Aug. 12, 2025).

138. Federal Officials and cybersecurity experts noted that the attack vector in 2025 leveraged basic software vulnerabilities that had been identified in the legacy CM/ECF software back in 2020

but never fully patched (i.e., the judiciary's slow adoption of security fixes left known holes exploitable) (See Wired, Aug. 14, 2025).

139. The decentralized nature of the federal courts' IT (with each district running its own instance of CM/ECF on sometimes aging infrastructure) meant inconsistent security – a fact explicitly acknowledged by U.S. Circuit Judge Amy St. Eve, who told Congress in 2023 that many court systems were running on "legacy" outdated technology with inadequate security protocols (See Reuters, Aug. 7, 2025).

140. This legacy tech environment likely made the 2025 breach easier: the attackers essentially re-opened an old backdoor that should have been closed, indicating a systemic failure to update and secure the judiciary's systems.

141. Federal authorities have been relatively tight-lipped about the full scope and damage of the 2020–2025 intrusions, given their sensitivity. However, the pattern is clear and grim: foreign cyber adversaries penetrated the electronic backbone of the U.S. court system, accessing confidential information and possibly tainting the integrity of case dockets.

142. These revelations reinforce that the same threat group (or allied groups) involved in sabotaging Farrow's cases were operating at a national scale as well. In fact, technical overlaps identified by the experts connect the Florida attacks with known global cybercrime operations.

143. The CNF report, for instance, found that some of the *command-and-control (C2) server infrastructure* used in the Florida Bar and e-filing breaches matched infrastructure previously tied to the notorious TrickBot malware botnet and its operators (the IP ranges and hosting providers corresponded to those used by the TrickBot gang) (See CNF Expert Report, p. 7).

144. This suggests that the same sophisticated criminal syndicate behind TrickBot – a group with suspected Russian connections that was disrupted by Microsoft and US Cyber Command in

2020 – has retooled and turned its sights on the legal sector. Not only are they stealing data, but they are also weaponizing it to undermine court proceedings, which is a modus operandi closer to state-sponsored espionage than to traditional cybercrime for profit.

145. The infiltration of email networks, state bar systems, and federal court databases by this threat actor (or actors) represents an unprecedented convergence of cybercrime and the subversion of justice.

146. Through a combination of DNS/email hijacking, credential theft, and exploitation of outdated "legacy" servers, the attackers have managed to read privileged communications, sabotage litigation processes, and plunder sealed court files – all while operating in the shadows.

147. As further described in the "Mirror Law Firm" Section, the cyber-criminal group or groups used each of these exploits in tandem to effectuate the purposes and objectives of their templated APT as against Plaintiff, his practice, over forty identified law firms, scores of identified attorneys, and, indeed, to achieve their objective of impugning the integrity and legitimacy of the decisions from the Honorable Jurists of this Court, those around the state of Florida and the United States.

148. The fallout from these attacks is profound: Here, Farrow, and other litigants, such as several of his clients, have been cheated of fair hearings, sensitive law enforcement information has been exfiltrated, and public trust in the security of our legal institutions is a stake should the cyber-criminals remain in possess of access to assets such as stolen attorney credentials and C2 Architecture which was disgorged from them in federal orders between 2020 and 2023.

149. Further evidencing and/or corroborating Plaintiff's allegations, the CNF Expert Report, the Marlin Expert Report, the three expert spreadsheets, the testimony of Microsoft's Digital Crime Unit and Google LLC's cyber-response teams, is that, at this very moment, and over the last three years, and most recently since July 4 and August 7, 2025, federal judicial authorities, have admitted

that CM/ECF portals were compromised using stolen credentials and federal judicial institutions were compromised through infiltration into legacy computer servers.

150. In fact, as further support, Court administrators have begun implementing emergency measures, such as routing highly sensitive filings through offline channels and accelerating efforts to modernize the case management infrastructure (reforms envisioned in proposals like the pending Open Courts Act aim to replace the old systems with a secure, unified platform).

151. Federal agencies including the FBI and Department of Homeland Security are investigating the breaches, and there are calls for greater transparency and coordination (for instance, engaging the Joint Cyber Defense Collaborative to help protect court networks).

152. On the defensive side, Plaintiff's experts, and many other associates and strategic partners of the JDCD experts urge immediate steps like patching DNS vulnerabilities (e.g. eliminating "lame" orphan name servers that attackers abused), mandating multi-factor authentication and encryption for court systems, and instituting centralized logging/monitoring across all court IT systems to detect intrusions sooner (See Wired, Aug. 14, 2025).

153. The courts themselves have acknowledged the need for improvement – judiciary officials concede that years of underinvestment left their systems "at regular risk of … compromising security breaches," and that many vulnerabilities must be urgently addressed (See Reuters, Aug. 7, 2025).

154. Finally, the expert reports in Farrow's case have recommended aggressive remediation actions to contain the threat actors. These include legal measures such as court orders to seize or sinkhole domains used by the hackers, emergency injunctions to lock down DNS records and preserve evidence, and coordinated efforts with ICANN and law enforcement to dismantle the attackers' infrastructure (See CNF Expert Report, p. 8).

155. While such steps are unusual, they underscore the severity of the situation – a *"state-of-the-art templated APT"* is effectively using the legal system's own technology against itself (See CNF Expert Report, p. 6).

156. In other words, the severity of the situation as it relates to Plaintiff, other attorneys, law firms, courts of law and this Honorable Court is this – all of the cyber-assets, by and through which this criminal organization functions to achieve its objectives for personal profit, non-monetary gain and/or strategic advantages – remains in the hands of these criminals who, at this hour, continue to perpetrate their attack against Farrow and others.

157. In fact, Plaintiff and his expert team conducted live tests of one of his computers on July 22, 2025, and, with in short order, the computer was call out to, and responses received from, the malicious architecture. As well, other than that 'test, Farrow's only digital presence outside his home related to this case was at the end of July 2025.

158. After uploading documents to the University of Miami Main Library's printer vendor, including a draft of the expert reports and other documents related to the testimony of Microsoft's DCU Team, the library printers posted an error message never seen before by the library IT, stating servers not available, minutes later his documents were exfiltrated and $400 was lost in copy fees paid to vendor.

159. At that moment, Plaintiff checked the vendor's website domain's ICANN.ORG DNS Records, and within 14 minutes of Plaintiff uploading his documents, the vendor's DNS records were changed, and the domain pointed to different servers which Plaintiff recognized as being used by five major law firms which he had investigated as part of his work with CNF's team.

160. In fact, within a three minute period, the DNS Records for nearly 30 servers which hosted two of the largest law firms in the United States (both of which were purportedly representing

defendants in the lawsuit Plaintiff filed on February 5, 2025 on behalf of his wife, infant child, his practice and himself, recorded updates to their or their named server DNS records revealing that five large law firms, all represented defendants in that legal matter, recorded updates to their DNS records of their Server records – which reveal that all five of those law firms where on Amazon's Route 53 Servers, and in at least two cases, two very large law firms were using the exact named server, awsdns-41.org. (See CNF Report, Section X). As such, the cyber-criminal group continues to demonstrate they remain in possession of the cyber-assets which allow them to perpetrated their template APT, as well as, their ability to control the communication traffic between lawyers at that firm and, at the very least Farrow, is present, ongoing and was demonstrated during a hand-on-key-board event as of the end of July 2025.

The Mirror Scheme – Creating Virtual Doubles of Law Firms and Attorneys which Exploit Stolen Credentials, Compromised Domains and Servers which Manipulate Judicial Systems, Processes, Procedures which Counterfeit Justice

161. Plaintiff's investigation has revealed that Defendants orchestrated a scheme to create a "mirror" version of Several Law firms which starts with DNS Hijacking, or lame designation cyber attack where the threat actors do not 'hack' into the law firm's network, they use either stolen credentials or exploit incomplete, outdated, and/or misconfigurations of DNS records to obtain admin privileges or direct access to the law firm's registrar portal.

162. Once inside, the threat actors are at the helm of, and can manage, every feature of a domain, including the suite of configurations of the domain's zones, where the domain is hosted, which email servers the domain points to, it can change, add or eliminate email addresses, add secondary email servers, and clone every functional and aesthetic feature of the domain and host the same on their C2 Servers.

163. In so doing, the threat actors, along with harvesting the credentials of accessing electronic filing portals and, *inter alia,* other federal, state and local portals, such as "CourtMaps" and the federal PACER database, the threat actors can operate, in all respects, a virtual law firm under the guise of the legitimate law firm, where opposing counsels would receive emails from both the normal and customary attorneys and their staff, opposing counsel could send email in return, and all the while neither the opposing counsel nor the legitimate law firm has any clue that the cyber-criminals are directing and controlling all communication traffic.

164. Exploiting the trust of an opposing law firm, the threat actors can and have, as was the case with Farrow, send their targets word documents, pdf and links otherwise related to the litigation. Once the target opens the file or link, the threat actors deliver their templated malware payload which begins the cycle of mapping opposing counsel's network, creating footholds, moving laterally, establishing redundant backdoors and reentry vectors should one or more fail such that they can maintain persistence within the target environment.

165. In this way, the threat actors can monitor the opposing counsel's activities, client communications, email accounts, harvest credentials, and manipulate client files, exfiltrate (steal) confidential information and slowly advance their network privileges to that of admin or SYSTEM.

166. At this point, the threat actors create alternative email folders, create email forwarding rules, add hidden email accounts, and gain access to the lead attorneys' email account and their paralegals/legal assistants such that they can send an email which emanates from the target attorney to themselves or to supply chain vendors, or, by example, to court judicial assistants approve the language of a proposed order or agreeing to the date of a hearing.

167. At this juncture, the threat actors can manipulate court documents from within their target's network and within the federal or state court portal once the attorney or their staff files a court

document. By this point, which may take days, weeks or months, the threat actors are receiving all outgoing communications and incoming communications, not just to opposing counsel, but also to the target's clients, as well as, have complete control over all filings, the scheduling of hearings, and over what the target and staff see as being filed online and what the court actually reviews.

168. In any number of ways, depending upon the services for which they were contracted or, based upon the advancement of the cyber-criminal group's own strategic advantages, they can manipulate the outcome of the judicial proceeding or even prevent claims from being filed.

169. Whatever the instance, obfuscation of their activities is paramount, and in most cases, their ability to bend the course of the litigation, by example, mid-court decisions on the scope of discovery, dismissal of a cause or action or allowing a bogus claim to proceed to trial, engineers the calculus of the target lawyer which informs their professional advice to their client as to the probative outcomes, settlement options and, in many cases studied by CNF and other experts, the entering of a federal lawsuit by a threat actor masquerading as lead counsel has consistent IoCs which materially affect, at the very least, a consistent end to the litigation without discovery motion practice, motions for summary judgment, or any pre-trial disputes such as motions in limine of trials for that matter.

170. In most cases, the malicious virtual law firm and the attorney or attorneys who appear through stolen credentials, file one of five types of documents, lack firm footers or branding, use clerk notice of appearance forms, lack bar numbers, have incorrect firm information, the documents have consistent errors and/or consistencies which would not exist between the same law firm let alone related to different law firms, some of which that were studied had over 100 and up to 2500 lawyers.

171. Moreover, the forensic evidence related to the federal lawsuits farrow was prosecuting in 2024 through 2025, had anomalies where the attorney author of a document would be the author for a firm which they did not work and upon a court document's meta for a client they did not represent, while the word processor to pdf converter was one of three non-enterprise products known to be used by threat actors whereas the law firms in question have eg adobe.

172. In total, Plaintiffs expert reports demonstrate the methods which a cyber-criminal group adapted and templated an Advanced Persistent Cyber Attack which could server many hack-as-a servers purposes, or be modified slightly to provide RaaS.

173. Plaintiff alleges that the same accounts for his inability to reach any of the opposing counsels in his current lawsuit wherein he represents his wife, infant child and law practice as against those who are alleged to have hired the cyber-criminal group and law firms which, failed to undertake the basic research regarding their DNS records, which, if checked through an internet search which could take one minute, would alert the firm to a possible IoC, that being an unusual 'updated' recorded to its official "ICANN.ORG" or Whois DNS Records.

174. By infiltrating a law firm's network and/or hijacking its DNS and email settings, Defendants effectively created a virtual cyber-double of law firms, and their online presence (See Marlin Tech Rpt, p. 5).

175. This allowed them to intercept or outright prevent genuine filings and e-mails, to insert themselves into electronic service (e-service) lists while removing legitimate recipients, and even to file pleadings or communications while impersonating Plaintiff and his colleagues (See CNF Report, p. 4)

176. Through these DNS and MX record manipulations (a form of domain hijacking), Defendants gained the ability to read all email intended for Farrow and respective other law firms, block or delay messages at will, and send emails that appeared to originate from Plaintiff's account.

177. Operating in the shadows via hidden email forwarding rules and spoofed domains, Defendants used over forty law firm and scores of attorneys as their unwitting "proxy" to carry out their objectives.

178. In essence, Defendants ran parallel law firms in cyberspace – one that bore the names of some of the most prominent firms in Florida, the United States and who have offices around the Globe – all of which are assets of the threat actor defendants as of the filing of this lawsuit.

179. The John Doe Defendants, individually, had separate roles and functions, by example, one of the elite John Doe cyber-criminals monitors and directs email traffic, while another locates dormant or orphaned domains from which the group can stage an operating to mirror and create a virtual law firm under using the name of a legitimate law firm, using the stolen credentials of legitimate attorneys, and use the same to their own advantage.

180. In so doing, neither the legitimate law firm nor courts have any notice of these malicious and criminal activities, however, courts have no reason to question the legitimacy of that firm or its attorney's actions, nor the activities or lack thereof, of the targeted firm and/or attorney. At day's end, as was the case in several of Farrow's federal and state lawsuits, the same were dismissed or worse, trials engineered by the very same threat actor group for the very same 'main' defendants who Farrow and his Family are attempting to assert claims against, occur in absentia without notice to Farrow.

181. Plaintiff's firm name and attorney identities – to clandestinely control and sabotage legal proceedings for their benefit (See CNF Report, p. 4).

182. Defendants' use of fake domains and websites to impersonate trusted institutions further facilitated the mirror law firm scheme. Investigators observed a surge in law-firm-themed spoof domains (often slight misspellings or hyphenations of real firm names) being used for scams and intrusions in recent years. Defendants exploited this method of deception, weaponizing look-alike domains to masquerade as official sources (including Plaintiff's firm and court sites) in order to steal credentials and hijack communications.

183. By using these convincingly spoofed domains, Defendants lured attorneys and staff into interacting with fake login pages and fraudulent emails, thereby gaining the keys to Plaintiff's practice and ongoing cases.

184. Defendants' mirror law firm scheme – leveraging DNS hijacking, email spoofing, and identity theft – prevented opposing counsel from even knowing a case was underway in some instances. It also deprived Plaintiff of any meaningful opportunity to respond or be heard, since his communications were being silently intercepted or misdirected. Only through extensive forensic analysis was Plaintiff able to uncover this scheme, which represents a next-generation APT tactic using the very name and reputation of a target law firm to carry out a farce of litigation, with real-world consequences.

185. After Farrow and his practice became aware of the victims of this scheme on or about June 3, 2024, the practice was effectively closed after 16 years in business by July 10, 2024. Thereafter, using an old computer and hard drives, Farrow filed two actions, one in Miami-Dade Circuit Court and one in Domestic Court seeking an injunction against one individual believed to have had great influence in procuring the threat actor group.

186. Thereafter, the threat actors did everything possible to thaw that those actions, while targeting Plaintiff and his family at their home, and from September through present, using their

infiltrations into the Florida Bar Network and Florida Electronic Filing Portal, and the federal CM/ECF System to interfere with the lawsuit he filed on February 5, 2025.

187. In that case, since the law firms appeared, the majority of which within a two hour span on a single day immediately Farrow initiated a controlled email test.

188. While 'what' has happened on 'real' court dockets in the cases Plaintiff filed since his law practice was effectively closed, and those matters, such as those filed ostensively by the Florida Bar seeking his immediate suspension from the practice of law at critical times, will, be addressed, when, and only when, due process of law can be restored – meaning in plain terms – that the threat actors have created a scheme which is by no means far-fetched as has caused and continues to cause substantial irreversible and immeasurable harm to Plaintiff, his family, his former clients, other attorneys, law firms, the Florida Bar and the jurisdiction and institutional integrity of this Court.

189. And, all of the same, functions, by and through a templated APT which, in part, leverages existing identified C2 Architecture (as defined at Appendixes A, B and C), stolen lawyer credentials (the names of those attorneys who have been so identified are found at Table B), infiltrations into existing judicial cyber-architecture or websites designed to trick users into providing their login credentials, exploiting the trusted relationships attorneys have with courts of law, and with each other as a legal profession and a host of other malicious cyber-assets, so as to, *inter alia,* cause intentional manipulations of judicial processes, procedures and mandates or otherwise serve the objectives of the cyber-criminal group or groups for their own profit, strategic advantage and/or gain.

190. **Injuries to Plaintiff and Others:** The racketeering activities of Defendants have directly and proximately caused injury to Plaintiff in his business and property. Plaintiff Farrow has suffered substantial economic losses, including but not limited to: loss of clients and prospective clients

(who lost confidence due to data breaches and disruptions), loss of contractual relationships and case opportunities, significant harm to his professional reputation and goodwill, and loss of the ability to practice law effectively (resulting in missed deadlines and the forfeiture of certain legal matters).

191. Farrow's law practice was essentially paralyzed by Defendants' actions—he was forced to shut down normal operations for extended periods while dealing with the breaches, resulting in missed deadlines and the loss of legal matters.

192. These injuries are concrete and quantifiable injuries to "business or property," as required by 18 U.S.C. § 1964(c). Plaintiff has also expended well over $75,000 in out-of-pocket costs for cybersecurity consultants, forensic analyses, hardware replacement, and security upgrades to respond to Defendants' intrusions. These costs are a direct injury to his property.

193. Furthermore, Plaintiff suffered damage to his computers and electronic data (e.g., destruction or encryption of files, physical wear on devices from repeated reformatting, etc.), which constitutes injury to property.

194. The interference with Plaintiff's and his family's personal electronic accounts (such as email and cloud storage) also resulted in the loss of valuable digital property (like important communications and documents).

195. The enterprise's acts have also injured the Florida Bar and the integrity of the state's judicial system (through the compromise of the eFiling Portal and court communications), though those broader injuries are relevant to public-interest considerations rather than Plaintiff's personal claim.

196. For RICO standing purposes, Plaintiff's losses in money, property, reputation, and now his law license, are directly attributable to Defendants' racketeering acts and were intended

consequences of the scheme (for example, causing Plaintiff to lose his cases or clients was part of Defendants' goal of benefitting whoever hired them, and of intimidating Plaintiff from pursuing his profession).

197. Each Defendant was a knowing participant in the pattern of racketeering, and each is jointly and severally liable for the resulting damages.

198. The scheme's success depended on the coordinated efforts of all Defendants, and the harm to Plaintiff was a foreseeable and natural consequence of the scheme (indeed, inflicting such harm was one of the scheme's primary objectives).

The Florida Judicial Infrastructure and Judicial Institutional Weaponization Scheme

199. As detailed above, prior court orders and law enforcement actions have not deterred Defendants' enterprise; rather, they adapted and continued their unlawful activities. Only comprehensive relief from this Court can redress Plaintiff's injuries and prevent future harm. Plaintiff alleges that unknown cyber-criminal actors infiltrated the Florida Bar's computer networks, disciplinary portals, and eFiling systems beginning in 2024, weaponizing those institutions to sabotage Plaintiff's rights and engineer fraudulent disciplinary outcomes.

200. On October 14, 2024, Plaintiff submitted a 70+ page response to Bar inquiries, addressing issues of communication failures and work stoppages caused by cyber interference. On October 15, 2024, Bar Counsel's assistant, Christine Mitchell, confirmed receipt of the response.

201. Despite this acknowledgment, within 24 hours grievance referral letters were issued under John Womack's name, reassigning all matters to Grievance Committee 17F under the chairmanship of Plaintiff's landlord's attorney, Richard Wiess. On October 18, 2024, Weiss Serota simultaneously posted an eviction notice on Farrow Law's office door.

202. Plaintiff alleges this was no coincidence: on the very day his response was confirmed, grievances were diverted to Wiess, while his firm acted against Plaintiff as landlord's counsel, a conflict of interest of the highest order.

203. Critically, two of the Bar complaints had response deadlines of November 12, 2024 — dates established by Womack's own letters to Plaintiff. Thus, even if Plaintiff had not responded on October 14, 2024, he was not tardy as to at least those two complaints on November 12, 2024.

204. Nevertheless, on November 12, 2024, Richard Wiess allegedly chaired a Grievance Committee 17F meeting that voted to escalate all 13 complaints to the Florida Supreme Court, characterizing Plaintiff as having "failed to respond." That decision was false: Plaintiff had responded timely, and as to two complaints, was not even due.

205. On November 25, 2024, a Petition for Order to Show Cause was filed in the Florida Supreme Court, purportedly signed by Womack. The petition omitted reference to Plaintiff's October 14 response and the November 12 due dates.

206. On December 6, 2024, Plaintiff drove again to Tallahassee to deliver the Marlin Technology Expert Report. From September 21, 2024 through that date, Plaintiff received no email or phone responses from Womack, despite repeated attempts.

207. On December 7, 2024, Weiss Serota filed a lawsuit on behalf of Regus Management to evict Plaintiff's firm. At an in-person meeting on February 25, 2025, Regus's representatives admitted Weiss Serota did not in fact represent them.

208. On December 8, 2024, Plaintiff received a letter from Womack warning him not to visit the Florida Bar in person again, and purporting to bar all communications except by email or regular mail.

209. On December 18, 2024, after an e-filing rejection, Plaintiff again drove to Tallahassee to hand-file his corrected response. That filing was partially corrupted: only 21 of 34 pages uploaded, with a blank placeholder page inserted — an anomaly consistent with adversarial tampering. A copy of same is being filed as Exhibit M.

210. On December 27, 2024, Plaintiff filed a Motion for Protective Order and Confidential Filing of three expert spreadsheets documenting infiltrations into the Florida Bar's network and Florida's eFiling Authority (myflcourtaccess.com). A copy of same is appended hereto as Exhbit N.

211. In that motion, Plaintiff warned the Florida Supreme Court that the evidence showed Bar employee usernames, passwords, and even law enforcement credentials had been compromised. He told the Court that the "discovered evidence provides the means to not only interfere with communications, but also to have access to all Florida Bar correspondence and pleading forms." The Florida Bar never responded to this motion, and the Florida Supreme Court never ruled upon it.

212. On January 3, 2025, Plaintiff and his wife, delivered the same spreadsheets in person to Bar staff in Tallahassee, again warning of systemic breaches. Despite this extraordinary hand-delivery, Plaintiff never received substantive acknowledgment.

213. In February 2025, Weiss Serota's Chief Operating Officer emailed Plaintiff, stating the firm had retained Florida Bar Staff Counsel Patricia "Patti" Savitz as its private attorney in a negligence action, and directed communications to her at **psavitz@floridabar.org**. At that same time, Savitz was still appearing in filings as counsel of record for the Florida Bar against Plaintiff.

214. On February 27, 2025, Plaintiff filed a Motion for Order to Show Cause, arguing that the case should be dismissed as moot because he had already complied with Bar inquiries and made

four separate trips to Tallahassee delivering responses, expert reports, and evidence. Plaintiff further raised that Weiss Serota had been represented by Bar Staff Counsel Patti Savitz while she simultaneously filed pleadings on behalf of the Florida Bar against Plaintiff. A copy of same is attached as Exhibit O.

215. On March 5, 2025, Staff Counsel Patti Savitz filed a response on behalf of the Bar. That response did not deny her connection to Weiss Serota, and it did not dispute Plaintiff's sworn statements that he had personally visited the Bar multiple times to deliver updated responses and materials.

216. On March 18, 2025, Plaintiff filed a Motion to Approve Stipulation for Dismissal Without Prejudice. The proposed resolution required Plaintiff to appear in person before new Bar Counsel, Randell Berman, at the Fort Lauderdale branch to bring his responses. A copy is appended as Exhibit P.

217. If Berman found the responses insufficient, Plaintiff agreed to cure them within two weeks. If Plaintiff failed, the Bar could reinstate the proceedings, at which point the Florida Supreme Court would have a straightforward record that Plaintiff had been given — and squandered — the opportunity to respond. In candor, Plaintiff disclosed that he had received an email from Investigator John Berrena claiming that Bar Counsel Berman "did not send" the stipulation email, and further asserting that Berrena himself tells Bar Counsel how to handle legal matters even though he is not an attorney.

218. On March 20, 2025, Plaintiff filed another motion, this one simply requesting an in-person meeting with Bar Counsel. Plaintiff asked that he be allowed to sit face-to-face with Berman, review the responses already submitted, and if any were deemed insufficient, provide supplements within five business days. Despite the modest scope of this request, the Bar never responded.

219. On June 18, 2025, the Florida Bar filed a **Second Petition for Emergency Suspension**. Unlike the November 25, 2024 petition, this filing was submitted under a rule that gave Plaintiff no opportunity to respond until after suspension. The petition was signed by Staff Counsel Savitz, but the line for the Bar's Executive Director — whose signature is required — was left blank.

220. The June 18 petition recycled seven complaints that had already been referred by the Supreme Court to a Miami Circuit Judge for handling in April 2025, yet it presented those same complaints as if they were established facts proving misconduct. This deprived Plaintiff of due process by treating contested allegations as adjudicated findings.

221. The June 18 petition also invoked cases involving Plaintiff's wife and Spagnuolo. Neither Garcia nor Spagnuolo had ever filed Bar complaints against Plaintiff, nor were they interviewed prior to the petition. Both were themselves documented victims of the same threat actor group.

222. Dr. Garcia, the named plaintiff in *Garcia v. PFS Financial*, submitted two affidavits confirming that Farrow could not have filed responses to motions in her case in July 2024 because his systems were disabled by cyber intrusions. She further attested that she too had been targeted by the threat actor group.

223. Spagnuolo had separately reported receiving threats from the threat actor group, yet the Bar still used his case as a basis to allege misconduct against Plaintiff. He too never filed a complaint or was interviewed before the June 18 petition.

224. The Second Petition leaned on affidavits that were themselves anomalous. Investigator Berman swore that Plaintiff had "forged a Florida Bar email" and that he had spoken with FBI agents who supposedly told him Plaintiff "had no case." It is highly unlikely, if not impossible, that FBI agents would comment in such terms on an active investigation.

225. Bar Counsel Berman further filed an affidavit denying he ever sent an email offering to stipulate to dismiss the First Petition — despite Plaintiff's candor to the Court acknowledging this irregularity months earlier.

226. Plaintiff alleges these cumulative anomalies — absent Executive Director signature, use of non-complainant witnesses, reliance on unverified affidavits, recycling complaints already referred to a referee, and presenting them as if adjudicated — constitute clear Indicators of Compromise ("IoCs"). They demonstrate that the June 18, 2025 Second Petition was not the product of ordinary disciplinary process but of a system under adversarial manipulation.

227. Plaintiff attaches hereto the Supplemental eForensic Report as Exhibit P and incorporates the same hereto. Plaintiff also is appended hereto and incorporating here with Appendix A, B, C and D from the CNF August 22, 2025 eForensic Expert Report and the September 1, 2025 forensic report as Composite Exhibit Q.

228. All Conditions Precedent to this action have occurred, been satisfied, or have been waived.

229. **Jury Demand:** Plaintiff demands a trial by jury on all issues so triable.

Count I – Violation of the Federal Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)

230. Plaintiff re-alleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 198 above, as if fully set forth herein.

231. This claim is brought under 18 U.S.C. § 1964(c) (civil remedies) for Defendants' violations of 18 U.S.C. § 1962(c). Section 1962(c) makes it unlawful for "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate… in the conduct of such enterprise's affairs through a pattern of racketeering activity."

232. **Enterprise:** Defendants John Does 1–15 and their co-conspirators form an *enterprise* within the meaning of 18 U.S.C. § 1961(4) – specifically, an association-in-fact enterprise. As alleged in detail above, this enterprise is an ongoing organization of individuals that functions as a continuing unit and has a common purpose of engaging in cybercrime (including fraud, extortion, and other illegal acts) for profit and malicious ends.

233. The enterprise is not a legal entity; it is an association-in-fact characterized by relationships among the Defendants, who each perform roles in furtherance of the enterprise's illicit activities.

234. The enterprise has the structural attributes of longevity, a degree of hierarchy (even if loose), and a shared purpose. Each Defendant is "associated with" the enterprise and has knowingly participated in the operation or management of the enterprise's affairs.

235. The enterprise is engaged in, and its activities affect, interstate and foreign commerce. The enterprise's operations span multiple states and countries, involve the transmission of data and funds across state lines, and target businesses and institutions involved in interstate commerce (e.g., multi-state law firms, cloud service providers, etc.).

236. The predicate acts (detailed below) themselves involve interstate communications and transactions (emails, internet transmissions, bank wires, etc.). By sabotaging a multi-state law practice and compromising national networks (such as Microsoft's and Google's services), the enterprise has impacted commerce well beyond the State of Florida.

237. **Pattern of Racketeering Activity:** Within the last ten years, Defendants have conducted and participated in the enterprise's affairs through a *pattern of racketeering activity* consisting of numerous predicate acts indictable under 18 U.S.C. § 1961(1). The pattern includes at least the following categories of racketeering acts: extortion (18 U.S.C. § 1951; Fla. Stat. § 836.05), wire fraud (18 U.S.C. § 1343), identity theft and fraud in connection with access devices (18 U.S.C.

§§ 1028, 1029), and acts indictable under 18 U.S.C. §§ 1503, 1512, and 1513 (obstruction of justice and retaliating against a witness/victim). These acts are described in detail in the preceding sections and are incorporated here.

238. Each of these acts is *related* in that they had the same or similar purposes (to enrich Defendants or their clients, to sabotage or gain advantage in legal matters, and to cover up the scheme), involved the same or similar participants (the Doe Defendants and their associates), and were committed in similar fashion (through sophisticated cyberattacks using malicious infrastructure and deceit).

239. The acts had overlapping victims – for instance, the theft of one attorney's identity was used to defraud that attorney's clients; the hacking of Plaintiff's email was used to extort Plaintiff and simultaneously defraud others. The racketeering acts reinforced and complemented each other as part of Defendants' overall scheme.

240. The racketeering acts constitute a *continuous* pattern. They began at least as early as 2019 (and investigations suggest planning and preliminary acts even before then) and continued through the filing of this suit (and, absent relief, are likely to continue thereafter). This timeframe far exceeds the statutory minimum for a "closed-ended" period of continuity (which generally means conduct over more than a year).

241. Moreover, the nature of Defendants' conduct indicates a threat of continued criminal activity. Defendants' business model is to carry out serial cyberattacks for hire; thus, even if their campaign against Plaintiff were successful or complete, they would continue targeting new victims as long as it is profitable. Indeed, Defendants have already targeted multiple law firms and attorneys beyond Plaintiff, as well as entities in other industries, and have demonstrated adaptability to

circumvent temporary setbacks. This threat of repetition establishes an "open-ended" continuity as well.

242. By engaging in the acts above, each Defendant *conducted or participated* in the conduct of the enterprise's affairs, directly and indirectly. Each Defendant played a part in directing the enterprise's affairs – whether by maintaining the C2 infrastructure, deploying malware, managing stolen data, or intimidating victims to prevent interference.

243. Their collective actions show a common purpose and knowledge: they worked together to further the enterprise's criminal goals. For example, one group of Defendants would compromise an attorney's accounts (wire fraud/identity theft), another would deploy ransomware or issue threats (extortion), and others would ensure that stolen data could be monetized or used in other schemes.

244. Each set of acts was coordinated through the enterprise's channels (e.g., via dark web forums or secure communications among members).

245. As Microsoft's DCU principal investigator noted about this enterprise, the Defendants "use common tools, a common codebase, and common tactics," and "share command and control resources," operating effectively as a criminal enterprise. Each Defendant's participation was knowing, necessary, and deliberate.

246. **Violation of § 1962(c):** By and through the foregoing conduct, each Defendant has violated 18 U.S.C. § 1962(c). Specifically, each Defendant, being a person employed by or associated with the aforementioned enterprise, conducted or participated in the conduct of the enterprise's affairs (which engage in and affect interstate commerce) through a pattern of racketeering activity as defined by 18 U.S.C. § 1961(1) and (5).

247. Each Defendant's actions and the predicate acts were interdependent pieces of the overall racketeering scheme.

248. **Injury:** As a direct and proximate result of Defendants' racketeering violations, Plaintiff Farrow has suffered injury to his business and property, as detailed above.

249. These injuries include significant loss of money (costs of remediation, lost income, lost clients), damage to property (computer systems and data), and loss of business opportunities and goodwill.

250. The injuries were caused "by reason of" the RICO violations in that they are the intended outcomes of Defendants' pattern of racketeering (for instance, Plaintiff's business was the target of the sabotage and extortion).

251. But for Defendants' conduct, Plaintiff would not have suffered these losses; and Defendants' conduct was a substantial factor in bringing about Plaintiff's harm.

252. Plaintiff's injuries are recoverable under civil RICO, which provides for treble damages, costs, and attorneys' fees to the injured party. In addition, because the racketeering acts are ongoing, Plaintiff seeks equitable relief to prevent further injury.

WHEREFORE, pursuant to 18 U.S.C. § 1964(c), Plaintiff demands judgment against Defendants, jointly and severally, for *treble* the amount of actual damages proven at trial, for the costs of this suit and reasonable attorneys' fees, and for such further relief as the Court deems just and proper. Plaintiff also seeks appropriate *injunctive relief* to prevent and restrain further violations of 18 U.S.C. § 1962(c) (to the extent such equitable relief is within the Court's powers in a civil RICO action), including an order enjoining Defendants from continuing the racketeering enterprise and prohibiting them from accessing Plaintiff's or others' computers and accounts, as set forth in more detail below.

Count II – Conspiracy to Violate RICO, 18 U.S.C. § 1962(d)

253. Plaintiff re-alleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 261 above.

254. This count is brought under 18 U.S.C. § 1962(d), which makes it unlawful for any person to conspire to violate any of the substantive provisions of § 1962 (including § 1962(c) as alleged in Count I). Section 1962(d) is violated when a defendant, by words or actions, objectively manifests an agreement to participate, directly or indirectly, in the affairs of an enterprise through the commission of multiple racketeering acts.

255. **Agreement and Common Plan:** As detailed above, Defendants knowingly agreed and conspired with each other (and with other unknown participants) to conduct and participate in the conduct of the enterprise's affairs through a pattern of racketeering activity.

256. The very existence of the coordinated scheme – involving distinct roles and a division of labor among the Doe Defendants – demonstrates a *meeting of the minds* and an agreement on the essential nature of the plan.

257. Defendants shared the common objective of the conspiracy: to unlawfully infiltrate computer systems, steal data, extort victims, and otherwise profit from cybercrime, all by way of the enterprise described.

258. Each Defendant knew that the enterprise's affairs would be conducted through a pattern of racketeering acts. Each agreed to facilitate or participate in the scheme with that knowledge.

259. The conspiracy is evidenced by, inter alia, the sharing of criminal tools and infrastructure, the synchronized actions taken by different Defendants in furtherance of the scheme, and communications among the actors (for example, coordination through online forums or secure messaging to deploy ransomware after initial access is obtained). No legitimate rationale can

explain the complex, orchestrated sequence of steps that Defendants collectively undertook – the only plausible inference is that they agreed to work together in furtherance of the criminal enterprise.

260. Each member of the conspiracy also knew and foresaw that the success of the overall scheme required the commission of multiple racketeering acts.

261. Defendants did not need to personally commit every act; by conspiring, each Defendant became responsible for the acts of his co-conspirators. In essence, Defendants manifested an agreement to pursue the same criminal objectives (the continuity of the enterprise and its illegal pattern of activity) and understood that predicate acts would be carried out by one or more of them to advance the scheme.

262. **Violation of § 1962(d):** Given that Plaintiff has pled the existence of the § 1962(c) enterprise and pattern, Defendants' agreement to facilitate that substantive violation is itself a violation of § 1962(d). Even if any Defendant might claim not to have personally committed two racketeering acts, they are still liable for the acts of the conspiracy as a whole. Each Defendant took part in the plan knowing of its scope and intending to help accomplish its goals; that is sufficient for RICO conspiracy liability.

WHEREFORE, Plaintiff demands judgment against Defendants, jointly and severally, for their conspiracy to violate RICO, including an award of *treble damages* in an amount to be proved at trial, plus costs and attorneys' fees pursuant to 18 U.S.C. § 1964(c). Plaintiff further requests that the Court enter all appropriate preliminary and permanent injunctive relief to prevent further violations of 18 U.S.C. § 1962, as set forth below and as justice requires.

Count III – Florida RICO (Florida RICO Act, Fla. Stat. § 895.02 *et seq.*); Request for Injunctive Relief Under Fla. Stat. § 895.05(6)

263. Plaintiff re-alleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 261 above.

264. 70. This count is brought under the Florida RICO Act, Fla. Stat. § 895.01 *et seq.*, which mirrors the federal RICO statute and likewise makes it unlawful to conduct an enterprise through a pattern of racketeering activity.

265. The Defendants' conduct described above constitutes racketeering activity under Florida law (including, e.g., violations of the Florida Communications Fraud Act, Fla. Stat. § 817.034; offenses relating to electronic mail under Fla. Stat. § 668.803; extortion under Fla. Stat. § 836.05; and computer-related crimes under Fla. Stat. § 815.06).

266. The enterprise and pattern elements under Florida law are satisfied for the same reasons detailed for the federal claim.

267. Because the pattern of racketeering is ongoing and threatens to continue, Plaintiff seeks injunctive relief under Fla. Stat. § 895.05(6) in addition to damages. Florida's RICO statute explicitly authorizes injunctive remedies "to prevent and restrain" violations of § 895.03, including preliminary injunctions.

268. Defendants' actions constitute a continuing threat of irreparable harm that cannot be fully remedied by monetary damages alone. As detailed, Defendants' pattern of racketeering is ongoing and shows no signs of voluntary cessation.

269. The damage includes compromise of highly sensitive and privileged information (once lost, confidentiality cannot be restored), erosion of trust in the legal system (a public harm), and imminent risk to personal safety (e.g., threats to Plaintiff's family).

270. These injuries cannot be adequately compensated after the fact, and they multiply each day the enterprise remains operational.

271. Courts have granted injunctive relief to private plaintiffs under this statute to freeze or disrupt criminal enterprises pending final judgment (the statute explicitly authorizes preliminary injunctions).

272. Here, an injunction would serve the same purpose: it would immediately halt Defendants' misuse of the instrumentalities (computers, accounts, servers, etc.) they have compromised and prevent further racketeering acts during the pendency of this case.

273. **Relief Sought (Florida RICO Injunction):** Plaintiff seeks a temporary, preliminary, and permanent injunction under Fla. Stat. § 895.05(6) to dismantle Defendants' illicit operations and prevent ongoing racketeering acts.

274. In particular, Plaintiff requests that the Court order relief including but not limited to:

a. **Disabling Current Infrastructure:** Ordering that all Internet domains and IP addresses owned, controlled, or used by Defendants in the course of the racketeering scheme (specifically including the malicious domains and IP addresses identified in Appendixes A, B and C, and any equivalent substitute domains or IPs they are using) be immediately suspended or placed under neutral control. This may include transferring those domains to a receiver or to Plaintiff, and instructing the relevant domain registries and registrars to lock and/or redirect those domains as needed to prevent further malicious use. Likewise, any cloud accounts or hosting accounts used by Defendants for the enterprise (such as those with Microsoft Azure, Amazon AWS, Google Cloud, etc., as identified in Appendixes A, B and C or the expert reports) should be suspended or rendered inaccessible. This relief parallels

that granted in prior cases: for example, in *Microsoft Corp. v. John Does*, No. 1:23-cv-02447 (E.D.N.Y. 2023), the court entered injunctive orders transferring and disabling the defendants' domains and IP addresses – relief which Plaintiff seeks here as well.

b. **Preventing New Infrastructure:** An order enjoining Defendants from establishing or using any new domain name, website, IP address, or online infrastructure to carry out the same or similar unlawful acts. In practical terms, should Defendants attempt to set up new servers or domains to continue their attacks, upon notice to the Court or Plaintiff's counsel, such substitute infrastructure shall be subject to the same provisions of the injunction (i.e., disabled or transferred to neutral control) without the need for additional proceedings. This provision will prevent Defendants from evading the injunction by simply shifting to alternative instrumentalities once their current tools are restrained.

c. **Monitoring and Enforcement:** Authorizing Plaintiff (through counsel, experts, or a court-appointed receiver) to engage in reasonable actions to monitor compliance and enforce the injunction. This may include operating "sinkhole" servers for any redirected domains/IPs to collect callback traffic (as courts have allowed in similar cases) and sharing such data with law enforcement or affected victims, solely for purposes of preventing further harm. Additionally, Plaintiff's agents may provide copies of the injunction to any third-party providers (domain registries, hosting companies, etc.) to ensure they take appropriate action; any such third parties should be immunized from liability for good-faith compliance with this Court's Order. Any attempt by Defendants to shift to new servers or accounts in violation

of the injunction shall be treated as a continuation of the prohibited conduct, and Plaintiff may seek expedited relief from the Court to neutralize the new instrumentalities.

275. Plaintiff has demonstrated a likelihood of success on the merits (through evidence linking Defendants to a pattern of criminal acts), a likelihood of irreparable harm absent relief, that the balance of harms favors an injunction, and that the public interest is served by preventing ongoing racketeering.

276. The requested injunctive relief is narrowly tailored to prohibit only unlawful activity and to dismantle the specific infrastructure being used to harm Plaintiff and others.

WHEREFORE, Plaintiff requests a preliminary and permanent injunction under Fla. Stat. § 895.05(6) to halt Defendants' ongoing racketeering and grant the relief outlined above, and such other relief as the Court deems just and proper.

Count IV – Violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030

277. Plaintiff re-alleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 228 above.

278. The Computer Fraud and Abuse Act ("CFAA") prohibits, inter alia, (a) the intentional unauthorized access to protected computers to obtain information, and (b) the transmission of programs, code, or commands that cause damage to protected computers.

279. Defendants' actions, as described above, violate multiple provisions of the CFAA, including but not limited to 18 U.S.C. § 1030(a)(2)(C) (intentionally accessing a computer without authorization, or exceeding authorized access, and obtaining information from a protected computer) and 18 U.S.C. § 1030(a)(5)(A) (knowingly causing the transmission of a program, code,

or command, and as a result intentionally causing damage without authorization to a protected computer).

280. Plaintiff's computers, email servers, and cloud accounts — as well as the computers of third parties (including clients, vendors, Plaintiff's counsel and colleagues, the Florida Bar, the Florida Courts' eFiling Authority, multiple Florida state court Clerk systems for multiple Circuits, and even the CM/ECF filing system of the U.S. District Court for the Southern District of Florida) — that have been affected by Defendants' intrusions are each "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

281. They are used in interstate commerce and communication (being connected to the Internet and used for communications across state lines).

282. Defendants, without authorization or by exceeding any authorized access, intentionally accessed these computers and systems via malware, stolen credentials, and other deceptive or fraudulent means.

283. By doing so, Defendants obtained information of value (including, but not limited to, emails, documents, and sensitive personal data stored on those systems).

284. 79. Defendants' installation of the *Cobalt Strike Beacon* malware on Plaintiff's computers constitutes the transmission of a program or code to a protected computer.

285. Defendants did this knowingly and with the intent to establish unauthorized control over those computers. That act caused both "damage" and "loss" as defined by the CFAA.

286. The damage includes impairment to the integrity and availability of Plaintiff's data and systems — for example, the malware caused system slowdowns and crashes, and required removal efforts that impaired the normal operation of the computers.

287. The loss includes the reasonable cost of responding to the offense, conducting damage assessments, restoring data and systems to their condition prior to the offense, and any revenue lost or other consequential damages because of interruption of service. Here, the loss from Defendants' conduct easily exceeds $5,000 in value during a one-year period, as Plaintiff has expended well over that amount on forensic and remediation measures, and has suffered additional losses as described above.

288. Defendants also unlawfully accessed email accounts and cloud storage belonging to Plaintiff and his law firm, which are part of protected computer systems (e.g., Microsoft's Office 365 cloud email servers).

289. By installing hidden forwarding rules and exfiltrating emails and files, Defendants obtained information from protected computers without authorization, further violating 18 U.S.C. § 1030(a)(2)(C).

290. Each instance in which Defendants accessed Plaintiff's email account (or cloud data) through deceptive means (such as using stolen credentials or a man-in-the-middle technique) is a separate, unauthorized access under the CFAA.

291. Defendants' conduct was intentional and malicious. They acted with intent to defraud (in the CFAA context, meaning to wrongfully obtain something of value or to deceive for wrongful gain) and with intent to extort.

292. By stealing information and even using it to threaten Plaintiff (for example, demanding that he drop certain legal matters or face the exposure of personal data), Defendants sought to obtain something of value — whether a litigation advantage or revenge — via their unauthorized access.

293. They also intended to enrich themselves or their clients (for instance, through ransomware payments or by selling stolen data).

294. Their interference with court filings and attorney accounts was likewise intentional and designed to obstruct justice and reap illicit benefits, with willful disregard for the law.

295. Plaintiff Farrow brings this CFAA claim as an individual whose protected computers were affected by some of the very same malicious cyber architecture that had been subject to federal injunctions in other cases, and as someone whose computers were compromised using identical or nearly identical cyber-tradecraft as that used in those other cases (both civil and criminal).

296. These facts underscore the willfulness and reckless disregard of Defendants' conduct under the CFAA, demonstrating that it was part of a broader malicious campaign.

297. Additionally, Farrow asserts this claim as a victim not only of direct attacks on his own computers, but also of attacks on protected computers belonging to institutions that directly affect him: for example, the protected computer networks of the Florida Bar and Florida's eFiling Authority, which were infiltrated as part of Defendants' scheme to target Farrow and others.

298. By infiltrating those systems, Defendants effectively compromised Farrow's ability to practice law and communicate, thus victimizing him through third-party systems as well.

299. As a direct and proximate result of Defendants' CFAA violations, Plaintiff has suffered and continues to suffer irreparable harm and economic losses.

300. Plaintiff has spent well over the CFAA's $5,000 statutory threshold on responding to and investigating the breaches, conducting damage assessments, restoring systems, and other remedial measures.

301. The precise loss figure is ongoing and will be proved at trial, but it includes the costs of multiple forensic analyses, replacement of computer hardware, extensive time investment (lost billable opportunities), and the value of data that could not be recovered.

302. Beyond these calculable costs, the harm caused by Defendants' actions includes loss of clients (and associated revenue), damage to Plaintiff's professional reputation, and severe disruption to his law practice. Farrow has suffered emotional distress and loss of use of his equipment and accounts. Importantly, many of these injuries (loss of client trust, missed legal opportunities, harm to professional standing) are *irreparable* and not readily compensable by money damages.

303. Absent injunctive relief, Defendants' ongoing ability to access and manipulate computers and accounts will continue to harm Plaintiff in ways that cannot be fully remedied after the fact.

304. Plaintiff is entitled to *compensatory damages* and *injunctive relief* pursuant to 18 U.S.C. § 1030(g).

305. At this juncture, given the urgent threat of continued attacks, Plaintiff primarily seeks injunctive relief as outlined below to prevent or minimize further irreparable harm from Defendants' actions. The CFAA explicitly allows victims to seek such equitable relief to halt ongoing violations.

WHEREFORE, Plaintiff requests that the Court enter an order granting the following relief under the CFAA:

a. *Injunctive Relief:* Temporarily, preliminarily, and permanently enjoin Defendants, and anyone acting in concert with them, from: (i) accessing or attempting to access Plaintiff's computers, email accounts, or cloud systems without authorization; (ii) using, disclosing, or altering any data obtained from Plaintiff through their unauthorized access; and (iii) engaging in any further unauthorized access of any computers or accounts belonging to Plaintiff or his law practice.

b. *Removal of Malware:* Require Defendants to immediately cease all use of malware or backdoors installed on Plaintiff's devices and to remove any such malware at their expense (or assist law enforcement in doing so).

c. *Limited Self-Help Authorization:* Authorize Plaintiff (and his designated experts) to take reasonable steps to remotely disable or remove Defendants' malware from his devices and related affected systems, including by communicating with the malicious C2 servers for the sole purpose of issuing uninstall commands or otherwise neutralizing the malware. Any data collected through such efforts will be used only to identify affected victims, to assess the scope of compromise, or to hand over to law enforcement.

d. *Staying Effect of August 4, 2025 Order of Florida Supreme Court.* Plaintiff requests a stay of the Florida Supreme Court Order of August 4, 2025, and to all its effects, for 90 days, or until further order of this Court.

e. *Other Relief:* Granting such other and further relief as this Court deems just and proper under the CFAA, including compensatory damages (to be trebled under RICO), punitive damages if warranted, and the costs of the suit and reasonable attorney's fees.

Count V – All Writs Act / Equitable Relief in Aid of Jurisdiction (28 U.S.C. § 1651)

306. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 268 and the foregoing paragraphs as if fully set forth herein.

307. Plaintiff seeks an injunction under the All Writs Act, 28 U.S.C. § 1651, as an aid to the Court's jurisdiction and in furtherance of the equitable relief sought under the substantive claims (in particular, under the CFAA and Florida RICO counts).

308. The All Writs Act authorizes this Court to "issue all writs necessary or appropriate in aid of [its] jurisdiction[] and agreeable to the usages and principles of law."

309. Pursuant to longstanding precedent, and precedent which relates specifically to the conduct and actions of the Defendants outlined herein, courts have utilized the All Writs Act to ensure their injunctions are effective against not only the defendants but also third parties whose action or inaction could frustrate the implementation of relief.

310. As detailed above, Defendants have persisted in using certain IP addresses, domain names, and online accounts as part of their attack infrastructure. Many of these resources are operated by third parties – for instance, domain name registries, registrars, hosting companies, VPN providers, and cloud service providers – that may not currently be before the Court.

311. In prior cases such as *Microsoft v. Does*, No. 1:23-cv-02447 (E.D.N.Y. 2023), as well as *Google LLC v. Starovikov* (S.D.N.Y. 2021), and others, courts exercised authority under the All Writs Act to direct third parties to take down or block access to malicious domains and IPs, to ensure that TROs and preliminary injunctions were effectively implemented. Here, similar intervention is warranted.

312. Specifically, Plaintiff requests that the Court invoke its All Writs Act power to compel the assistance of relevant third parties in executing any injunction entered in this case.

313. Without binding these third parties, there is a significant risk that Defendants could simply shift their operations to new accounts or slightly modified domain names, thereby evading the Court's direct injunction against Defendants.

314. With coordinated relief – such as orders compelling domain registries to suspend or transfer the malicious domains listed in Appendixes A, B and C, and orders authorizing infrastructure providers to block network traffic to and from Defendants' IP addresses – the Court can halt the abuse comprehensively.

315. This Court's jurisdiction to grant such ancillary relief is well-established. For example, in *Microsoft v. Does*(E.D.N.Y. 2023), the court invoked the All Writs Act to enjoin the world's top-level domain registries (Verisign for .com, Public Interest Registry for .org, etc.) from allowing those defendants to continue using certain domains.

316. Likewise, in *Google v. Starovikov*, the court used the Act to direct Internet hosting providers to take down the botnet's servers. These precedents demonstrate that where, as here, non-parties are in a position to help enforce an injunction (and are not themselves adverse to the plaintiff), the All Writs Act can be applied.

317. The relief sought is "necessary or appropriate" in aid of the Court's jurisdiction because it ensures that Defendants cannot defeat the Court's ability to grant meaningful relief. The heart of this case is stopping Defendants' illegal cyberattacks.

318. If the Court issues only a bare injunction against Defendants, they (being elusive and likely offshore) might ignore it, and the vital step of disabling their infrastructure would not occur unless third parties cooperate.

319. By binding the third-party registrars, registries, hosting firms, etc., the Court closes off Defendants' escape routes and preserves its jurisdiction to fully resolve the controversy.

320. There is minimal, if any, burden on legitimate interests by doing so: the targeted IP addresses and domains are being used exclusively for wrongdoing (e.g., a Nexeon server at 172.93.148.174 that serves as a C2 node, or domains like those in Appendixes A, B, C and D that have no legitimate content).

321. To the extent any legitimate services are co-hosted on an IP that is to be blocked, the injunction can be tailored in coordination with the provider to minimize collateral impact.

322. Notably, Microsoft's lead investigator in 2023 attested that it is technologically feasible to surgically disable malicious subdomains or processes on a shared server without affecting others. Plaintiff's experts concur and stand ready to assist in implementing such narrowly tailored measures.

323. An All Writs Act order here also serves to *enforce and extend the effect of prior court orders* that Defendants have flouted. As described, infrastructure that was enjoined in earlier cases (for example, certain IP ranges like 172.93.148.0/16, or specific malicious domains named in those cases) is still being used by Defendants.

324. This Court's injunction will put Defendants (and the world) on notice that continuing to use any part of that previously-enjoined infrastructure, or any slight variant of it, will result in immediate action and potential contempt.

325. It also signals to infrastructure providers that they must be vigilant and act decisively when presented with evidence of abuse (as here). In essence, it reinforces prior injunctions and ensures Defendants gain no advantage from the lapsing or geographic limitations of those orders.

326. In sum, the All Writs Act provides the Court with flexibility to cut off Defendants' avenues of attack. Plaintiff has shown a clear need for expansive relief to stop ongoing violations and to protect the Court's ability to render a judgment.

327. Without such ancillary relief, any narrower injunction could be easily evaded by Defendants simply by shifting tactics or using third-party services beyond the direct control of the litigants. The relief requested is carefully tailored to prevent that outcome and to bring the entire malicious scheme to a halt.

328. No relief broader than necessary is sought. Plaintiff does not ask to affect any innocent party's assets or operations.

329. The focus is solely on malicious domains, IPs, and accounts for which there is substantial evidence of their use in Defendants' unlawful conduct (as identified in Appendixes A, B and C and in the expert reports). Implementing the All Writs Act injunction will simply ensure those instrumentalities are disabled and remain unavailable to Defendants, thereby preserving the status quo of a secure environment free from Defendants' interference.

330. This Court has both the authority and the duty to protect its ability to provide effective relief; binding the relevant third parties in this manner is in service of that duty.

331. The *public interest* heavily favors the issuance of the requested writs. Defendants' actions undermine public trust in the legal system, threaten the confidentiality of legal communications, and endanger the security of countless individuals and organizations.

332. By granting relief under the All Writs Act, the Court will protect not only Plaintiff's rights but also those of numerous other potential victims (attorneys, clients, courts) from continuing harm. The requested injunctions will bolster the cybersecurity of the legal community and affirm that the judicial system can defend itself against such malign attacks.

333. The All Writs Act relief, in combination with the relief sought under the CFAA, RICO, and Florida law, will comprehensively address the threat posed by Defendants. It fills any gaps by empowering third parties to act decisively.

334. The requested relief is narrowly focused on preventing ongoing illegal conduct and protecting the Court's ability to render a final decision in this case without being undermined by Defendants' evasions.

335. Lastly, Plaintiff notes that such All Writs Act relief has been granted in at least half a dozen similar cases in the last few years without any known harm to third parties' legitimate operations. It is a proven approach to contain sophisticated cyber threats. Plaintiff stands ready to assist the Court in crafting and executing the details of these writs to ensure effective and equitable implementation.

WHEREFORE, Plaintiff respectfully requests that the Court issue an Order under the All Writs Act and the Court's inherent equitable powers as follows:

a. **Ordering a Meeting Between Plaintiff and Department of Justice and Report and Recommendations:** Plaintiff requests this Court Order Service of its Written Order with Respect to Plaintiffs' Motion for Ex Parte Emergency Relief Be Served Via Hand-Delivery by the Federal Mashal upon the Department of Justice, Miami Office, and the Special Agent in Charge of the Miami Field Office of the Federal Bureau of Investigation within 48 Hours and that Plaintiff meet with the DOJ and/or the FBI's Cyber-Team with Respect to his Evidence of Attribution and Containment Directives, and that a Meeting be Scheduled As Soon As Practicable but no more than three business days after service of the Order. And, within 48 hours of that meeting, that the DOJ and Plaintiff respectively file any requested limitations, recommendations or otherwise upon Plaintiff's containment directives which this Court is authorizing in a Temporary Restraining Order prepare separate reports and recommendations with respect to any of the other directives within this Court's

Order not later than five business days after the entry of this Court's Initial Restraining and Service Order. Plaintiff requests that the attendance at this meeting by representatives of Microsoft Digital Unit as placed Microsoft Corporation in possession of the access to the IP addresses, domains and other cyber-infrastructure noted at Appendixes A, B and C from, at the very least, the United States District Court for the Eastern District of New York, and United States District Court for the Eastern District of Virginia. As such, Plaintiff requests that he be permitted to serve a copy of the injunction order in person, upon Microsoft Corporation and/or its Attorneys of Record, Crowell & Morning.

b. **Orders as the Florida Bar:** Plaintiff requests that this Court enter an Order pursuant to its Authority Under the All Writs Act that the Florida Bar Request a Stay of the Referee Proceedings and a Stay of the September 3, 2025 suspension date, as well as, as to any other requirements of Plaintiff in this Case, such request to be filed under all Case Numbers related to any Suspension Proceedings in person with live signatures of all Bar Counsel with the Clerk of the Florida Supreme Court to avoid any possibility of the cyber-criminal interference and such request to be filed under seal with the Florida Supreme Court with a hand-delivered copy to Plaintiff. Plaintiff requests the Florida Bar to file the request within 24 hours of service and that the same include a request to modify or suspend that portion of the Florida Supreme Court's Order which prevents him from initiating cases, or that require him from withdrawing from representation from pending cases before this Court, especially the litigation wherein Plaintiff represents his wife, his child, himself and his practice. Plaintiff Requests that the Florida Bar file a notice of

compliance with this Court with copy of the hand signed and filed Request to the Florida Supreme Court under seal within 48 hours of filing same with the Florida Supreme Court.

c. **Orders as to Related Cases:** Plaintiff requests that this Honorable Court Consolidate for all purposes or for the purpose of effectuating a stay of proceedings, or that this Court's Order permit Plaintiff to File an Ex Parte Motion Under Seal in the related case matter styled: Farrow v. IOA Group, Inc, U.S.D.C., S.D.Fla, 25-cv-20544 Smith-Hunt conventionally with the Clerk of this Honorable Court.

d. Directing the relevant domain name registries and registrars (including, but not limited to, Verisign for ".com" domains, Public Interest Registry for ".org" domains, and any other registry or registrar responsible for the top-level domains of the malicious domains listed in Appendixes A, B and C) to immediately take down, transfer to Plaintiff's control, or otherwise render inaccessible all domain names identified in Appendixes A, B and C (and any domains proven to be controlled by Defendants for their scheme). This may include changing the authoritative name servers for those domains to servers controlled by or accessible to Plaintiff's experts (i.e., "sinkhole" servers), to ensure any traffic intended for those domains is redirected for defensive collection and analysis.

e. **Hosting and Infrastructure Providers:** Directing any Internet hosting providers, cloud service providers, and data centers providing service to the IP addresses listed in Appendixes A, B and C (or to any new IP addresses Defendants migrate to, once known) to cease routing traffic to and from those IPs, or to otherwise disable those IP addresses, until further order of the Court. This includes, without limitation,

providers such as Nexeon (for IP 172.93.148.174 and related range 172.93.148.0/16), Rackspace or its affiliates (for any IPs in the 146.20.161.0/24 range found in Appendixes A, B and C), Proofpoint or its cloud subsidiaries (for any IPs in the 148.163.0.0/16 range, if identified), and *any other entity* assigned any IP address listed in Appendixes A, B and C. Upon being served with the Court's Order, such providers should take reasonable steps to isolate and block the malicious use of those IPs (for example, by null-routing them or otherwise preventing any traffic to or from those addresses). If an IP address hosts legitimate customers in addition to Defendants' malicious content, the provider is directed to work with Plaintiff's counsel to either (i) disconnect the specific virtual server or account associated with Defendants' use, or (ii) apply filtering rules that drop any traffic associated with Defendants' malware communications (to be identified by Plaintiff's experts). The goal is to suspend Defendants' access while minimizing impact on others.

f. **Assistance in Enforcement:** Authorizing Plaintiff himself, through counsel or designated agents to deliver copies of the Court's Order to any such third-party including the law firms of record in the Farrow v IOA Group Case, as well as, providers and, in coordination with them, to take steps to ensure compliance. For example, Plaintiff may provide a domain registrar a list of domains from Appendix A and request their immediate suspension or transfer; the Order would oblige the registrar to comply forthwith. Likewise, Plaintiff's experts may work with a data center to redirect malicious domain traffic to a controlled sinkhole server (as mentioned, to collect evidence of victim IPs and the extent of

compromise). Any data collected in this manner will be used solely for lawful purposes — such as identifying affected victims to notify them or understanding Defendants' methods — and will be safeguarded under protocols approved by the Court.

g. **No New Variants:** Ordering that Defendants, and any persons in active concert or participation with them, are forbidden from using, or registering, any new domain or IP address that is merely a variant or successor of the ones enumerated in Appendixes A, B and C, if done for the purpose of engaging in the same or similar unlawful conduct. In practical terms, should Defendants attempt to set up a new domain or server to continue their attacks, upon notice to the Court or Plaintiff's counsel, such domain or server shall be subject to the same disabling and transfer provisions of this Order. This clause will prevent trivial work-arounds like adding a numeral to a blocked domain or moving to an adjacent IP address block.

h. **Immunity for Compliance:** Providing that any actions taken by third parties in compliance with this Order shall not give rise to any liability, and that such third parties are hereby immunized and held harmless for good-faith compliance. The All Writs Act, in conjunction with the Court's equitable authority, permits the Court to ensure that those assisting the Court are protected from potential contractual or legal claims. For example, if a hosting provider terminates an account due to this Order, Defendants cannot sue them for breach of contract; if a domain registry suspends a domain pursuant to the Order, that compliance shall not be deemed a violation of any duty to Defendants. This relief is consistent with that granted in similar cases under Rule 65 and 28 U.S.C. § 1651.

i. **Service of Order:** Allowing that Plaintiff (through counsel or court-appointed agents) may serve copies of this Order on any third parties as needed to effectuate the disabling of Defendants' infrastructure. Service may be accomplished by electronic means (email, web portal, etc.) or personal delivery, whichever is most practical. If the Court issues this Order ex parte, it may be temporarily sealed until execution, and thereafter Plaintiff may provide notice of the Order to Defendants by any reasonable means. Plaintiff shall file a notice with the Court identifying which third parties have been served, to keep the Court apprised of compliance efforts.

j. **Continued Jurisdiction:** Stating that the Court retains jurisdiction to modify, enforce, or clarify the Order upon application by any party or any affected third party. If any third party, upon receiving the Order, has uncertainty or seeks modification (for instance, a hosting provider needing to clarify scope), they may apply to the Court for appropriate relief. Defendants, once they receive notice of the Order, may also appear (through counsel or anonymously, if necessary) to seek dissolution or modification of the Order. Until or unless modified by the Court, the Order shall remain in full force.

k. **Other Relief:** Granting such other and further relief as may be necessary to carry out the terms of the injunction and to ensure that Defendants' malicious cyber activities are fully halted. This catch-all allows the Court to address unforeseen issues in executing the injunction and to ensure the intended result (cessation of the attacks) is achieved. Given the evolving nature of cyber threats, flexibility in enforcement is important.

Respectfully Submitted,

September 2, 2025

Plaintiff Jay Lewis Farrow, hereby certifies, under penalty of perjury, that all of the above factual statements made within this Corrected Verified Complaint are true and correct, to the best of his knowledge, recollection and belief.

Jay F. Farrow, pro se
[1409 Baracoa Ave]
[Coral Gables, Florida 33146]
[jay_farrow@tuta.com]

3472768652