UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

JAY LEWIS FARROW, an individual, Plaintiff, v. JOHN DOES 1 through 20, Defendants.	Case No. 25-cv-0633 **FILED UNDER SEAL**

VERIFIED COMPLAINT

COMES NOW Plaintiff Jay Lewis Farrow ("Plaintiff" or "Farrow"), pr se, and hereby alleges the following against Defendants John Does 1 through 20 ("Defendants"):

Introduction and Preliminary Statement

Emergency Nature of Action: This is an emergency action to halt a years-long and ongoing Advanced Persistent Threat ("APT") cyberattack targeting the legal system and those who operate within it. Defendants are sophisticated threat actors who have spent years infiltrating court networks, e-filing portals, law firm systems, and related digital infrastructure in order to sabotage active court proceedings and undermine the administration of justice. Their tactics include hijacking official court communications, manipulating electronic filings, and even threatening physical harm to coerce and intimidate Plaintiff. The ongoing attack presents an extraordinary convergence of cybercrime and the subversion of judicial processes, warranting immediate relief.

1. Defendants' Organized Enterprise: Upon information and belief, Defendants comprise a coordinated hacking enterprise virtually indistinguishable from the notorious TrickBot/Conti ransomware group and related cybercrime operations. Forensic investigations

have determined that the same infrastructure and malicious tools used by those groups (e.g. cracked Cobalt Strike malware) are being deployed here. Defendants operate in concert as a single illicit enterprise, employing tactics akin to state-sponsored espionage units and organized ransomware gangs. All Defendants acted as agents or co-conspirators of one another, such that each action alleged herein was authorized or ratified by the others in furtherance of the enterprise.

2. Continuing Threat and Injury: From at least 2019 through the present, Defendants have orchestrated a multi-layered hacking campaign infiltrating numerous layers of the legal system's digital infrastructure. They have hijacked court and law firm networks, stolen confidential information, manipulated court filings, and even threatened violence – all to sabotage Plaintiff's legal practice and court cases. Defendants' campaign has effectively built a shadow IT system on top of the justice system, wherein the attackers secretly control the flow of information between attorneys, courts, and clients to rig case outcomes in their favor. Their actions have caused catastrophic harm to Plaintiff's practice, reputation, and personal well-being, as detailed below, and continue to pose an imminent threat of irreparable injury.

3. Overlap with Prior Cases – Need for Coordinated Relief: The same core group of hackers targeting Plaintiff was previously the subject of successful federal enforcement actions by technology companies. In prior cases, Microsoft and Google obtained injunctions against John Doe hackers deploying similar cracked Cobalt Strike malware and expansive "command-and-control" ("C2") server networks. Plaintiff's investigators have now mapped specific servers, IP addresses, and malware from those prior cases directly to intrusions in Plaintiff's systems. There is substantial overlap between Defendants' infrastructure and the infrastructure already enjoined in those big-tech cases. In effect, Defendants have re-tooled parts of the

previously disrupted hacker networks and redeployed them against new targets like Farrow. Given this overlap, Plaintiff seeks coordinated relief harmonized with the remedies in Microsoft Corp. v. John Does 1-16 (E.D.N.Y.) and related cases. In particular, Plaintiff requests declaratory and injunctive relief to recognize that the Final Judgment entered in Microsoft v. Does on September 8, 2025 binds these Defendants, who are one and the same or in active concert with the enjoined parties. Such relief is necessary to immediately neutralize Defendants' infrastructure and prevent further abuse of the courts.

4. Plaintiff: Jay Lewis Farrow is an individual residing in the State of Florida and an attorney in good standing, licensed in New York and Florida for over 20 years. Farrow maintains a law practice serving clients in New York (among other jurisdictions) and regularly uses New York-based courts and computer systems in furtherance of his practice. At all relevant times, Farrow's law firm computers, email accounts, and cloud storage systems contained confidential client information and were used in interstate commerce and communication. Plaintiff brings this action to seek redress for the severe harm Defendants have caused to his business, clients, and personal life.

5. Defendants: John Does 1–20 are unknown persons and entities who perpetrated the unlawful acts described in this Complaint. Their true names and locations are currently unknown to Plaintiff. Upon information and belief, the Doe Defendants acted as a unified group engaged in a sophisticated cybercrime campaign targeting Plaintiff and others in the legal community. The Doe Defendants are being sued under fictitious names until their true identities can be ascertained in discovery.

6. For purposes of this Complaint, all allegations against "Defendants" encompass acts by each of the Doe Defendants, and each Defendant is jointly and severally liable for the

acts of the others as co-conspirators and agents of the enterprise. Each Defendant benefited from and/or directed the conduct of the others such that all were knowing participants in the common scheme.

7. Agency and Concert of Action: At all relevant times, each of the Defendants was acting in concert with, and as an agent or co-conspirator of, the other Defendants with respect to the actions, omissions, and offenses alleged herein. Each Defendant performed acts in furtherance of the enterprise and ratified the illegal conduct of the others, such that Defendants are legally responsible for each other's actions. The Defendants' coordinated campaign was characterized by a singular malicious purpose and a high degree of planning and cooperation, as further detailed below.

8. Subject Matter Jurisdiction: This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under federal statutes, including the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), and the All Writs Act (28 U.S.C. § 1651).

9. The Court also has jurisdiction under 18 U.S.C. § 1964(c) (civil RICO) and supplemental jurisdiction over the related state-law claims (e.g. the Florida RICO count) under 28 U.S.C. § 1367, because those claims form part of the same case or controversy.

10. Personal Jurisdiction: Defendants are subject to personal jurisdiction in New York and in this District because they purposefully directed their activities toward New York and caused injury to Plaintiff in New York. A substantial portion of the wrongful acts alleged herein occurred in or were targeted at New York. For example, forensic evidence shows that the same malicious C2 servers used by Defendants to communicate with Plaintiff's infected devices

overlapped with servers located in New York and even within the Eastern District of New York. Microsoft's investigators identified and mapped many of Defendants' command-and-control IP addresses to physical locations in this District (Coy Dec. 2023, ¶39). By using New York-based infrastructure and impacting court proceedings in New York (including federal cases in this District), Defendants have availed themselves of the laws and protections of New York such that exercising jurisdiction is proper. Moreover, the enterprise's conduct affected interstate commerce and U.S. judicial networks on a national scale, including critical systems based in New York, which further supports jurisdiction.

11. Venue: Venue is proper in the Eastern District of New York pursuant to 28 U.S.C. § 1391(b) and (c). A substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Defendants made use of instrumentalities located in this District (including New York-based servers, domain registries, and networks) to carry out the acts alleged herein.

12. The harms inflicted on Plaintiff – such as interference with court cases and electronic communications – were also felt in this District, where Plaintiff practices law and litigated matters that Defendants targeted. In addition, Defendants' prior and ongoing use of New York infrastructure (e.g., data centers and hosting services in Brooklyn/EDNY) was integral to their scheme, making this District a locus of their racketeering activity.

13. APT Targeting the Legal Industry: Plaintiff Farrow is one of many victims of a years-long, highly sophisticated cyber-attack campaign targeting the legal industry. From at least 2019 to 2025, the John Doe Defendants orchestrated a multi-layered hacking operation that infiltrated numerous components of the legal system's digital infrastructure. The campaign represents a paradigm shift in cybercrime – an amalgam of traditional hacking and direct

subversion of justice. Rather than merely stealing data for profit, Defendants weaponize their access to court processes and attorney communications to corrupt legal proceedings from within. Defendants' operation has been described by experts as "strategic cAPTure-and-kill," whereby the attackers capture control of the digital channels that courts and lawyers rely on, and then "kill" or sabotage the victim's case through unseen manipulation (CNF Rpt., p. 182; CNF Dec., ¶X).

14. Notorious Affiliation – TrickBot/Conti Lineage: The responsible threat actors are virtually and "digitally indistinguishable" from those behind the infamous TrickBot, Conti, and LockBit cybercrime groups. Indeed, forensic analysis indicates that the same group or a closely affiliated group is behind the attacks on Farrow.

15. This group is known for blending techniques of state-sponsored espionage with high-stakes ransomware extortion. Defendants have utilized cracked versions of Cobalt Strike (a red-team software often abused by ransomware actors) as a core tool in their attack, consistent with the modus operandi of Conti and LockBit operators. As Microsoft's cybercrime experts have observed, cracked Cobalt Strike has become a go-to platform for malware operators to persist in victims' machines, and Conti and LockBit are prime examples of ransomware families leveraging that tool (Finones Dec. 2023, ¶27).

16. In short, the Defendants in this case are part of an illicit hacking enterprise whose tactics mirror – and indeed overlap with – those used by some of the world's most notorious cybercriminal syndicates i.e. the Cracked Cobalt, Conti/Spiderwizard Group.

17. Persistent Infiltration of Plaintiff's Systems: Defendants executed an "advanced persistent threat" intrusion into Plaintiff's professional and personal digital life, maintaining stealthy, continuous access for several years. They first infiltrated Plaintiff's law firm network

no later than 2019, and despite Plaintiff's efforts at remediation, they repeatedly re-established footholds.

18. From mid-2024 through 2025, Plaintiff had to replace multiple computers that had been compromised; yet Defendants managed to infect even the newly purchased devices within days or even hours. In one instance, after Plaintiff acquired a brand-new computer, the attackers obtained information about the device (including its Microsoft 365 setup credentials and serial number) by intercepting an email containing the purchase details. Defendants then remotely penetrated the new machine during its initial setup and locked it with their own password as soon as the operating system was installed, effectively bricking the device. This extraordinary event – compromising a fresh, out-of-the-box PC in real-time – exemplifies the threat actors' speed, reach, and boldness.

19. Scope of Compromise and Data Theft: The compromise extended to essentially all of Plaintiff's digital assets. In early 2025, Plaintiff even tried using an older, previously offline laptop (a refurbished Lenovo ThinkPad) at his office, only to have that machine compromised within weeks as well. Forensic investigators ultimately catalogued nearly 400 distinct endpoint intrusions traceable to Defendants between 2019 and mid-2025.

20. By way of example, on June 12, 2024, over 3,600 files on Plaintiff's law firm network were exfiltrated, modified, or destroyed by Defendants within a four-minute window around midnight. Defendants repeatedly gained unauthorized access to Plaintiff's email accounts, cloud storage, and case management systems, siphoning privileged client information and sensitive data.

21. These incursions were ongoing and continuous, persisting even after portions of Defendants' infrastructure were exposed or taken down by third parties. The result was a

wholesale compromise of Plaintiff's practice: confidential client files were pilfered or corrupted, work product was destroyed, and adversaries had visibility into Plaintiff's legal strategies in real time.

22. Goal: Sabotage of Legal Proceedings: Defendants' multifaceted objectives coalesced into a singular overarching purpose – to undermine Plaintiff's legal matters and tip the scales of justice in the enterprise's favor. While part of the operation involved classic cybercrime (e.g. espionage on client files, identity theft, and periodic ransomware deployment threats), the distinctive feature of this APT is its focus on controlling and counterfeiting judicial procedures.

23. Defendants leveraged their illicit access not just to steal, but to manipulate litigation proceedings that Plaintiff was involved in, both as an attorney for clients and as a litigant himself. In essence, the hackers built a parallel shadow network atop the legitimate judicial system – intercepting and altering communications and filings to engineer outcomes they desired.

24. By infiltrating computers, email accounts, domain registrars, and court filing systems, Defendants could secretly steer the course of lawsuits, effectively depriving Plaintiff and his clients of their right to a fair legal process. All the while, the public facade of court proceedings appeared normal; the distortion was behind the scenes, where Defendants pulled the strings.

25. Harassment, Intimidation, and Threats: Defendants did not stop at technical subterfuge; they also engaged in direct harassment and extortion against Plaintiff to further their scheme. Beginning in 2024, Plaintiff and his family began receiving chilling threats clearly emanating from the hackers. For example, on June 3, 2024, just days after Plaintiff filed

an amended complaint in a case against a large insurance company, Farrow received an alarming phone call and text message from an unknown actor.

26. The message included a photograph of Plaintiff in the hospital holding his newborn son – a photo that had never been shared publicly or with Plaintiff (it was taken by a nurse and not distributed).

27. This demonstrated that Defendants had penetrated deeply into Plaintiff's personal life. Thereafter, Defendants periodically threatened Plaintiff's family, with particular focus on his young child.

28. On July 11, 2025, Plaintiff received a credible death threat against his now three-year-old child – almost exactly one year after the hackers had first menaced that same child when he was only 22 months old. These unlawful threats (targeting an attorney's family to influence his actions) constitute criminal extortion under state and federal law.

29. They underscore the malicious intent behind Defendants' actions and have caused Plaintiff and his family extreme emotional trauma and fear for their safety.

30. Overlaps with Prior Cybercrime Cases: Farrow's forensic investigation uncovered extensive overlaps between the infrastructure used against him and the infrastructure identified in prior federal cybercrime cases from 2018–2025.

31. For instance, many of the same Internet domain names and IP addresses that appear in Plaintiff's network logs and malware configuration files also appeared in court filings and evidence from those earlier cases. This strongly suggests that the same organized threat actors behind those cases are involved here, or at least that Defendants are reusing the exact same malicious infrastructure that was previously attributed to groups like Conti/TrickBot. In fact, Microsoft's Digital Crimes Unit ("DCU") investigators in 2023 identified numerous malicious

IP addresses and domains used by Conti/LockBit ransomware operators, some of which were traced to servers in New York.

32. Significantly, many of those very IP addresses later showed up communicating with Plaintiff's own systems. Microsoft DCU expert Christopher Coy mapped Defendants' C2 infrastructure and confirmed it spanned across various locations, including multiple nodes within this District.

33. These findings confirm that Defendants are part of the same threat ecosystem previously targeted by Microsoft and others, and that they have simply shifted their resources to new victims. Plaintiff has incorporated into this Complaint the expert declarations and reports from those prior actions – including the March 30, 2023 Declarations of Microsoft DCU investigators Christopher Coy and Rodel Finones, the December 5, 2024 Marlin Forensics Report, and the October 22, 2025 Cyber-N.E.T. Forensics ("CNF") Expert Report – all of which corroborate the technical underpinnings of Defendants' scheme. The convergence of evidence from these sources paints a consistent picture of a single cybercrime enterprise orchestrating all of these attacks.

34. Command of Court Communications: The John Doe Defendants have demonstrated an unprecedented ability to assume control over the communication channels that attorneys and courts rely upon. According to the CNF forensic analysis, from 2019 through 2025 Defendants executed a "multi-layered attack" that wove together DNS hijacking, cloud proxying, and email interception to achieve near-total control over their targets' digital communications.

35. In practical terms, Defendants positioned themselves in the middle of virtually every electronic interaction involving Plaintiff's practice – without detection. They effectively

built a "shadow command-and-control structure over the victims' own infrastructure," enabling them to step in at will to surveil, disrupt, or falsify digital communications.

36. With this clandestine leverage, the hackers could monitor Plaintiff's emails, intercept or alter court filings and notices, and even impersonate Plaintiff or other attorneys in official communications. As described below, Defendants' techniques allowed them to dictate the flow of litigation from the shadows.

37. DNS Hijacking of Legal Infrastructure: A cornerstone of Defendants' operation was the hijacking of Domain Name System (DNS) records for key websites and servers in the legal system. By illicitly altering the authoritative DNS entries for law firm domains, court portals, and even state Bar websites, Defendants were able to redirect internet traffic for those services into their own control.

38. For example, on or about September 19, 2024, a cluster of Florida court-related domains – including the official statewide e-filing portal myflcourtaccess.com – suddenly had their registrar and name server information switched in unison. Within days of these DNS changes, an unusual spike of unauthorized filing activity occurred on the e-filing portal, indicating that the attackers were funneling the portal's traffic through their own systems at precisely the moment they initiated fraudulent filings. As the CNF Report notes, such a flurry of coordinated DNS changes at critical moments is "not housekeeping…that is orchestrated control," meaning it was a deliberate act by the adversary rather than any benign maintenance.

39. By effectively "moving the front door" of important services to servers they operated, Defendants ensured that all communications to those services (web or email) would pass through the adversary first. This DNS manipulation tactic is identified in the MITRE ATT&CK framework as Technique T1565.002 (DNS Redirect) (MITRE Rpt., p. 100),

essentially giving Defendants the "keys to the internet's address book" for the affected domains. Armed with that control, the attackers could intercept or alter information at will under the guise of the legitimate domain.

40. TLS/SSL Abuse via Cloud Proxying ("Cloud Fronting"): To avoid tipping off users while hijacking DNS, Defendants leveraged trusted cloud infrastructure to proxy their malicious traffic. In practice, after rerouting a target domain to an attacker-controlled server, Defendants would channel the traffic through reputable content delivery networks (CDNs) or cloud services (such as Amazon Web Services CloudFront) to mask the deception.

41. This technique, known as "cloud fronting," allowed the fake sites to appear virtually identical to the real ones. For instance, on August 5, 2025, the official website of the Florida Supreme Court (flcourts.gov) was briefly redirected to an AWS CloudFront address controlled by Defendants.

42. During that window, any user visiting the court's site or transmitting data believed they were interacting with a secure government website, when in reality their connection was being transparently proxied through the attackers' system.

43. Because Defendants also obtained or generated valid TLS/SSL certificates for the hijacked domains (for example, by using automated services like Let's Encrypt shortly after registering spoofed domains), the browser would still show the trusted padlock icon and "https://" prefix.

44. By "keeping the padlock green," Defendants maintained a facade of legitimacy – everything looked authentic and encrypted – even as they subtly altered or monitored the content behind the scenes. A Microsoft expert described this tactic as "preserving the padlock

while controlling content," meaning the attackers ensure all outward signs of security are present while they manipulate the substance of communications. T

45. Through such cloud proxying tradecraft (akin to MITRE ATT&CK Technique T1090, "Proxy: Cloud"), the hackers could conduct a silent man-in-the-middle attack on critical web services without immediate detection. Even vigilant users or security tools were not alarmed, since the network traffic appeared to be going to legitimate cloud endpoints over encrypted channels. In sum, Defendants "kept the front door locked (secure), but had the key," enabling them to surreptitiously puppeteer the interactions between lawyers, courts, and clients.

46. Email Relay Interception: Defendants treated the email ecosystem of the legal community as a prime target for surveillance and manipulation. By timing their DNS hijacks to coincide with modifications of email MX records (which direct mail routing) and setting up shadow SMTP relay servers, the attackers could invisibly intercept, delay, or suppress email communications between Plaintiff, his clients, and the courts.

47. Unlike a crude phishing attack, this method did not require sending fake emails. Instead, genuine emails were silently rerouted through malicious mail gateways under Defendants' control. Beginning in 2024, Florida court and Bar email systems began exhibiting odd behavior: emails sporadically failed DKIM authentication or showed slight anomalies in their headers, suggesting that legitimate messages were being relayed through non-standard servers (i.e. intercepted and re-sent by the attackers). In one forensic example, investigators discovered a subtle fingerprint of tampering: certain email headers had the domain "IPHmx.com" capitalized oddly (as "IPHmx.com" instead of lowercase), indicating a manual

edit during relay – essentially a telltale sign that an email had passed through an unauthorized intermediary.

48. By seizing such control of the legal sector's "mailroom," Defendants gained the power to make critical notifications vanish or arrive too late, all while both the sender and recipient remained oblivious that anything was amiss. For instance, Defendants could quietly remove Plaintiff's email address (or add their own) on e-service lists for a case, thus diverting court filings to themselves and leaving Plaintiff uninformed. Plaintiff and others noticed periods where expected court emails (e.g. filing receipts, scheduling notices) never arrived, or came only after unusual delay – occurrences now understood to be the result of Defendants' mail interception scheme.

49. As Google's cybercrime expert Shane Huntley observed regarding this group, they have the capability to "invisibly proxy email threads, with malicious SMTP nodes inserted between correspondents", and the evidence here strongly corroborates that statement. In effect, Defendants owned the communications pipeline, granting them free rein to manipulate the flow of information in litigation.

50. Impersonation and Insertion into Court Systems: Taking their interference a step further, Defendants actively impersonated attorneys (including Farrow) and insinuated themselves into official court e-filing systems to directly influence case dockets.

51. The investigation revealed that the hackers at times forged electronic filings and emails while posing as Plaintiff or other lawyers, even going so far as to create fake lawyer accounts in e-filing portals. In multiple Florida cases, filings were submitted by persons using real attorneys' names and bar numbers without authorization – essentially a digital identity theft of lawyers.

52. The affected attorneys later provided sworn statements that they had never filed those documents and had no idea their identities were being misused. By infiltrating the Florida Courts E-Filing Portal (and analogous systems), Defendants were able to intercept court notices or alter filings in transit. Logs from the statewide portal show suspicious logins to Plaintiff's own e-filing account from unknown IP addresses (e.g., a login on June 25, 2025 that did not originate from Plaintiff). With such access, the attackers effectively had the ability to manipulate court filings in transit – in practice, they could intercept a filing or order before it reached its destination, modify or suppress it, and then pass along a doctored version (or none at all).

53. As one report summarized, the threat actors could "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 [sees]," thereby dictating the progress of litigation unbeknownst to the victims (CNF Rpt., p. 153). This is precisely what happened to Plaintiff: in at least one instance, Defendants filed a pleading with a court impersonating Plaintiff's firm (without Plaintiff's knowledge or consent) with the intent to derail that case.

54. In another, Defendants secretly inserted their own email addresses as e-service recipients on Plaintiff's case, while blocking Plaintiff's address, so that Defendants received all notices and Plaintiff received none.

55. Through these methods, the hackers were able to rig case schedules (e.g. by ensuring Plaintiff missed hearings or deadlines he was never informed of), and plant fraudulent documents to prejudice Plaintiff's position. This conduct amounts to a direct attack on the judicial process. It also demonstrates Defendants' deep understanding of court procedures –

they knew exactly how to exploit procedural rules and electronic systems to cause maximum chaos while avoiding detection.

56. Case Study – "Capture-and-Kill" of Plaintiff's Federal Case: The most striking example of Defendants' influence over court proceedings was their apparent sabotage of a sealed federal lawsuit Plaintiff attempted to file in August 2025.

57. On August 22, 2025, Plaintiff Farrow (through counsel) initiated a confidential case in federal court aimed at exposing and halting Defendants' activities. What transpired next was a series of highly irregular events that strongly indicate Defendants interfered to swiftly terminate the case before it could gain traction.

58. Specifically: (a) Despite being filed as a new civil action, the case was inexplicably assigned only to a magistrate judge immediately upon filing, rather than receiving a district judge as is standard. This anomaly suggested someone may have manipulated the case metadata (e.g. mislabeling it to force a lower-level assignment), likely to keep the matter off the radar and vulnerable to quick dismissal. (b) No notice of a filing fee deficiency was ever sent to Plaintiff, even though the docket indicated no fee was recorded (Plaintiff's payment apparently did not register).

59. Ordinarily, the Clerk's office promptly issues a deficiency notice if a fee is missing, but here there was silence – a red flag that communications were suppressed. (c) Within 24 hours of filing, the case was summarily dismissed by a one-page order, citing non-payment of the fee, and the magistrate also denied Plaintiff's motion for reconsideration almost immediately thereafter.

60. The speed of this dismissal was extraordinary – less than a day – and was carried out without any of the usual grace period or opportunity for Plaintiff to cure the fee issue. (d)

Critically, Plaintiff never received ECF email notices for the key events (the magistrate's order or the dismissal); he learned of the dismissal only after manually checking the docket.

61. The lack of ECF service to Plaintiff, combined with the rest of the anomalies, underscores that the adversary was likely "operating in the middle" of the court's communication flow and possibly manipulating docket entries. CNF's experts concluded that these events were no coincidence but rather the result of a deliberate, covert intervention by Defendants – essentially a textbook "capture-and-kill" operation against Plaintiff's lawsuit.

62. By capturing control of the case assignment and notifications (through their prior compromises of court systems and email), the attackers "killed" the case at inception via procedural trickery. Notably, the dismissal order was issued without apparent awareness that Plaintiff had in fact paid the fee shortly after filing (using a backup method) and that the case was under seal; this suggests the court was acting on false/incomplete information, which could be attributed to Defendants' tampering with court records or intercepting communications.

63. In the aftermath, CNF analysts mapped each irregularity to known tactics of the adversary: e.g., blocking filings or payment records to induce dismissal corresponds to their demonstrated ability to truncate or delay e-portal submissions; suppressing notices maps to their man-in-the-middle email interception; fast-tracking a dismissal aligns with their goal of cutting off any legal challenge before it exposes them.

64. Indeed, this pattern mirrored past incidents in Florida where lawsuits mysteriously terminated after imposter attorneys appeared – cases later suspected to have been sabotaged by the same threat group. In short, Defendants succeeded in weaponizing the federal court's own procedures against Plaintiff, achieving in days what their cyber intrusions alone could not: the outright dismissal of a case aimed at bringing them to justice.

65. This egregious interference with the judicial function highlights the urgent need for extraordinary relief in the present action.

66. Nationwide Impact – New York Included: While many specific examples above reference Florida (where Plaintiff's practice was centered during much of the attack), Defendants' templated APT has affected the legal system nationally, including in New York. Over forty law firms of various sizes – including some of the oldest and most reputable firms in the United States, with offices across multiple states – have been targeted as part of this enterprise.

67. Evidence indicates that federal and state court systems in jurisdictions beyond Florida have been probed or compromised by the same group. In early 2021, the Administrative Office of U.S. Courts publicly acknowledged an "apparent compromise" of the federal judiciary's CM/ECF electronic filing system, noting that sealed filings had been viewed by unauthorized actors.

68. The pattern of that breach (later linked by experts to the TrickBot/Conti constellation) presaged what happened to Plaintiff. Indeed, Defendants' interference with Plaintiff's own federal cases (through hijacking PACER/CM/ECF portals and email notices) directly impacted proceedings in New York-based courts as well. The same core group of hackers is thus responsible for "penetrat[ing] the electronic backbone of the U.S. court system" across multiple jurisdictions.

69. By exploiting vulnerabilities in electronic filing and communication systems, they have shown the ability to reach into any courtroom in the country – New York included – from behind a keyboard. This lawsuit, filed in New York, reflects not only Plaintiff's personal stake

but the broader public interest in protecting the integrity of our courts from such cyber-subversion.

70. Harm to Plaintiff: The damage Defendants have inflicted upon Plaintiff Farrow is severe, ongoing, and irreparable. Professionally, Plaintiff's law practice has been thrown into chaos.

71. By infiltrating Farrow's computers, email, and files, Defendants effectively compromised his ability to practice law and represent clients. They caused the loss or corruption of critical client data and legal work product, and on multiple occasions blocked Plaintiff's access to important accounts or systems at pivotal times. Plaintiff has been forced to expend enormous time and money to investigate the breaches, consult cybersecurity experts, replace hardware, and implement new security measures – costs that well exceed $100,000 (far above the $5,000 threshold under the CFAA) in out-of-pocket expenses alone.

72. This figure does not include the hundreds of hours of lost billable time and opportunity cost spent remediating the damage.

73. Beyond direct monetary loss, Defendants' actions have gravely damaged Plaintiff's reputation and client relationships.

74. By sabotaging court communications and filings, the hackers made it appear as though Plaintiff was missing deadlines or neglecting cases (when in fact he had been kept unaware of proceedings).

75. Some of Plaintiff's clients, not understanding the true cause of these irregularities, lost trust and terminated his representation. Prospective clients were similarly deterred by the confusion and adverse outcomes engineered by the attackers.

76. These losses of goodwill, client confidence, and professional standing cannot be easily quantified and constitute irreparable harm to Plaintiff's career. Personally, Plaintiff and his family have suffered extreme emotional distress and loss of any sense of security.

77. The constant surveillance by Defendants – who read privileged attorney-client emails and even intimate family communications – is a profound invasion of privacy. The explicit threats to Plaintiff's child and spouse have caused severe anguish, requiring involvement of law enforcement and significant personal protective measures.

78. Plaintiff has had to live and work under siege, not knowing which parts of his digital life are actually under his control or being manipulated by unseen hands. In sum, Defendants' unlawful acts have damaged Plaintiff in his "business or property" and caused mental suffering, meeting the injury requirements of the causes of action below. Moreover, absent immediate intervention by this Court, Plaintiff's injuries will continue to compound, and other victims will likewise remain at grave risk.

Count I – Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030)

79. Plaintiff re-alleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 78 above.

80. Protected Computers: The computers and electronic devices that Defendants targeted and accessed – including Plaintiff's law firm PCs, servers, and cloud-based accounts – are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2)(B) because they are used in interstate commerce or communication. Plaintiff's devices and email/cloud accounts are part of networks that facilitate interstate communications (e.g. email servers, cloud storage) and are used to conduct legal business across state lines, including in New York and Florida.

81. Unauthorized Access and Exceeding Authorization: Defendants, without authorization, knowingly accessed Plaintiff's protected computers and online accounts. They did so by illicit means including installing malware (such as Cobalt Strike beacon payloads), using stolen credentials, and exploiting security vulnerabilities.

82. At no time did Plaintiff or any authorized party give Defendants permission to access these systems. To the extent Defendants leveraged any valid login credentials (e.g. stolen passwords or session cookies), their use was wholly without authorization or exceeded any authorized access by circumventing security measures.

83. For example, Defendants accessed Plaintiff's email accounts by rerouting DNS/MX records and logging into the mail server as if they were the legitimate user, which far exceeds any authorized use.

84. Intent and Fraud: Defendants acted with the intent to defraud and extort. By accessing Plaintiff's computers, they intended to further a fraudulent scheme – namely, to steal information and sabotage Plaintiff's legal matters to their own advantage.

85. They obtained valuable data (client information, case strategies, etc.) via these intrusions and used it to procure something of value for themselves and/or others (e.g. an advantage in litigation, avoidance of legal liability, or monetary gain through extortion).

86. Additionally, through threats and extortionate communications, Defendants attempted to coerce Plaintiff into refraining from exposing their scheme (e.g. implied threats if he pursued legal action). All such conduct was fraudulent and for the purpose of achieving unlawful ends.

87. CFAA Violations (Access, Damage, and Loss): Defendants' actions violated multiple subsections of 18 U.S.C. § 1030. Without limitation, Defendants: (a) obtained

information from protected computers in a financial or consumer context by intentionally accessing those computers without authorization, in violation of § 1030(a)(2)(C); (b) knowingly caused the transmission of programs or code (malware) to Plaintiff's computers, and as a result intentionally caused damage without authorization, in violation of § 1030(a)(5)(A); and (c) intentionally accessed protected computers without authorization and caused damage and loss, in violation of § 1030(a)(5)(C).

88. The term "damage" under the CFAA includes any impairment to the integrity or availability of data, programs, systems, or information – here, Defendants caused widespread data corruption, deletion, and encryption of Plaintiff's files (for example, the June 12, 2024 incident where thousands of files were damaged in minutes), as well as denial of access to Plaintiff's accounts and devices (e.g. the computer locked with an unknown password).

89. The term "loss" includes the cost of responding to the offense, conducting damage assessments, restoring data/systems, and lost revenue or other consequential damages. Plaintiff has incurred well over $100,000 in losses responding to and investigating Defendants' intrusions and mitigating their effects.

90. This far exceeds the $5,000 statutory threshold in a one-year period (indeed, Plaintiff's losses in 2024-2025 run into the six figures). Moreover, Defendants' acts caused a loss of at least that amount to one or more persons during any one-year period, given the harm to Plaintiff's clients and potentially other attorneys whose data was impacted as part of the same campaign.

91. Aggravated Offenses: Further, Defendants' conduct affected computers used by or for governmental entities and the administration of justice. By infiltrating court e-filing systems and clerk communications, Defendants effectively trespassed into government

computer infrastructure (court servers, etc.) as part of their scheme. This heightens the seriousness of the offense (see 18 U.S.C. § 1030(a)(3) and (c)(4)(A)(i)(III)). Defendants also recklessly caused damage and at least attempted to cause damage to systems used for justice administration, which could be considered under § 1030(a)(5)(B).

92. Damages and Relief: As a direct and proximate result of Defendants' CFAA violations, Plaintiff has suffered damages and loss as described. Plaintiff's business has been disrupted, data has been destroyed or rendered unusable, and significant costs have been incurred to diagnose and remediate the attacks.

93. Under 18 U.S.C. § 1030(g), Plaintiff is entitled to maintain a civil action against Defendants to obtain compensatory damages and injunctive relief or other equitable relief. Here, Plaintiff seeks injunctive relief (as further detailed in the Prayer for Relief) to prevent ongoing and future unauthorized access and to compel Defendants (and relevant third parties) to cease and remediate the harm. Plaintiff also seeks damages in an amount to be proven at trial, including without limitation the value of stolen data and the costs of remedial measures, to the extent such damages are available under the CFAA.

Count II – Violation of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 et seq. and § 2510 et seq.

94. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 78 as if fully set forth herein.

95. Unauthorized Access to Stored Communications (Stored Communications Act, 18 U.S.C. § 2701): Defendants, by the acts described, violated Title II of the ECPA (the Stored Communications Act, "SCA").

96. They intentionally accessed without authorization (or exceeded authorized access to) facilities through which electronic communications services are provided, namely email

servers and cloud storage systems, and thereby obtained, altered, or prevented authorized access to electronic communications while in electronic storage.

97. Specifically, Defendants broke into Plaintiff's email accounts (including cloud-based Microsoft 365 email and other accounts) by covertly rerouting DNS/MX and using stolen credentials, thereby accessing the content of email messages stored on those servers. They also accessed Plaintiff's cloud data (documents, files, and backups) maintained by service providers, without authority, via similar means.

98. In doing so, Defendants obtained and removed emails and attachments that were in storage on those systems (for example, grabbing copies of court e-service emails and client communications stored in mailboxes). They also prevented Plaintiff from accessing certain communications (e.g. by deleting or moving messages on the server, or by altering password reset links to lock Plaintiff out).

99. Such conduct violates 18 U.S.C. § 2701(a). No statutory exceptions apply; for instance, Defendants were not service providers or authorized users of the accounts. Plaintiff and his law firm were the exclusive authorized users, and they never gave permission for Defendants' intrusions.

100. Interception of Communications (Wiretap Act, 18 U.S.C. § 2511): Defendants further violated Title I of the ECPA (the Wiretap Act) by intentionally intercepting electronic communications in transit.

101. Through their DNS hijacking and "man-in-the-middle" email relay scheme, Defendants intercepted the contents of emails and electronic documents as they were being transmitted between Plaintiff, clients, courts, and others. For example, when Plaintiff's court notification emails were redirected to Defendants' shadow SMTP server, the Defendants

acquired those communications contemporaneously with their transmission, before they reached Plaintiff.

102. Likewise, Defendants' proxying of web traffic (including e-filing submissions) allowed them to intercept data packets in real time as attorneys and court systems exchanged them. None of the parties to those communications consented to such interception. The Wiretap Act forbids intentionally intercepting any wire or electronic communication without consent (18 U.S.C. § 2511(1)(a)), as well as using or disclosing the contents of any such unlawfully intercepted communication (18 U.S.C. § 2511(1)(c)–(d)). Defendants did all of the above.

103. They not only intercepted emails and web submissions, but also used the knowledge gained (e.g. contents of sealed filings, scheduling info, etc.) to further their illegal ends and even disclosed some of it to third parties (for instance, sharing Plaintiff's confidential information with his litigation adversaries or using it to extort him). Each interception was deliberate, without justification, and in violation of the ECPA.

104. Pattern and Timing: Defendants' ECPA violations were not isolated incidents but a systematic pattern. The forensic record shows that during key legal events – such as when motions were filed or hearings scheduled – Plaintiff's email and filing communications would mysteriously misroute or fail authentication.

105. This corresponds to Defendants timing their interception infrastructure to peak when valuable communications could be captured. By operating their own rogue DNS and mail servers and leveraging cloud proxies, Defendants essentially tapped into the communication lines of the legal system at will, without detection.

106. Damages and Relief: As a direct and proximate result of Defendants' ECPA violations, Plaintiff has suffered damages including but not limited to the loss of privacy, compromise of privileged and confidential information, disruption of legal matters, and emotional distress.

107. The ECPA (both Title I and II) provides for a civil cause of action (18 U.S.C. § 2520 for interceptions, and 18 U.S.C. § 2707 for stored communications), allowing for declaratory and equitable relief, damages, and reasonable attorney's fees. Plaintiff seeks declaratory relief that Defendants' conduct violated the ECPA, an injunction restraining Defendants from any further interception or unauthorized access of electronic communications, and an order requiring Defendants to surrender or destroy any and all information obtained through their unlawful access.

108. Plaintiff also seeks statutory damages and/or actual damages to be proven, including profits made by Defendants from these violations (if any) or $100 per day of violation (or $10,000), whichever is greater, for each Defendant, as provided under 18 U.S.C. § 2520(c). Given the egregiousness of Defendants' conduct – intercepting officers of the court and sabotaging legal proceedings – Plaintiff further requests the maximum allowed punitive or enhanced damages to deter such conduct, to the extent permitted by law.

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

109. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 78 above as if fully set forth herein.

110. RICO Enterprise: Defendants and their co-conspirators form an association-in-fact enterprise engaged in, and whose activities affect, interstate and foreign commerce, as defined in 18 U.S.C. §§ 1961(4) and 1962(c).

111. This enterprise – referred to herein as the Farrow Attack Enterprise or "the Enterprise" – consists of the network of individuals (John Does 1–20 and others unknown) and entities (shell companies, hacker groups, etc.) that have associated together for the common purpose of carrying out the unlawful scheme described in this Complaint.

112. The Enterprise has an ongoing organization, either formal or informal: it has structure and continuity, evidenced by the multi-year duration of the coordinated cyberattacks, the repeated use of the same infrastructure (malware, servers, domains), and the recurring patterns of tactics to achieve the group's illicit goals.

113. The members of the Enterprise function as a unit, with each participant playing roles such as malware developer, initial access broker, money launderer (for ransomware or extortion proceeds), and "field agent" in charge of manipulating legal processes.

114. The Enterprise is separate and distinct from the Defendants themselves (though the Defendants are members of the Enterprise) – it has its own identity as a continuing unit that transcends the individual capers, coordinating a broad campaign of cybercrime.

115. Conduct/Participation: Each Defendant conducted or participated in the affairs of the Enterprise through a pattern of racketeering activity, in violation of 18 U.S.C. § 1962(c). Defendants willingly joined the Enterprise and actively performed acts to further its illicit objectives.

116. Their participation was necessary and integral – without their contributions (hacking skills, infrastructure, etc.), the Enterprise's scheme could not succeed. For example, one or more Defendants managed the malware and servers that obtained unauthorized access to computers; others orchestrated the intimidation campaign against Plaintiff (phone threats,

etc.); others handled the exfiltration and use of stolen data to derail lawsuits. All Defendants knowingly coordinated with each other (directly or indirectly) with the common purpose of sabotaging legal proceedings for profit or benefit, as described herein.

117. Each Defendant agreed to and did, in fact, conduct the Enterprise's affairs (as opposed to merely pursuing their own individual affairs) through a pattern of racketeering, by acting in furtherance of the overall scheme.

118. Pattern of Racketeering Activity: Defendants' actions constitute a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(1) and (5). The pattern includes multiple acts indictable under specified provisions of Title 18 of the United States Code, as well as under state laws, all related to each other and continuous.

119. The racketeering acts ("predicates") committed by Defendants include, but are not limited to:

A. Extortion and Threats: Defendants transmitted interstate communications containing threats to injure the person or property of Plaintiff (specifically, threats to harm Plaintiff's child and family) with the intent to extort and to influence Plaintiff's conduct. This is indictable under 18 U.S.C. § 875(c) (interstate threats) and constitutes "extortion" as defined in 18 U.S.C. § 1951 (Hobbs Act) and as criminalized under state law (e.g., Fla. Stat. § 836.05). By threatening Plaintiff's child to coerce Plaintiff's behavior, Defendants engaged in criminal extortion. Extortion is expressly enumerated as racketeering activity under 18 U.S.C. § 1961(1)(A) (incorporating state felonies involving extortion) and § 1961(1)(B) (Hobbs Act extortion). These threats were not isolated: they occurred repeatedly (e.g., in 2024 and again in 2025) showing continuity.

B. Fraud and Identity Theft: Defendants committed wire fraud in violation of 18 U.S.C. § 1343 by devising a scheme to defraud Plaintiff and others (including courts and clients) and to obtain money or property by means of false pretenses, and executing that scheme via interstate wires. For instance, Defendants sent fraudulent electronic communications (such as impersonated emails and filings) to courts and parties, pretending to be Plaintiff or other attorneys, thereby deceiving the recipients and gaining unwarranted advantage in lawsuits. Those acts were in furtherance of depriving Plaintiff and his clients of money (legal fees, favorable outcomes) and tangible property

(confidential data). Additionally, by stealing and using the identities and passwords of real attorneys (including Plaintiff) to file documents, Defendants committed acts indictable under 18 U.S.C. § 1028 (fraud in connection with identification documents) and § 1029 (fraud in connection with access devices). Use of another's Bar credentials and e-filing access to submit unauthorized filings is effectively identity theft and access device fraud. Predicate acts of mail/wire fraud are included in § 1961(1)(B), and acts of identity theft/fraud are within the "fraud" category of state/federal offenses that qualify as racketeering (also potentially as part of an ongoing scheme to defraud multiple victims).

C. Computer Fraud and Abuse (CFAA) Felonies: As detailed in Count I, Defendants accessed protected computers without authorization and furthered fraud and obtained valuable information. Certain of these acts are chargeable as felonies under the CFAA (18 U.S.C. § 1030). For example, accessing a government or financial institution computer, or any computer in furtherance of fraud, that causes loss >$5,000 in a year is a felony (§ 1030(c)(4)(A)). Defendants' actions meet those criteria (losses in tens of thousands, plus affecting government systems). "Fraud in connection with computers" and similar offenses can be considered predicate acts under RICO either as wire fraud, as they involved interstate electronic communications, or as offenses indictable under 18 U.S.C. § 1030 (which are not explicitly listed in § 1961, but the wire fraud and extortion elements of the conduct suffice for predicate listing). Additionally, Defendants transmitted extortionate threats in relation to damaging computers (akin to 18 U.S.C. § 1030(a)(7), which is obtaining something of value by threats to damage a computer). In any event, their hacking facilitated other predicate acts like fraud and identity theft, tying into the pattern.

D. Obstruction of Justice: Defendants' interference with court proceedings may be chargeable as obstruction of justice (18 U.S.C. §§ 1503, 1512) or retaliation against a party/witness (18 U.S.C. § 1513). By sabotaging Plaintiff's lawsuit and tampering with court communications, Defendants endeavored to "influence, obstruct, or impede, the due administration of justice," which is a federal crime (18 U.S.C. § 1503) and also likely a state crime. Such acts can qualify as racketeering if they are indictable under federal law (e.g., § 1512 which covers tampering with a proceeding by corrupt means). The pattern here shows repeated interference in multiple cases (Plaintiff's and others), indicating continuity.

120. These acts are collectively "racketeering activity" under § 1961(1). They have occurred over an extended period (2019–2025) and are not isolated events but rather related

acts with a similar purpose, involving similar methods (cyber intrusions, deception, threats), and directed at multiple victims (Plaintiff, his clients, and the courts). Thus, they constitute a pattern of racketeering activity with both continuity (ongoing, repeated conduct) and relatedness.

121. Injury to Business or Property: Plaintiff has been injured in his business or property by reason of Defendants' racketeering violations. Plaintiff's law practice (a business/legal enterprise) has lost substantial revenue and assets due to Defendants' acts. He lost clients and the associated income (property) as a direct result of Defendants' fraudulent and extortionate interference with his cases. He expended significant funds to replace and repair computer systems because of Defendants' hackings.

122. These are concrete financial losses.

123. Additionally, Plaintiff's property interest in his confidential information was harmed when Defendants stole and exploited that information.

124. The injuries to Plaintiff were directly caused by the pattern of racketeering: for example, the loss of client revenue flows directly from Defendants' scheme to disrupt court communications (wire fraud predicate) and extort Plaintiff (threats predicate) which made him appear unreliable to clients.

125. But for Defendants' racketeering acts, Plaintiff would not have suffered these specific losses. Plaintiff's injuries were the foreseeable and natural consequence of Defendants' scheme (indeed, causing financial harm to Plaintiff was one objective of their enterprise – to punish Plaintiff and deter his exposure of them).

126. Relief Sought (Civil RICO): Pursuant to 18 U.S.C. § 1964(c), Plaintiff is entitled to recover treble damages for his losses, plus the costs of suit and reasonable attorney's

fees. Plaintiff also seeks appropriate equitable relief to prevent and restrain further violations of RICO by Defendants (18 U.S.C. § 1964(a)), including but not limited to orders enjoining Defendants from continuing the above-described activities and imposing restrictions or performance bonds to deter future misconduct.

127. Specifically, Plaintiff seeks injunctive relief directing the dismantling or seizure of the Enterprise's infrastructure (domains, servers, etc.) as allowed by law, and any other relief the Court deems just to mitigate the ongoing threat. The trebling of damages is warranted given the willful and malicious nature of Defendants' conduct. Additionally, Plaintiff's attorney's fees and investigative costs (substantial in attempting to trace and attribute this scheme) should be awarded under § 1964(c).

128. Plaintiff also alleges that to the extent any Defendant is not directly liable under § 1962(c), they are liable for conspiring to violate § 1962(c) under 18 U.S.C. § 1962(d), as all Defendants agreed and conspired with each other to carry out the pattern of racketeering. Each Defendant committed or caused to be committed at least two overt acts of racketeering in furtherance of the conspiracy. Thus, in addition or in the alternative, Plaintiff pleads a RICO conspiracy claim under § 1962(d) against all Defendants, with the same damages as above.

Count IV – Florida RICO (Florida Racketeer Influenced and Corrupt Organization Act, Fla. Stat. § 895.02 et seq.); Injunctive Relief under Fla. Stat. § 895.05(6)

129. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 78 and 110 through 128 above as though fully set forth herein.

130. Florida RICO Enterprise and Pattern: The Defendants' conduct also violates Florida's RICO Act (Fla. Stat. § 895.03). Florida's RICO statute mirrors the federal RICO statute in material respects and prohibits any person employed by or associated with an

enterprise from conducting or participating in the enterprise through a pattern of criminal activity. In this case, the enterprise is the same association-in-fact described in Count III, and it operates in or affecting Florida as well as other states. Defendants, through their unified cybercriminal campaign, engaged in a pattern of criminal activity as defined by Fla. Stat. § 895.02(8).

131. This pattern includes at least two incidents of criminal activity that have the same or similar intents, results, accomplices, victims, or methods of commission, or otherwise are interrelated and not isolated.

132. The predicate "criminal activity" under Florida law includes, among other things, the commission of, attempt to commit, or conspiracy to commit various Florida felonies and certain federal offenses.

133. The Defendants' acts outlined previously qualify as such criminal acts, including: extortion (a Florida first-degree felony under Fla. Stat. § 836.05, and thus a predicate act under Fla. RICO), offenses concerning computer-related crimes (e.g. offenses under Florida's Computer Abuse and Data Recovery Act or other Florida statutes prohibiting unauthorized computer access, which are felonies), theft and fraudulent use of personal identification information (Florida identity theft statutes), and any applicable fraud, obstruction of justice, or retaliatory acts under Florida law.

134. Each Defendant's conduct of infiltrating Florida's court systems, law firms, and Bar (and threatening a Florida resident's family) constitutes violation of multiple Florida criminal statutes.

135. These acts had the same goal – to subvert legal proceedings and harm Plaintiff – and thus are related, and they occurred over a period exceeding two years, establishing continuity.

136. Persons and Enterprise Distinctness: The "persons" (John Does 1–20) are separate from the "enterprise" in that they are individuals (or entities) distinct from the association-in-fact through which they acted. Defendants operated the enterprise's affairs (the overall unlawful scheme), not merely their own personal affairs, by coordinating hacking operations, harassment, and fraudulent filings as part of a larger group effort.

137. Injury in Florida: Plaintiff is a Florida resident and an attorney whose principal law practice was in Florida during much of the relevant time.

138. Farrow and his law practice (a Florida professional enterprise) suffered substantial injury in Florida due to Defendants' actions. Among other things, Defendants' sabotage of Plaintiff's cases in Florida courts and hacking of his Florida-based law firm network directly caused loss of clients and income in Florida, and required expenditures in Florida for remediation.

139. Additionally, the integrity of Florida's judicial system was harmed by Defendants' infiltration (though the State itself is not a plaintiff here, the point underscores the far-reaching impact in Florida). Plaintiff's personal losses, as described, are cognizable under Florida RICO – loss of money and property (client contracts, firm data, etc.) within Florida.

140. Relief under Florida RICO: Under Fla. Stat. § 895.05(6), any person injured by reason of a violation of Fla. Stat. § 895.03 has a cause of action for threefold the actual damages sustained, as well as reasonable attorney's fees and costs.

141. Plaintiff seeks treble damages for the injury to his business and property, in an amount to be determined at trial, but well in excess of the jurisdictional minimum, reflecting the severe financial harm described.

142. Plaintiff also seeks injunctive relief as expressly authorized by § 895.05(6). Given the ongoing nature of Defendants' unlawful enterprise and the threat of continuing irreparable harm, Plaintiff requests that the Court issue appropriate orders to prevent and restrain further violations.

143. This includes, but is not limited to: (a) an injunction prohibiting Defendants from accessing or attempting to access any of Plaintiff's (or his firm's) computers, email accounts, or other electronic systems; (b) an injunction prohibiting Defendants from contacting or threatening Plaintiff or his family; (c) measures to disconnect Defendants from the instrumentalities of their scheme (e.g. disabling domains, servers, and email accounts under their control that were used in the pattern of criminal activity); and (d) any other relief necessary to dismantle the Enterprise's ability to continue operating (such as requiring third-party internet registrars or service providers to take down malicious domains, etc.), pursuant to the Court's equitable powers. Florida's RICO statute explicitly empowers courts to issue equitable relief including restraining orders, divestiture of interests, restrictions on future activities, and dissolution or reorganization of enterprises, as necessary to prevent ongoing violations.

144. Plaintiff seeks the full breadth of such relief to ensure the safety of his practice and the public.

145. Additionally, Plaintiff seeks an award of litigation costs and attorney's fees under Fla. Stat. § 895.05(6), as the Defendants' actions have forced Plaintiff to incur substantial

fees to investigate and pursue this matter. The trebling of damages and fee award are warranted given the willful and malicious nature of the racketeering activity.

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

146. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 78, above, and further incorporates by reference the allegations of the substantive counts (Counts I–IV) to the extent relevant to this claim.

147. Necessity for Ancillary Relief: Plaintiff seeks an injunction and ancillary orders under the All Writs Act, 28 U.S.C. § 1651(a), in order to aid the Court's jurisdiction and to ensure that the relief granted on the substantive causes of action is effective.

148. 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." This includes the power to issue orders directed at third parties who, though not themselves accused of wrongdoing in this case, may be in a position to facilitate or thwart the implementation of the Court's decrees.

149. Third-Party Cooperation to Disable Defendants' Infrastructure: As detailed above, Defendants have persisted in using certain IP addresses, domain names, and online services as part of their attack infrastructure. Many of these resources are operated or hosted by third-party entities – for example, domain name registries (for .com, .net, etc.), domain registrars, cloud hosting providers (like Amazon Web Services, Cloudflare), email service providers, and others.

150. These third parties are not currently before the Court as defendants, yet their action or inaction could significantly influence the efficacy of any injunctive relief. Absent a

court order, these third parties might unwittingly continue to provide services to Defendants' malicious infrastructure, thereby undermining the Court's ability to stop the ongoing harm.

151. Precedent for All Writs Relief: In prior analogous cases, courts have utilized the All Writs Act to enjoin third parties from allowing defendants to evade an injunction. For example, in Microsoft Corp. v. John Does (E.D.N.Y. 2023, Case No. 1:23-cv-02447) – a case targeting a similar hacking enterprise – the court invoked the All Writs Act to direct domain registries and hosting companies to take down or block access to the defendants' malicious domains and IP addresses.

152. Similarly, in Google LLC v. Starovikov, No. 1:21-cv-10260 (S.D.N.Y. 2021), an All Writs order was used to compel third-party infrastructure providers to disable the command-and-control servers of a botnet, ensuring the effectiveness of the TRO and preliminary injunction.

153. These precedents confirm that such relief is both available and appropriate where, as here, a complex international cyber scheme would otherwise be beyond the reach of the Court's direct orders.

154. Writ Necessary in this Case: Here, immediate All Writs Act relief is warranted to prevent Defendants from evading this Court's jurisdiction or rendering any judgment ineffective.

155. The heart of this case is stopping Defendants' illegal cyberattacks and interference with court proceedings.

156. If the Court grants injunctive relief on the CFAA, ECPA, and RICO claims (for instance, ordering Defendants to cease certain activity and relinquish certain infrastructure), that relief could be frustrated unless third parties are compelled to assist.

Defendants have shown extraordinary ability to "shape-shift" their infrastructure – moving to new domains, IPs, or platforms if one is shut down (Coy Dec. 2023, ¶39).

157. Thus, a coordinated shutdown of all known malicious domains and accounts, at the same time, is critical. The Court's jurisdiction to grant complete relief over the controversy would be impaired if Defendants can simply continue their attacks via untouched infrastructure or if they can block Plaintiff's access to this very lawsuit (as they tried before) by abusing electronic filing systems.

158. The All Writs Act allows the Court to close off such escape routes and preserve its ability to resolve the case on the merits.

159. Scope of Requested All Writs Orders: Plaintiff specifically requests that the Court issue orders under the All Writs Act directing certain actions by third parties, including but not limited to:

A. Domain Registries and Registrars: Ordering the registries and/or registrars for any domain names identified in evidence as being used by Defendants (for malicious command-and-control, phishing portals, fake e-filing sites, etc.) to promptly deactivate or transfer those domain names to the control of Plaintiff or a Court-appointed neutral agent, such that Defendants can no longer use them. This may include domains resembling official court sites (myflcourtaccess.com and variants, floridabar[.]org subdomains, etc.) which Defendants have co-opted.
B. Internet Service Providers / Hosting Companies: Ordering any known hosting providers or ISPs that have been providing service to Defendants' IP addresses or servers (as identified in the CNF Report and evidence) to cease hosting those addresses/servers and preserve any related evidence. For example, cloud service operators (AWS, Google Cloud, DigitalOcean, etc.) should be directed to cut off service to the specific instances linked to Defendants' infrastructure, to the extent within their control.
C. Email Service Providers: Directing providers like Google (Gmail), Microsoft, or other email hosts to disable any email accounts under Defendants' control that were used in furtherance of the scheme (such as email addresses used to register fake e-filing accounts or to send threats), and to filter or block any outgoing emails that spoof court addresses as identified in the evidence. Also, instructing them to assist in restoring

Plaintiff's accounts if any forwarding rules or unauthorized access by Defendants remain.

D. Court IT Personnel / Clerks: Utilizing the All Writs Act in conjunction with the Court's inherent powers to direct the Clerk of this Court (E.D.N.Y.) and, as needed, other courts' clerks or IT departments, to implement special measures to safeguard court communications in cases involving Plaintiff. This includes maintaining this case's docket under seal or paper-only (as requested in the Prayer for Relief) and verifying any future filings or orders via non-digital means to prevent Defendants' interference. While clerks are part of the judiciary (and normally would comply with Court orders without needing All Writs invocation), specifying these directives under the Court's authority reinforces their necessity.

E. Other Persons in Active Concert: Generally, an order that any persons who are in active concert or participation with Defendants and receive actual notice of the injunction are bound to obey it. This mirrors Fed. R. Civ. P. 65(d) but may be reinforced via the All Writs Act to ensure that even those not yet identified but later found to be aiding Defendants (such as certain "hackers-for-hire" or complicit insiders) will be subject to the injunction.

160. Legal Basis: The relief requested is "necessary or appropriate" in aid of the Court's jurisdiction because it ensures the Court can grant complete and meaningful relief on the claims.

161. It is also "agreeable to the usages and principles of law" because similar relief has been granted in comparable anti-cybercrime cases, and it does not impose an undue burden on third parties – it essentially requires them to take reasonable actions to suspend illegal activities using their services. The All Writs Act is to be used judiciously, and here, given the demonstrated subversion of the legal process by Defendants, strong ancillary measures are justified.

162. Notice and Scope: Plaintiff will provide notice of the Court's orders to affected third parties as directed by the Court. The proposed All Writs relief will be narrowly tailored to those domains, IPs, and accounts specifically identified as part of Defendants' operation (e.g., listed in the CNF and Marlin reports and Microsoft's evidence).

163. Additionally, Plaintiff requests that the Court retain jurisdiction to modify or clarify any All Writs Act orders as needed to adapt to attempts by Defendants to circumvent them (for instance, if Defendants register new domains, the injunction could be extended to those).

164. In sum, invoking the All Writs Act will fill the gaps left by the direct causes of action, by binding the infrastructure and third-party support systems that Defendants exploit. This Court's ability to accord full justice in this matter – including stopping the ongoing attack and preserving the integrity of its own proceedings – hinges on such comprehensive relief. Plaintiff therefore respectfully asks that the Court issue the requested writs and orders in aid of its jurisdiction and to prevent continuing irreparable harm.

Count VI – Declaratory Judgment (28 U.S.C. § 2201) – Recognition of Microsoft v. Does Final Judgment (Sept. 8, 2025) as Binding on Defendants

165. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 25 above.

166. Actual Controversy: An actual, present controversy exists between Plaintiff and Defendants regarding the legal effect of a prior federal court judgment on Defendants' ongoing conduct.

167. Specifically, on September 8, 2025, in Microsoft Corp. et al. v. John Does 1–16, No. 1:23-cv-02447 (E.D.N.Y.), the United States District Court for the Eastern District of New York entered a Final Judgment and Permanent Injunction ("Final Judgment") against those John Doe defendants. A copy of the September 8, 2025 Final Judgment and the August 6, 2025 Report and Recommendations are Appended Hereto as Exhibit "A."

168. That case targeted the same hacking enterprise at issue here. The Final Judgment (upon default) permanently enjoined the Doe defendants – identified by their involvement in the Conti/TrickBot/LockBit Cobalt Strike infrastructure – from continuing their illicit

activities, and granted various equitable relief including domain seizures and other measures to dismantle the criminal infrastructure.

169. The controversy here is whether that Final Judgment binds and applies to the Defendants in this case, who Plaintiff alleges are in fact the very same persons (or successors in interest) as the enjoined John Does in the Microsoft case, and therefore subject to the same injunction terms.

170. Identity of Parties and Privity: Plaintiff contends that Defendants in the instant action are either identical to, or in privity with, the defendants in Microsoft v. Does.

171. The Microsoft case was brought against multiple John Doe individuals and groups known by monikers (including the Conti Ransomware Group, LockBit, DEV-0193, etc.). The evidence in this case (overlapping domains, IPs, tools) demonstrates that the John Does 1–20 here are part of that same set of actors enjoined by the Final Judgment.

172. At a minimum, Defendants here have been acting "in active concert or participation" with those enjoined persons, such that they would ordinarily be bound by the injunction under Fed. R. Civ. P. 65(d)(2) (even if not named, those with notice who aid/abet a violation are bound).

173. However, because the Microsoft judgment was obtained in a case to which Plaintiff Farrow was not a party, and Defendants dispute its applicability to them, a declaratory judgment from this Court is necessary to affirm the binding effect.

174. Relief Sought: Pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, Plaintiff seeks a declaration from this Court that the Final Judgment entered on Sept. 8, 2025 in Microsoft Corp. v. John Does 1–16 (E.D.N.Y.) is valid and binding upon the Defendants in this case. Specifically, Plaintiff requests the Court to declare that:

175. The individuals and entities operating the malicious infrastructure that harmed Plaintiff Farrow are the same individuals/entities that were defendants in the Microsoft case or are their agents, and thus are bound by the injunction issued in that case.

176. By continuing to engage in the enjoined conduct (e.g., operating the cracked Cobalt Strike servers, registering new malicious domains, interfering with victim networks), Defendants are in violation of the Microsoft Final Judgment's permanent injunction.

177. Accordingly, the terms of the Microsoft Final Judgment (including any prohibitions on operating or facilitating the malicious infrastructure, and any provisions for remedial action such as domain and IP address surrender) are enforceable in this Court against these Defendants, as if they were named in that judgment.

178. This declaratory judgment shall have the effect of giving preclusive and immediate force to the Microsoft Final Judgment in relation to Defendants' conduct toward Plaintiff, meaning that Defendants must cease any activity already prohibited by that prior injunction, independent of the relief in the current action.

179. Purpose and Effect: Such a declaration is warranted to avoid duplicative litigation and to expedite relief. The Microsoft v. Does case covered much of the same ground – it established the illegality of Defendants' infrastructure and obtained a permanent injunction dismantling it. Recognizing that judgment's binding effect here will essentially fast-track the neutralization of Defendants' operation, because the heavy lifting of technical findings and injunctive crafting has been done.

180. It will also serve the interests of justice by preventing Defendants from arguing in this case what has already been conclusively determined in the prior case (for example, they cannot relitigate the ownership or misuse of certain servers that were at issue). Plaintiff, though

not a party to the Microsoft case, is a beneficiary of the injunctive relief in the sense that disabling Defendants' infrastructure globally helps all victims, including Plaintiff.

181. Further Legal Basis: Courts can declare rights and relations under existing judgments especially when privity or identical parties are present. Given that John Doe defendants are a unique scenario, this declaratory relief provides clarity: it tells Defendants unequivocally that the prior injunction applies to them (no matter that they were anonymous there and here).

182. It also gives Plaintiff a means to enforce that injunction: once declared bound, if Defendants violate it, Plaintiff could seek contempt remedies leveraging that final judgment's authority.

183. In sum, a declaratory judgment in these terms will resolve an immediate dispute – Defendants have acted as though the Microsoft injunction does not constrain them, while Plaintiff asserts it does. The Court's declaration will settle this and pave the way for efficient enforcement. Plaintiff stands ready to provide the Court with a copy of the Microsoft Final Judgment and related records for review.

184. The declaration sought will not unduly prejudice Defendants (they had full opportunity to contest the Microsoft case but chose not to appear, resulting in default judgment). Equitably, they should not get a second bite to avoid that outcome. Thus, the Court's declaration will advance the interests of justice and judicial economy.

185. Prayer for Relief: WHEREFORE, Plaintiff Jay Lewis Farrow respectfully prays that the Court enter judgment in his favor and grant the following relief:

A. Emergency Meeting Injunction: An Order requiring Defendants to immediately (within 24 to 48 hours of the Order) participate in a meeting with representatives of Microsoft

Corporation and its attorneys, as well as Plaintiff's counsel, under Court supervision. The purpose of this meeting is to facilitate information-sharing and coordination of threat containment strategies. Defendants shall fully cooperate in revealing the scope of their infrastructure and malfeasance to Microsoft's Digital Crimes Unit and Plaintiff's team, enabling swift implementation of remedial measures.

B. Containment Directives (CNF/Marlin Modeled): A comprehensive injunction mandating that Defendants comply with all cyber-threat containment protocols recommended in the Cyber-N.E.T. Forensics Report (Oct. 22, 2025) and the December 5, 2024 Marlin Forensics Report. This includes, but is not limited to: immediately ceasing all network communications with infected devices; providing to Plaintiff's experts a complete list of domains, IP addresses, and accounts used in their operations; preserving and surrendering forensic data (logs, malware samples, etc.); and taking any other steps outlined by CNF and Marlin to isolate and neutralize the threat. The Court's Order should essentially mirror the emergency containment steps identified by those experts, thereby halting Defendants' ability to continue their attacks.

C. Secure Court Docket Directive: An Order directing the Clerk of the Court (E.D.N.Y.) to maintain the docket in this case under seal and on a paper-only (non-electronic) basis, until further notice. All filings, orders, and communications in this case are to be made via hard copy or in-person proceedings, with no use of CM/ECF or standard email for case documents. This measure ensures that Defendants cannot exploit electronic filing or notification systems to sabotage this action. The Order should also permit only designated Court personnel, vetted for this purpose, to handle any digital records (if

any) for internal use, and to require multi-factor verification for any actions affecting the case docket.

D. Florida System Audit and Dismantlement Injunction: Immediate injunctive relief compelling an independent, Court-supervised security audit and temporary shutdown of certain Florida state legal technology platforms that Defendants have demonstrably compromised. In particular, the Order should direct the State of Florida (through appropriate officials or directly to the system operators) to audit and temporarily dismantle or disconnect the Florida Courts E-Filing Portal (myflcourtaccess.com) and the Florida Bar's online platforms (including the Bar's membership portal and any lawyer credential databases). This may involve taking these systems offline, purging any malicious code or accounts (such as fake attorneys Defendants registered), and remediating vulnerabilities (like weak password flows or DNS issues) before restoring service. The injunction should also require Florida officials to cooperate with federal authorities (and Plaintiff's experts) in this process, and to preserve all logs and evidence of the intrusions for investigative purposes. The Floridabar.org website and email systems should similarly be audited and fortified or taken down as needed. By this relief, the Court protects not just Plaintiff but the wider legal community from the continuation of Defendants' abuse of those state systems.

E. Stay of Florida Supreme Court Order (Aug. 4, 2025): A preliminary and permanent injunction staying the effect of the Florida Supreme Court's Order dated August 4, 2025, to the extent that Order pertains to Plaintiff or was influenced by Defendants' misconduct. (On information and belief, that August 4, 2025 Order may relate to Plaintiff's professional status or a case outcome that Defendants improperly

engineered.) This Court should enjoin enforcement of that Order and any related disciplinary or legal action in Florida against Plaintiff, pending a thorough review. The stay is necessary because there is a strong likelihood that Defendants' fraud and interference (e.g., submission of false filings, suppression of notices) tainted the proceedings leading to the Florida Supreme Court's Order. By staying the Order, this Court will prevent further irreparable harm to Plaintiff's rights (such as unjust suspension of his law license or dismissal of his case) until the matter can be sorted out without Defendants' interference.

F. Seizure of Domains & DNS Infrastructure: An Order authorizing and directing the immediate seizure or disabling of all domain names, DNS records, and related Internet infrastructure used by Defendants in furtherance of their scheme, consistent with the containment protocols outlined by CNF and Microsoft's experts. This should include (i) transferring ownership of malicious domain names to a Court-approved receiver (or to Plaintiff's control) so that they no longer resolve for Defendants' use; (ii) revoking any TLS/SSL certificates associated with those domains to break the "padlock" trust Defendants abused; (iii) ordering DNS registries (e.g., Verisign for .com, PIR for .org) to propagate the necessary changes or sinkhole the domains; and (iv) enjoining any domain registrars or hosting services from providing service to those domains or IPs. A non-exhaustive list of such domains and assets (as identified in exhibits to the CNF Report, Marlin Report, and Microsoft declarations) should be attached to the Order, and it should include a catch-all for any additional infrastructure later identified as part of Defendants' arsenal. The purpose is to cripple the command-and-control infrastructure of Defendants immediately and prevent them from simply shifting to a new set of

servers. The Court should further order Defendants to surrender any cryptographic keys, credentials, or access tokens associated with their infrastructure, to facilitate a complete lockdown.

G. Any Further Relief Deemed Just and Proper: Such other and further relief as the Court deems just and equitable, including but not limited to compensatory damages (trebled where applicable), punitive damages, disgorgement of any ill-gotten gains, and investigative costs. Plaintiff also requests an award of reasonable attorney's fees and costs as allowed by statute (including under RICO, Florida RICO, CFAA, and ECPA provisions). Given the egregious and willful nature of Defendants' conduct, Plaintiff asks the Court to retain jurisdiction to enforce and modify its orders as necessary to ensure Defendants' full compliance and to address any attempt to circumvent the relief granted.

Verification: I, Jay Lewis Farrow, declare under penalty of perjury, under the laws of the United States of America, that I have read the foregoing Verified Complaint and that the factual allegations therein are true and correct to the best of my knowledge, information, and belief.

Jay L. Farrow
Dated: October 27, 2025 /s/ Jay Lewis Farrow
Jay Lewis Farrow, Plaintiff
1409 Baracoa Ave
Coral Gables, Florida 33146
786-719-8209
jaylewisfarrow@tuta.com
jcdc_ucdg@proton.me