UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.

JAY LEWIS FARROW, FARROW LAW, P.A., DR. JANE DOE, and INFANT DOE, Plaintiffs, vs. IOA GROUP, LLC, INSURANCE OFFICE OF AMERICA, INC., HEATH RITENOUR, JOHN RITENOUR, FTI CONSULTING, INC., STEVEN H. GUNBY, TIMOTHY KOLAYA, STUMPHAUZER, KOLAYA, NADLER & SLOMAN, PLLC, BRIAN MORAN, MORAN, KIDD, LYONS, JOHNSON, GARCIA, P.A., GUNSTER LAW, BENJAMIN WIEDER, MCCLATCHY MEDIA COMPANY, DUANE MORRIS, LLP, JOE TAYLOR RESTORATION, INC., JOSEPH CLIFFORD TAYLOR, WIESS, SEROTA, HELFMAN, COLE & BIERMAN, P.L., DUANE MORRIS, LLP, BUCKNERMILES, P.A., ROIG, ROSENBERG, MARTIN & BELLIDO, P.A., TELAN, MELTZ, WALLACE & EIDE, P.A., AMERICAN CASUALTY COMPANY OF READING, PENNSYLVANIA, BERKSHIRE HATHAWAY SPECIALTY INSURANCE COMPANY, CHUBB CUSTOM INSURANCE COMPANY, HARTFORD CASUALTY INSURANCE COMPANY, MARKEL INSURANCE COMPANY, NATIONWIDE INSURANCE COMPANY OF AMERICA, PHILADELPHIA INDEMNITY INSURANCE COMPANY, and SAFEPOINT INSURANCE COMPANY, Defendants._____	

VERIFIED COMPLAINT

COME NOW, Plaintiffs, JAY L. FARROW ("Farrow"), FARROW LAW, P.A., ("FLF" or "Farrow Law"), DR. JANE DOE ("Dr. Doe") and INFANT DOE (collectively "Plaintiffs"), by and through undersigned counsel, and hereby sue Defendants, and allege as follows:

PRELIMINARY SUMMARY STATEMENT

Since June 3, 2024, Plaintiffs, a mother, a father, and their infant child and have fought, inch by inch, through a waking nightmare being targets of an Advanced Persistent Threat Cyber-Attack ("APT") perpetrated by Heath Ritenour, John Ritenour, Insurance Office of America, Inc., IOA Group, LLC, Steven Gunby, FTI Consulting, Inc., along with their strategic partners and others ("Threat Actor Defendants").

On June 21 and 25, 2024, due to substantial cyber-attacks which commenced following the filing of an Amended Complaint against FTI Consulting and other Threat Actor Defendants in a separate federal case on May 28, 2024, Farrow, on behalf of his client and family, filed two Emergency Motions requesting they 'knock it off.' Days later, in their Joint Response, FTI and the others, did not deny they were causing the implosion of an opposing law firm, they said even if they "did it", there's nothing that could legally be done about it.

On Monday July 1, 2024, the Court denied the emergency relief, holding in part that mere temporal proximity of cyber-attacks corresponding to litigation events was not enough by itself to prove the defendants 'did it' even if they are computer hackers. **On July 10, 2024, just four business days later, Farrow Law was effectively closed after 16 years of business,** its clients left without lawyers and a family was left to fight for their very survival.

The following is a summary of where Plaintiffs were, how they survived and what they are prepared to do to see that these criminals be held to account and Justice be done:

Where they Were: Friday, July 12, 2024:

(1) Farrow Law Firm had effectively closed after over 16 ½ years in business;
(2) the Threat Actor Defendants stole files and evidence from the Farrow Law Network related to cases which affected them, sabotaging others, and rendering further prosecution improbable and practically impossible and leaving other Farrow Law clients without their legal counsel;
(3) the Threat Actor Defendants had engaged and completed substantial efforts to cover their tracks by deleting files, user accounts and other means of detecting their unauthorized access into Farrow Law's Network;
(4) Farrow's last attempt for a judicial hearing was denied on July 10, 2024;
(5) Farrow's communications with all but a few contacts had been severed;
(6) unauthorized access into collateral networks and computers of individuals and entities associated with Farrow and Farrow Law had been manipulated to filter and reject communications from Farrow, such as opposing counsels in cases affecting the Threat Actor Defendants and in all other cases;
(7) Farrow and Farrow Law's banking institution of over 25 years abruptly froze and permanently closed they accounts;
(8) the Threat Actor Defendants directed AI voice clone calls to Farrow and Dr. Doe to create situational crisis events directed at inflicting the maximum amount of pain, stress and interference with their relationships and, most importantly, causing Infant Doe trauma;
(9) The Coral Gables Police had been dispatched on three occasions after Farrow and Dr. Doe called for help, one of which was for a man sitting in a running parked car with lights off after 12:00 a.m. on July 3, 2024

How Plaintiffs Survived, and what they experienced during the last 7 months: Plaintiffs with, in no small measure, the psychological relief provided by the Federal Bureau of Investigation ("F.B.I.") (Miami Field Office) undertaking an investigation of their claims in early September 2024, file this Verified Complaint with the following snapshot summary of what they did to survive, what was thrown at them and how they survived as a family since July 10, 2024:

(1) **July 15, 2024 Family Circuit Case**: On July 15, 2024, Plaintiffs together sought relief under Florida's civil injunctive remedy for Cyberstalking. Ultimately, Plaintiffs' efforts to advance this litigation were thawed through the Threat Actor Defendants' unlawful infiltration into Florida's eFiling Authority's Network, the Miami-Dade CourtMap website and through a scheme using unlawful access to the Florida Bar's Network to target Farrow's law license.

(2) **July 19, 2024 Domestic Circuit Court**: On July 19, 2024, Farrow filed a Domestic Circuit Court Petition against Defendant Steven Gunby requesting an injunction be entered to prevent further cyberstalking. The Circuit Court entered an Order requiring Gunby's appearance on August 8, 2024, and as he failed to appear, it entered another order on August 29, 2024 for Gunby to appear, and he failed to do so…A third order was entered scheduling an October 9, 2024, which was cancelled and the fourth order rescheduling was not received via U.S. Mail until after the hearing was to occur.

(3) **Federal Bureau of Investigation ("F.B.I.") September 3, 2024**: On September 3, 2024, Special Agents Morton and Schafer of the Miami Field Office came to Farrow and Dr. Doe's home in response to their separate complaints

(4) **F.B.I. September 4, 2024**: On September 4, 2024, Farrow met with the Special Agents at the Miami Field Office and provided them with some electronic devices and documents.

(5) **F.B.I. September 7, 10, 17, October 10, 17 and 25, 2024, November 8, 28 and December 12 and 18, 2024**: On September 7, 2024, Special Agent Morton sent Farrow a portal for uploading documents and files directly to the F.B.I. Thereafter, through January 2025, Farrow has provided regular updates with respect to ongoing activities, supplemented with documentation and other evidence through subsequent F.B.I. portal links.

(6) **F.B.I. November 2, 2024**: - On November 2, 2024, Farrow met Special Agents Morton and Schafer at the F.B.I. Miami Field Office and reported some of his clients(s) were working with federal agencies in active domestic law enforcement field operations, and that one or more of these individual(s) electronic devices had been substantially compromised creating an opportunity for the Threat Actor Defendants to exploit a proximity vulnerability.

(7) **Three Client Affidavits Corroborate Substantially Identical Interferences with Devices and Emails**: From August 30 through Present, the Three Clients who were able to reestablish contact with Farrow have submitted Affidavits herewith reporting that after contact was reestablished, they experienced identical issues with the electronic communication devices and/or personal emails in addition to threats for physical altercations through email and/or text messages.

(8) **Affidavit of Medical Director of Pediatric Transplant, Adult Liver and Intestinal Transplant at Jackson Memorial Hospital, Associate Professor of Medicine Dr. Jane Doe**: Dr. Jane Doe is the Medical Director of Pediatric Transplant, Adult Liver and Intestinal Transplant at Jackson Memorial Hospital and UM Heath's Miami Transplant Center and her Affidavit testimony is clear and unequivocal as to her evaluation of the facts, her experience of being the target, for example, of AI Voice Spoofing Calls which come through the same cell phone which is essentially the 911 number for organ transplant

offers from around the country and a lifeline to physicians around the world treating pediatric patients experiencing organ failure.

(9) **Farrow and Farrow Law's Affidavit of October 22, 2024** describing the continuing cyber and non-digital attacks which exploded after the filing of an Amended Complaint and an Amended Injunction Motion in Miami-Circuit Court on September 30, 2024. While Farrow requested an emergency hearing several times through the Miami-Dade County CourtMap portal, this emergency motion, nor two others, were delivered or delay due to the Threat Actor Defendants unlawful access and manipulation of Florida's eFiling Portal's Network and/or other malicious activities which prevented access to courts.

(10) **Interferences with Active Federal Law Enforcement Domestic Field Operations: November 11, 2024 Ex Parte Motion:** After Farrow's meeting with Special Agents Morton and Schafer at the FBI Miami Field Office in early November, the conduct escalated leading to the filing a November 11, 2024 Ex Parte Emergency Motion and the discovery that the Threat Actor Defendants had interfered with the Miami-Dade County, Florida CourtMap website to block and/or delay the delivery motions upload for court review on that system.

(11) **December 5, 2024 Expert Report**: The Expert Report Summary Opinion dated December 5, 2024 not only concludes that Plaintiffs were and are the subject of an APT Cyber Attack, it also describes in detail how the Threat Actor Defendants accomplished the effective closure of Farrow Law and also the conduct and activities which occurred after July 10, 2024 which were directed to prevent the discovery of years of criminal conduct. More specifically, the Expert Report describes, in part, a pattern of activity involving practically each and every website domain, or its Top Level Server ("TLS") that Farrow, Farrow Law and Dr. Doe interacted with since July 2019. This pattern, along with the analysis of two of Farrow's computers, provided that there was a high probability that hundreds of web domains were the subject of a 'lame designation' attack, or Sitting Duck Cyber Attacks.

(12) **December 5, 2024 Expert Report Summary Opinion**: The Expert Report Summary Opinion concludes that there is a high probability that that FTI, in particular, orchestrated, planned, and executed the APT Cyber-Attack Against Plaintiffs.

(13) **Official Records of Nearly 225 Web Domains and Hosting Server Domains Reflect Nefarious Compromises after July 10, 2024 related to the Threat Actor Defendants Malicious Activates directed at Plaintiffs:** By exploiting an array of vulnerabilities, the Threat Actor Defendants gained access into over 40 computer networks and the protected computers connected to those networks, such as those belonging to over **(a) thirty-four (34) law firms**, **(b) Florida's eFiling Authority**, **(c)the Florida Bar**, **(d) Florida's Lawyer's Assistant, Inc.**, **(e) and networks associated with the Jackson Memorial Hospital, Jackson Heath, and the UM Heath System** which were used for malicious purposes all in pursuit of their Ultimate Goals of causing Plaintiffs substantial damages as specifically defined herein.

(14) **The Florida Bar and Florida ePortal Authority Network Breaches**: From August through December 2024, Plaintiffs encountered substantial issues logging into, filing and paying for state court filings. In late December 2024, Farrow and Dr. Doe

procured substantial evidence of thousands of unauthorized breaches into the Florida Bar's Network and Florida's eFiling Authority's Network. These included three spreadsheets containing the precise username, passwords, URLs and email addresses to Florida Bar staff attorneys and/or employee accounts.

(15) **Florida Lawyers Assistance, Inc.'s Network Breach and the Stealing of FLA Client Information**: The Threat Actor Defendants theft of confidential information from the Farrow Law Network included information contained within the reoccurring calendar entries related to the Remote Video Conference Meetings of the Tuesday, 5:30 pm Fort Lauderdale Florida Lawyers Assistance Group. These entries included the "RingCentral" link, and the private emails of over forty (40) lawyers who were invited to attend that group. The FLA meetings had been continuous since the group switch from live to remove meetings in March 2020 due to the pandemic. FLA has changed its protocol for the weekly Fort Lauderdale meeting in response to the reported conduct and activities. Farrow's computer's hard drive also revealed that the Threat Actor Defendants monitored these confidential meetings as they illegally recorded at least three of them, such as one on Tuesday May 9, 2022. Notably, the Threat Actor Defendants use of this and other stolen information from Farrow Law's Administration File related to Farrow's Health is known as extortionist medical shaming.

(16) **The Florida Supreme Court**: As a direct result of the interferences with the Florida Bar's Computer Network, ***within days of serving Threat Actor Defendants Heath Ritenour, John Ritenour and FTI Consulting*** in early October 2024 with the 2024 Family Circuit Court Complaint and a September 30, 2024 Verified Emergency Motion, from October 15 through October 25, 2024, a Florida Bar 'legal assistant' sent over a dozen letters to Richard Wiess of Wiess Serota, in his capacity of the alleged ***"Grievance Committee Chair" of Broward Section 17F*** accusing Farrow of failing to respond to official bar inquires. On October 17, 2024, ***Chairman Richard Wiess' Law Firm also posted a 3-Day Eviction Notice on Farrow Law's Office Door*** claiming it represented Regus Management, the firm's landlord. Ultimately, on November 4, 2024, Farrow drove from Miami to Tallahassee to hand-deliver updated responses, as well as, all of his communications with the F.B.I. so as to ensure that the Florida Bar received the same. Nevertheless, Grievance Committee 17F Chaired by ***Mr. Wiess advanced a Petition to the Florida Supreme Court filed on November 25, 2024 in the name of the Florida Bar demanding Farrow's immediate suspension*** and representing that Farrow failed to respond or provide any cause for allegedly not responding to official bar inquires.

(17) **January 3, 2024 -the Evidence of Unlawful Interference with the Florida Bar and Florida's eFiling Authority's Network:** On January 3, 2024, Farrow, Dr. Doe and Infant Doe hand-delivered evidence to the Florida Bar in Tallahassee contained within three spreadsheets showing the precise usernames, passwords, URLs and timestamps of unlawful infiltrations into its network and that of Florida's eFiling Authority. In response, in rapid succession, two 'Florida Bar' lawyers left the FSC case, and yet another legal secretary sent over a dozen letters to Farrow from a bogus email account and a third "Bar Counsel" filed a substitution of counsel, yet otherwise, neither Farrow, or Dr. Doe, have been contacted by the Florida Bar with respect to having hand-delivered evidence which,

by example, provides not only access to the Florida Bar, but also whatever access that Florida Bar employee had to law enforcement agencies throughout the United States:

	ip	url
2	73.1.75.247	https://member.floridabar.org/CPB
3	None	https://member.floridabar.org/
4	None	https://member.floridabar.org/
5	172.93.148.174	https://member.floridabar.org/
6	172.93.148.174	https://member.floridabar.org
7	172.93.148.174	https://member.floridabar.org/
8	172.93.148.174	https://member.floridabar.org
9	73.35.85.168	https://member.floridabar.org/CPB
10	None	https://member.floridabar.org/CPB
11	73.0.216.215	https://member.floridabar.org/
12	73.0.216.215	https://member.floridabar.org/
13	73.1.75.247	https://member.floridabar.org/CPB
14	None	https://member.floridabar.org/CPB
15	None	https://member.floridabar.org/CPB
16	73.125.172.145	https://member.floridabar.org/CPB
17	None	https://member.floridabar.org/CPB
18	None	https://member.floridabar.org/CPB
19	None	https://member.floridabar.org/
20	None	https://member.floridabar.org/CPB
21	None	https://member.floridabar.org/
22	None	https://member.floridabar.org/CPB
23	None	https://member.floridabar.org/CPB
24	None	https://member.floridabar.org/CPB
25	None	https://member.floridabar.org/
26	None	https://member.floridabar.org/CPB
27	None	https://member.floridabar.org/CPB
28	None	https://member.floridabar.org/
29	None	https://member.floridabar.org/CPB
30	158.62.50.143	https://www.floridabar.org/wps/port

	email	passw
2	mimifried@aol.com	Happy
3	z.zimlaw@gmail.com	602sta
4	z.zimlaw@gmail.com	602sta
5		602sta
6	az@zipilaw.com	602sta
7	az@zipilaw.com	602sta
8		602sta
9	dhabell@yahoo.com	Semin
10	benayat.111@gmail.com	jood00
11	emask@flcourts.org	Marilyı
12		Marilyı
13	mimifried@aol.com	Happy
14	mimifried@aol.com	Happy
15	mimifried@aol.com	Happy
16	mimifried@aol.com	Happy
17	edkellyatlaw@aol.com	ryanbe
18	edkellyatlaw@aol.com	Serge
19		Serge
20	mimifried@aol.com	Happy
21		Serge
22	edkellyatlaw@aol.com	Serge
23	edkellyatlaw@aol.com	ryanbe
24	edkellyatlaw@aol.com	Serge
25		Serge
26	edkellyatlaw@aol.com	ryanbe
27	edkellyatlaw@aol.com	ryanbe
28		Serge
29	edkellyatlaw@aol.com	Serge
30	:0CCtm1lLqRPI ksMqk-KbGoahS8k	Jetthe

	insertion_time
2	2024-09-27 0(
3	2024-06-21 0(
4	2024-06-21 0(
5	2024-06-19 0(
6	2024-06-19 0(
7	2024-06-19 0(
8	2024-06-19 0(
9	2024-06-17 0(
10	2024-05-02 0(
11	2024-04-20 0(
12	2024-04-20 0(
13	2024-04-16 0(
14	2024-02-09 12
15	2024-02-09 12
16	2024-02-19 12
17	2024-02-09 12
18	2024-02-09 12
19	2024-02-09 12
20	2024-02-09 12
21	2024-02-09 12
22	2024-02-09 12
23	2024-02-09 12
24	2024-02-09 12
25	2024-02-09 12
26	2024-02-09 12
27	2024-02-09 12
28	2024-02-09 12
29	2024-02-09 12
30	2023-12-31 12

https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://clearwaterfl.mycusthelp.com/WEBAPP/_rs/(S(jxgqedtpbf5siyh3osj3	jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezrı	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezrı	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://leecountysheriff.govqa.us/WEBAPP/_rs/(S(dztht24ymq1vebykx0dm:	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://securemail.csbflorida.com/s/e	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org
https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org

(18) **January 3 through present:** One of Farrow Law's clients received a threat of physical altercation, and Farrow discovered that the email he had been using from September through January had been compromised due to an unlawful infiltration of computer he had been using since from August 2024.

Plaintiffs Stand Ready to Pursue Justice: Evidence Summary and Expert Conclusions:

Pointedly and factually, this is not a complicated case of "who did it." Over the last Seven Months, Plaintiffs have collected substantial evidence, most of which was not available to be organized, cataloged and or discovered until late December 2024, however, herein Plaintiffs are prepared to fight back with evidence derived from:

(1) electronic devices;
(2) photos taken in real time of computer hacking activities;
(3) screenshots from laptops and cell phones,
(4) business and personal emails;
(5) text messages and emails from clients, opposing counsel and vendors;
(6) metadata from websites;
(7) metadata from email Dropbox links, documents and attachments sent by Defendants;
(8) unauthorized installed applications, programs, updates and shortcuts;
(9) CVEs issued by National Cyber-Security and Infrastructure Agency;
(10) exploitation of permission enhancing software located in FLF's network;
(11) detected and identified static IP Addresses revealing sources of malicious code,
(12) unauthorized user device signatures, and stolen certificates;
(13) distinctive Living off the Land maneuvering, and initial infiltration vectors
(14) user interface device detection and location software;
(15) Situational Awareness and Counterintelligence Gathering Module Incident Reports;
(16) Register of Executable Remote Commands by Unauthorized FLF Network Users
(17) Trace Ping Routes, forensic code analysis of suspect C2 Domains;
(18) pattern utilizations of application and code languages in suspect C2 Dead Drops;
(19) Locating and cataloging DNS records reflecting unauthorized 'updates' 287 domains;
(20) Locating 'root' Top Level Servers for Suspect Compromised Domains;
(20) Exfiltrating admin data from FLF hard drives registering errors and warnings;
(21) Florida Bar's Computer Network and Compromised User interfaces;
(22) Florida's eFiling Authority's Network Compromised URLs and User PII
(23) location of part of FTI's team which executed at least some of the SAPT's operations.

In this Verified Complaint, which is supported by Verified Motions, 5 Affidavits, an Expert Report and Documentary evidence, and within Plaintiffs' contemporaneously filed Emergency Injunction

Motions, the facts are strait forward, the methodology of analysis is simple, and the resulting conclusions are undeniable:

(1) Plaintiffs the victim of a Cyber-Attack;
(2) the Threat Actor Defendants are the only ones with the motive, army of elite cyber experts trained in conducting an Advanced Persistent Threat Cyber Attack ("SAPT"), the incredible financial means to sustain an APT, and documented histories of abuses of legal proceedings,
(3) the Threat Actor Defendants are the only ones that benefitted from the sabotaging Farrow; and
(4) Plaintiffs sustained substantial damages and continue to suffer irreparable harm for which there is not adequate remedy at law.

INTRODUCTION

1. The truth is, before all else, there is no sugarcoating that Plaintiff Farrow's mindset that cyber-security could be delegated to professionals without him developing his own cyber-health habits was an exploitable vulnerability – a vulnerability most have until they become the victim of cyber-crime. As of June 2, 2024, Farrow's mindset encountered no resistance as everything in Farrow Law's Network appeared to be working, yet just four weeks later, after over 16 and ½ years in business, Farrow Law was effectively closed due to the Threat Actors striking after they had fortified their positions.

2. After July 11, 2024, all the might haves, should haves, could haves and maybes do nothing to mitigate the real-life consequences which emerged after Plaintiffs' lives as they knew them were completely decimated.

3. By the beginning of August 2024, due to the environmental stressors, the situational crisis events designed by the Threat Actor Defendants and the general upending of Farrow and Dr.

Doe's lives and lifestyles, Farrow and Dr. Doe may have lived in the same residence, but it was anything but home.

4. Yet, the real-life manifestations caused by the Threat Actor Defendants' incessant and persistent harassment emerged through traumatic symptoms, most noticeably when Infant Doe stopped saying the words he had been saying months before.

5. Dr. Doe was blameless, yet she could not stop her instinctive parental guilt, and by any measure, her pain and her suffering were exponentially worse observing Infant Doe's sudden inability to speak. And that's because her entire career as an attending physician and medical director of pediatric transplant has been centered around taking care of infants, babies and children fighting for a chance to have a childhood with all the trauma that surrounds months-long hospitalizations.

6. With that experience, Dr. Doe immediately recognized that the sudden and drastic changes to Infant Doe's environment and the ongoing conduct and activities directed to ensure that her and her husband not only got knocked out, but stayed down correlated to regressive development.

7. Over the last eight months, the Threat Actor Defendants watched from a distance as Plaintiffs lost material things and stopped engaging social activities. Yet, that was only part of what they sought to accomplish which was using their cyber-fence to piece by piece, and day by day, slowly deprive this family of the real magic that makes life so precious and beautiful.

8. But – this family did not stay down – and as admirable as that may seem, it should never happen here – not ever - that folks like Heath Ritenour and Steven Gunby can use a cyber-attack to steal a law firm, deprive clients their legal counsel in active cases, delete the rule of law

and then target a family with the intention to use powerful cyber-weapons to cause permanent emotional trauma to a baby and his parents, and simultaneous cause catastrophic financial damages to ensure their voices were never heard in this or any other court again.

12. Plaintiffs are filing contemporaneously herewith, a motion seeking emergency injunctive relief requesting, at the very least, a narrowly tailored order directed to ensure Plaintiffs can present their case with the same protections, freedoms, liberty and privacy that the Threat Actor Defendants have had, and should have, to present theirs.

13. Thereafter, said motion requests a full evidentiary hearing such that the plethora of evidence which they had and now have may be presented in the daylight of an open court where Plaintiffs seek the only thing that may stop the Threat Actor Defendants – suspensions, restrictions and/or conditions on their insurance licenses and or their corporate charters.

OVERVIEW OF PLAINTIFFS' CLAIMS FOR RELIEF

14. Plaintiffs Farrow, Dr. Jane Doe, Infant Doe and Farrow Law seek claims for violations of the Federal Civil Racketeering Statute, 18 U.S.C. 1962(c) and 1964, Civil Remedies for Violations of 18 U.S.C. § 1030(g), and common law intentional torts and negligence.

15. Plaintiffs seek damages against the Law Firm Defendants as they either knew, should have known, recklessly, or through gross negligence or negligence, failed to implement reasonable policies, procedures and operational guidelines with respect to monitoring their DNS records for, *inter alia,* irregular 'updates' – which can be located through open sources, such as ICANN.ORG. Pursuant to their actions and omissions, the Law Firm Defendants, wittingly or unwittingly, left open a gaping and well-established vulnerability which the Threat Actor Defendants used for malicious purposes and that caused Plaintiffs substantial damages.

16. Plaintiffs also seek an emergency restraining order and emergency temporary injunctive relief pursuant to 18 U.S.C. 1030(g), and/or **Florida's Criminal RICO Act "Civil Remedies", Fla. Stat. §§895.05(1)(a)(e) and (6)**, ordering and directing specific defendants to cease interfering with the protected computers, electronic devices, private emails, and other networked protected computers which have been used and are being used to interfere with Plaintiffs' access to Florida's eFiling Portal, the Florida Bar's Computer Network or otherwise with Plaintiffs' access to Florida state courts.

17. Plaintiffs seek compensatory damages, statutory damages, special damages, and punitive damages in excess of $75,000,000.00 to send the message that using an Advanced Persistent Threat to accomplish closing an opposing law firm, stealing its files, interfering with unrelated litigation cases, especially using the cloak of legitimate legal proceedings to serve discovery DropBox links and pdfs to implant malicious code and malware is considered by courts of law in these United States as the pinnacle of legal depravity, and that then to persistently terrorize a family thereafter to escape the consequences of such crime will never be tolerated.

I. JURISDICTION AND VENUE

18. Court has jurisdiction over the subject matter of the causes of action in this Complaint by virtue of:

19. Federal question jurisdiction pursuant to 28 U.S.C. § 1331, under (A) the Federal Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§ 1964(a), (c) and (d); and (B) pursuant to the Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030(g).

20. Supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a), involving claims that are so related to claims in the action within the Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

21. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendants transact business in this district or, alternatively, this district is where a substantial part of the events or omissions giving rise to the claim occurred.

22. Venue is also proper in this district pursuant to 18 U.S.C. § 1965.

II. PARTIES

23. Plaintiff Jay L. Farrow ("Farrow") is a Florida resident residing in Miami-Dade County, Florida and is otherwise *sui juris*.

24. Plaintiff Dr. Jane Doe ("Dr. Doe") is a Florida resident residing in Miami-Dade County, Florida and is otherwise *sui juris*.

25. Plaintiff Farrow Law, P.A, a Florida Profit Corporation, authorized to do business in the State of Florida and conducts business in Miami-Dade County, Florida.

26. Plaintiff Infant Doe is a Florida resident residing in Miami-Dade County, Florida and is otherwise *sui juris*. Infant Doe is the minor child of Farrow and Dr. Jane Doe.

27. Defendant FTI CONSULTING, INC. is a Company incorporated and existing under the laws of Maryland. This Defendant is subject to personal jurisdiction pursuant to Fla. Stat. § 48.193 in that Defendant engages in substantial and not isolated activities within the State of Florida, has sufficient contacts within this jurisdiction upon which to support personal jurisdiction, and because subjecting it to personal jurisdiction in Miami-Dade County Florida does not otherwise offend traditional notions of fair play and substantial justice. Specifically, Defendant

engaged in and/or carried on business and business ventures in the State of Florida, has an office for its regularly conducted business activities in Miami-Dade County, Florida and throughout the United States relative to the offering of business advisory services to Heath Ritenour, John Ritenour, Insurance Office of America, Inc., IOA Group, LLC, and the Insurance Carrier Defendants. Additionally, Defendant has caused Plaintiffs to suffer injury in this State as a consequence of the acts alleged herein. This Defendant is also subject to jurisdiction pursuant to 18 U.S.C. § 1965.

28. Defendant STEVEN H. GUNBY is a resident of Bethesda, Maryland. This Defendant is subject to personal jurisdiction pursuant to Fla. Stat. § 48.193 in that Defendant engages in substantial and not isolated activities within the State of Florida, has sufficient contacts within this jurisdiction upon which to support personal jurisdiction, and because subjecting it to personal jurisdiction in Miami-Dade County Florida and the Southern District of Florida does not otherwise offend traditional notions of fair play and substantial justice. Defendant has committed tortious acts within this state, and within the Southern District of Florida, and through those acts, Defendant has caused Plaintiffs to suffer injury in this jurisdiction. Defendant is also subject to jurisdiction pursuant to 18 U.S.C. § 1965.

29. Defendant HEALTH RITENOUR is a Florida resident residing in Seminole County, Florida and is otherwise *sui juris*.

30. Defendant JOHN RITENOUR is a Florida resident residing in Seminole County, Florida and is otherwise *sui juris*.

31. Defendant IOA GROUP, LLC ("IOA, LLC") is a Florida Limited Liability Company, is a Florida Limited Liability Company, with its principal place of business located in Seminole County, Florida.

32. Defendant INSURANCE OFFICE OF AMERICA, INC. ("IOA, Inc.") is a Florida corporation with its principal place of business located in Seminole County, Florida.

33. Defendant JOE TAYLOR RESTORATION, INC. ("JTR, Inc.") is a Florida corporation with its principal place of business located in Palm Beach County, Florida.

34. Defendant JOSEPH CLIFFORD TAYLOR ("Taylor") is a Florida resident residing in Palm Beach County, Florida and is otherwise, *sui juris.*

35. Defendant TIMOTHY KOLAYA ("Kolaya") is a Florida resident, residing in Miami-Dade County, Florida.

36. Defendant BRIAN MORAN ("Moran") is a Florida resident, residing in Seminole County, Florida.

37. Defendant CHRIS OPRISON is a Florida resident and is otherwise *sui juris.*

38. Defendant BENJAMIN WIEDER ("Wieder") is a resident of Maryland.[2]

---

[2] This Defendant is subject to personal jurisdiction pursuant to Fla. Stat. § 48.193 in that Defendant engages in substantial and not isolated activities within the State of Florida, has sufficient contacts within this jurisdiction upon which to support personal jurisdiction, and because subjecting it to personal jurisdiction in Miami-Dade County Florida and the Southern District of Florida does not otherwise offend traditional notions of fair play and substantial justice. Defendant has committed tortious acts within this state, and within the Southern District of Florida, and through those acts, Defendant has caused Plaintiffs to suffer injury in this jurisdiction.

39. Defendant MCCLATCHY MEDIA COMPANY is a Delaware Corporation with its principal headquarters located in New Jersey. McClatchy is a media company who owns over fifty (50) newspapers, including the Miami Herald, a newspaper with online and printed circulation within Florida and the Southern District of Florida. McClatchy is subject to personal jurisdiction pursuant Footnote 2.

40. STUMPHAUZER, KOLAYA, NADLER & SLOMAN, PLLC ("SKNS PLLC") is a Florida Professional Limited Liability Company, with its principal office located in Miami-Dade County, Florida. Defendant is defined herein as a Law Firm Defendant.

41. Defendant GUNSTER LAW is a Florida law firm with an office located in Miami Dade County, Florida where it carries on its normal and not isolated business activities. Defendant is defined herein as a Law Firm Defendant.

42. Defendant WIESS, SEROTA, HELFMAN, COLE & BIERMAN, P.L, is a Florida law firm with offices in Miami-Dade County, Florida. Defendant is defined herein as a Law Firm Defendant.

43. Defendant MORAN, KIDD, LYONS, JOHNSON, GARCIA, P.A. ("Moran&Kidd") is a Florida Professional Association, having an office in Miami-Dade County, Florida where it conducts regular and not isolated business activities. Defendant is defined herein as a Law Firm Defendant.

44. Defendant ROIG, ROSENBERG, MARTIN & BELLIDO, P.A. is a Florida law firm having it headquarters in Broward County, Florida. Defendant is defined herein as a Law Firm Defendant.

45. Defendant TELAN, MELTZ, WALLACE & EIDE, P.A. is a Florida law firm having its headquarters in Orange County, Florida. Defendant is defined herein as a Law Firm Defendant.

46. Defendant BUCKNER AND MILES, P.A. is a Florida law firm with its headquarters in Miami Dad County, Florida. Defendant is defined herein as a Law Firm Defendant.

47. Defendant DUANE MORRIS, LLP, is Pennsylvania Limited Liability Partnership, with offices in Miami-Dade County, Florida where it conducts regular and not isolated business activities. This Defendant is subject to personal jurisdiction pursuant to Footnote 4. Defendant is defined herein as a Law Firm Defendant.

48. Defendant AMERICAN CASUALTY COMPANY OF READING, PENNSYLVANIA is a Pennsylvania corporation. This Defendant is also subject to personal jurisdiction pursuant to Fla. Stat. § 48.193 in that Defendant engages in substantial and not isolated activities within the State of Florida, has sufficient contacts within this jurisdiction upon which to support personal jurisdiction, and because subjecting it to personal jurisdiction in Miami-Dade County does not otherwise offend traditional notions of fair play and substantial justice. Specifically, Defendant engaged in and/or carried on business and business ventures in the State of Florida and throughout the United States relative to the offering of insurance policies and collection of policy premiums on various lines of insurance, of which the Heath Ritenour, John Ritenour and/or Insurance Office of America, Inc. were or are brokers/agents of record and this action arises out of those activities. Additionally, Defendant has caused Plaintiff to suffer injury

in this State as a consequence of the acts alleged herein. This Defendant is subject to jurisdiction pursuant to 18 U.S.C. § 1965.

49. Defendant, BERKSHIRE HATHAWAY SPECIALTY INSURANCE COMPANY, is a company incorporated and existing under the laws of Nebraska.[3]

50. Defendant CHUBB CUSTOM INSURANCE COMPANY is a Company incorporated and existing under the laws of Delaware. Plaintiff incorporates Footnote 3 as if fully set forth herein.

51. Defendant HARLEYSVILLE INSURANCE COMPANY is a Company incorporated and existing under the laws of Ohio. Plaintiff incorporates Footnote 3 as if fully set forth herein.

52. Defendant HARTFORD CASUALTY INSURANCE COMPANY is a Company incorporated and existing under the laws of Connecticut. Plaintiff incorporates Footnote 3 as if fully set forth herein.

---

[3] This Defendant is also subject to personal jurisdiction pursuant to Fla. Stat. § 48.193 in that Defendant engages in substantial and not isolated activities within the State of Florida, has sufficient contacts within this jurisdiction upon which to support personal jurisdiction, and because subjecting it to personal jurisdiction in Miami-Dade County does not otherwise offend traditional notions of fair play and substantial justice. Specifically, Defendant engaged in and/or carried on business and business ventures in the State of Florida and throughout the United States relative to the offering of insurance policies and collection of policy premiums on various lines of insurance, of which the Heath Ritenour, John Ritenour and/or Insurance Office of America, Inc. were or are brokers/agents of record and this action arises out of those activities. Additionally, Defendant has caused Plaintiff to suffer injury in this State as a consequence of the acts alleged herein. This Defendant is subject to jurisdiction pursuant to 18 U.S.C. § 1965.

53. Defendant MARKEL INSURANCE COMPANY is a Company incorporated and existing under the laws of Illinois. Plaintiff incorporates Footnote 3 as if fully set forth herein.

54. Defendant NATIONWIDE INSURANCE COMPANY OF AMERICA is a Company incorporated and existing under the laws of Ohio. Plaintiff incorporates Footnote 3 as if fully set forth herein.

55. Defendant PHILADELPHIA INDEMNITY INSURANCE COMPANY is a Company incorporated and existing under the laws of Pennsylvania. Plaintiff incorporates Footnote 3 as if fully set forth herein.

56. The Insurance Carriers named hereinabove shall collectively be referred to as the Carrier Defendants or Insurance Carrier Defendants.

57. The Law Firms named above shall collectively be referred to as the Law Firm Defendants.

III. GENERAL ALLEGATIONS REGARDING PLAINTIFFS AND DEFENDANTS

Plaintiff Farrow Law, P.A.

58. On January 8, 2008, Farrow opened Farrow Law, P.A. d/b/a Farrow Law Firm. Farrow Law Firm ("FLF" or "Farrow Law").[4]

59. From 2008, FLF has represented hundreds of clients throughout the State of Florida with various legal issues involving foreclosures, business disputes, commercial litigation, post-

[4] See Affidavit Farrow and Corporate Representative of FLF dated October 22, 2024. A copy of same is appended hereto and incorporated herein as Exhibit "A".

judgment relief actions, civil remedies for criminal practices and transactional matters such as the preparation of limited liability operating agreements and business closings.

60. From May 2009 through January 2023, FLA maintained its main office in the same office executive building in Davie, Florida.

61. In January 2023, FLF's main office moved to 1 Alhambra Plaza, PH, Coral Gables, Florida 33134.

62. From March 2020 through December 2024, FLF transformed its logistical operations to allow its employees to work remotely due to the Covid pandemic, while also maintaining a physical office for employees to work and to meet with clients in Davie and then Coral Gables, Florida.

63. As of March 2024, FLF had three full time attorneys, a firm manager/administrator, one paralegal and two legal assistants.

64. As of March 2024, FLF had maintained relationships with several contract attorneys who provided support services, and at least three of these attorneys had worked with FLF from nearly 4 to 6 years.

65. As of March 2024, FLF had developed valuable relationships from 4 to over 7 years with vendors including an Information Technology company, a web-developer, court reporters, process servers, and its telephone system provider.

66. As of April 1, 2024, FLF had never been sued for default of any loan, eviction, replevin, or for taking money for legal services which were not rendered.

67. As of April 1, 2024, FLF was not late paying revolving commercial credit accounts for more than 30 days, nor had it reported any fraudulent activity for unknown charges to its credit

cards or business debt cards seeking reimbursements more than a handful of times in over 16 years in business.

68. As of June 1, 2024, no client had ever reported being the target of a cyber-attack or having any of their personal emails/cell phones being compromised, nor had any client reported having emails from FLF or to FLF, or any of its employees, be placed directly into "spam" or "drafts".

69. As of June 1, 2024, FLF had never experienced any known breach of its Microsoft One Drive Cloud-based Network ("FLF Network"). As of June 1, 2024, each FLF employee had a business email address with the law firm which was firstname@farrowlawfirm.com.

70. As of June 1, 2024, FLF had an excellent online reputation, with numerous previous clients voluntarily writing complimentary reviews of their experiences with the firm and its staff over the previous decade, and within the previous year.

71. By July 3, 2024, as alleged in detail, *infra,* pursuant to the Threat Actor Defendants' conduct, FLF was effectively closed after over 16 and ½ years in business as the FLF Network was overtaken, secure and verifiable communications were severed and access to electronic court filings made impossible.

72. Pursuant to this effective closure of July 3, 2024, and the continuing conduct of the Threat Actor Defendants since that time through the filing of this lawsuit, FLF lost five employees, access to its computer network, communications with all but a few clients has been constructively or actually impossible, and its online reputation has been severely damaged.

Plaintiff Jay L. Farrow

73. Plaintiff Jay Farrow was born in Miami, Florida in July 1975.[5] Farrow graduated from the University of Florida in 1999.

74. During law school, Farrow clerked for the Miami-Dade State Attorney's Office in 2000 and was a certified intern for that office in 2002. During Farrow's certified internship, he requested and was assigned to a forensic team compiling research geared to create legislative amendments to various Florida Criminal Statutes using statistical data extracted from hundreds of electronic devices to form theoretical models which informed the relationship between statutory threshold variances and probative behavioral modifications.

75. In 2022, Farrow graduated from the University of Miami School of Law, cum laude, where he was the Senior Articles and Comments Editor to the Business Law Review.

76. Farrow has been practicing law since March 2003.

77. Farrow has worked in forensic fraud and white-collar fraud cases since 2003.

78. Farrow has been a member of the Southern District of Florida since 2005, the Middle District of Florida since 2023 and is also a member of the Bankruptcy Court for the Southern District.

79. For over ten years through present, Farrow has been associated with an attorney, judge and law student group organization known as Florida Lawyer's Assistance ("FLA"), and,

[5] Each of the allegations with the Section "Plaintiff Jay L. Farrow", along with other designated Sections of the Factual Allegations are verified by Jay Farrow, individually, and as the Corporate Representative of Farrow Law, P.A, immediately following the "Jury Demand" herein below. See also the October 22, 2024 Affidavit of Jay Lewis Farrow Exhibit "A" hereto.

based upon his relationship with FLA and having honored his commitments, Farrow has had the honor to serve as a designated 'monitor' of other lawyers and law students as they begin their journey with FLA.

80. Farrow has formed a small niche providing pro bono legal services to individuals in need of an organ transplant but have legal issues related to their receiving the same – either related to pre or post operation care.

81. For example, in 2023, Farrow provided pro bono work to an eighteen-month-old infant needing a liver transplant which cleared an issue with her insurance such that she was able to be listed and receive a lifesaving transplant. This child is now nearly four years old and thriving.

82. In 2024, Farrow provided pro bono legal services to an adult male needing a liver transplant, and while the legal work allowed him to be cleared for the transplant, unfortunately, he passed away hours after being listed by the transplant team.

83. From 2014 through 2023, Farrow was a member of the St. Anthony Church Music Ministry located in downtown Fort Lauderdale where he composed and performed weekly piano preludes to mass services and sang in the widely acclaimed St. Anthony Choir.

84. From 2014 through present, Farrow has also provided legal representation and confidential support resources to individual(s) working in various roles with federal law enforcement agencies, and in some cases, Farrow's confidential support is provided while these individual(s) are working with federal agencies in domestic law enforcement field operations.

85. Up to June 2024, Farrow was not more than 30 days late in paying personal credit cards, car loans and had an average credit score of approximately 720 for the previous three years.

86. After June 2024, Farrow lost his income, and his ability to generate income as the Threat Actor Defendants have consistently interference with every single email address and every single new telephone he has purchased, and even one that was provided to him.

87. After June 2024, Farrows bank accounts with cash on deposit were closed after 24 years based upon interferences by the Threat Actor Defendants with his previous banking institution.

88. On June 21 and 25, 2024, I prepared and caused to be filed, on behalf of Farrow Law's Client, Louis Spagnuolo two Verified Emergency Motions in the matter styled Spagnuolo v. American Casualty Company of Reading, Pennsylvania, United States District Court, Southern District of Florida et. al., Case Number: 24-cv-60422-SMITH-HUNT. On June 27, 2024, I also caused to be filed as counsel for Spagnuolo a Reply to the Defendants "Joint Response."[6]

89. On November 21, 2020, Farrow married Dr. Jane Doe.

90. On August 10, 2022, Farrow and Dr. Jane Doe became first-time parents to Infant Doe.

91. Pursuant to the conduct of the Threat Actor Defendants through the filing of this lawsuit, Farrow has suffered substantial financial, reputational, consequential and emotional damages, as well as special damages.

[6] A copy of these Court Filings are appended hereto and incorporated herein as Composite "B".

92. Pursuant to the ongoing conduct directed at Farrow, he continues to irreparable harm through the Threat Actor Defendants unauthorized access to and use of: (1) media entities' computer networks; (2) the Florida Bar's Computer Network; (3) Florida's eFiling Authority's Computer Network; (4) Florida Lawyer's Assistance's Employee Emails and (4) emails, devices, email servers and website hosting servers belonging to business relationships and colleagues, family members, banking institutions, credit companies, and friends.

Plaintiff Dr. Jane Doe

93. Dr. Jane Doe was raised in West Miami, Florida, and attended the University of Michigan on full scholarship where she graduated with high honors.[7]

94. Dr. Jane Doe then attended and graduated Tufts Medical School in Boston, MA.

95. Thereafter, Dr. Jane Doe returned to Miami, and began as a resident at Jackson Memorial Hospital where she would ultimately become an attending physician and associate professor of medicine at the University of Miami Miller School of Medicine.

96. Dr. Jane Doe's is now the Medical Director of Pediatric Transplant and Adult Liver and Intestinal Transplant at the Jackson Heath/UM Health Miami Transplant Center.

97. Dr. Jane Doe's is also one of 10 Pediatric Transplant Physicians who sub-specialize in intestinal transplant.

[7] See Affidavit of Jane Doe which incorporated herein by reference and attached hereto as Exhibit "C".

98. Dr. Jane Doe is first author or contributing author of authoritative medical journal articles and chapters related to her and her team's groundbreaking work at the largest academic transplant institute in the United States.

99. Dr. Jane Doe is "on-call" an average of 10 days out of any given month. And, given her role as the Medical Director of Pediatric Transplant, her cell phone is "911" with regards to receiving transplant offers from around the country and coordinating the patients, surgeons and staff once an organ has been accepted.

100. Additionally, as the medical director of pediatric transplant and adult liver, she is on-call as to receiving donor offers and calls from physicians around the world seeking her advice as to patient issues practically every day.

101. Dr. Jane Doe has received numerous accolades from those residents and fellows for the time she takes to teach and lead by example.

102. In January 2020, Dr. Jane Doe and Farrow became engaged to be married.

103. In March 2020, Dr. Jane Doe discovered she was pregnant with what would have been her first child weeks after the Threat Actor Defendants caused two lawsuits to be filed against Farrow and Farrow Law.

104. On November 21, 2020, Dr. Jane Doe married Farrow and became a mother for the first time on August 10, 2022.

105. One year later, in August 2023, Dr. Jane Doe became pregnant with what would have been her second child.

106. Since at least March 2023, Dr. Jane Doe has been a direct target of the Threat Actor Defendants APT's conduct and activities and has suffered substantial financial, emotional, consequential and special damages as a result of that conduct.

107. In her Affidavit, Dr. Doe stated and testified as to her work, independent evaluation of the facts, and intentional acts directed to cause her, Farrow, and Infant Doe pain, distress and harm, her written testimony plainly states:

> I am, at the end of the day, a scientist. I am an associate professor of medicine and have been an attending physician and first responder to the most critically ill patients and most precious in our hospital system. I am also the director of the program and oversee other attendings, fellows, residents and work very closely with my surgeons even in the operating room and base my work on facts, empirical data and the truth. **Anything less, someone dies. And, here, I had to see and observe and come to my own conclusions as I do in my work….**
>
> Here, I observed for myself the attacks, the compromise of my devices, the unauthorized expenditures, the hacking into my Gmail, the Wi-Fi going out, the corruption of my alarm system, my husband's inability to call his staff, clients and IT vendor, him working all hours to document this complete destruction of his work and I have experienced seeing the photographs which were manipulated to show that his continuance in any case using the evidence he found would result in harm.
>
> I cannot have this, nor do any of my patients…. nor those patients that will come in the door over the next week deserve to have any interference with my or my staff's work. **I do not understand that they don't understand what they are doing can get someone killed, but I am telling them every moment of mine and my staff work is a moment we cannot afford to lose** and if they would bother to check or care enough to know, *perhaps they should round with my staff in the Pediatric Intensive Care Unit as we do daily and see what it looks like for a baby to fight for their life – before they send another threating call* attempting to investigate our child's schedule…

> Again, I witnessed the conduct at issue here, I investigated it myself as I cannot afford to trust anything but my own experience when it comes to things as serious as attempting to harm a child or destroy a family. [Emphasis added].

108. The Threat Actor Defendants conduct and ongoing activities Dr. Doe include, *inter alia* which includes, *inter alia,* (1) persistently hacking her home internet account and router; (2) persistently using the unauthorized access to her personal cell phone; (3) using non-digital attacks to cause substantial situational emotional distress such as mailing through the U.S. Mail letters directly from alleged former clients of Farrow and Farrow Law implying Farrow has engaged in conduct which would result in Florida Bar consequences; and (4) directly or indirectly, harassing Dr. Doe at her office through a social engineering campaign related to the son of one of the nurse practitioners in her department.

Plaintiff Infant Doe

109. In or about November 2021, Dr. Jane Doe became pregnant with Infant Doe.

110. Infant Doe was born in Miami-Dade County, Florida in August 2022.

111. In May 2024, Infant Doe had been developing normally in speech and motor skills, using an age-appropriate vocabulary.

112. By August 2024, due to the specific targeting of Infant Doe by the Threat Actor Defendants using intentional circumstantial crisis events, Infant Doe suffered substantial trauma resulting in being diagnosed with developmental regression of approximately 12 months.

The Defendants

- **John Ritenour, Heath Ritenour, IOA Group, LLC and IOA, Inc.**

113. Defendant IOA, Inc. was founded in or about 1988 by Defendant John Ritenour and his wife, Valli Ritenour.

114. Defendant John Ritenour has been a licensed insurance agent in Florida for over thirty (30) years, he was IOA, Inc.'s first President, CEO and Chairman of the Board of Directors.

115. Defendant IOA Group, LLC is the parent of IOA, Inc. and, at all times material hereto, either Defendant Heath Ritenour or John Ritenour has maintained direct or indirect managerial and operational control over IOA, LLC and otherwise been its manager pursuant to its Operating Agreement and Articles of Incorporation.

116. Defendant John Ritenour is also the managing member of 1188 Partners, LLC ("1188 Partners").

117. Defendant John Ritenour is also the managing member of JKR Professional, LLC ("JR, LLC").

118. Defendant John Ritenour remained IOA's CEO until 2008 and remain its Chairman of the Board of Directors until early 2019.

119. IOA, upon information and belief, is one of the largest independent insurance agencies in the United States, with over 1500 Agents.

120. Defendant Heath Ritenour is the son of John Ritenour and Valli Ritenour.

121. In 2008, Defendant Heath became IOA's CEO.

122. In 2019, Defendant Heath Ritenour became IOA, Inc.'s Chairman.

123. Defendant Heath is the current CEO of Defendant IOA, LLC.

124. From approximately 2008 through present, Defendant Heath makes yearly presentations as to the value of IOA, LLC's private stock at the annual shareholder's meetings on or about April of each year.

125. From 2014 through present, Defendants Heath Ritenour and John Ritenour submitted applications for appointment and/or reappointment to be the agents of the Carrier Defendants which were approved by the Carrier Defendants.

126. From 2019 through Present, Defendant Heath and Defendant John have received, directly or indirectly, insurance commissions from the insurance policies they submit to the Carrier Defendants.

127. In or about 2018, Defendant Heath became IOA's Chairman of the Board of Directors, and he remains in such capacity either in name and/or through his activities and conduct he regularly engages in and/or exhibits over IOA.

128. From 2007 through the filing of this lawsuit, Defendants Heath Ritenour and/or John Ritenour maintain actual or constructive operational control over IOA, LLC and IOA, Inc., notwithstanding any purported other individual's title or actual or apparent authority within those entities.

129. Defendants Heath and John are also licensed Insurance Producers for IOA, and these Defendants are licensed insurance agents in over 15 states.

130. Defendants Heath, John and Noah Talesnick own, manage, direct and/or operate Web Solutions of America, Think Creative, LLC and Think Integrated, LLC.

Defendant FTI Consulting, Inc.

131. Over the course of over forty (40) years, FTI has grown to be a publicly traded company with over 9,000 employees, with offices in approximately forty-five (45) countries, and has one of the most infamous reputations for having one of the most aggressive, experienced and well-equipped corporate crisis management/cyber-security remediation teams in the world.[8]

132. FTI also touts it is one of the only companies in the world which offers crisis management services, that is to say, there rapid deployment teams include cyber-security experts for offensive and defensive responses, as well as highly trained experts who create what FTI (and those in the industry) call communication strategies.

133. FTI's communication strategies involve researching, developing and deploying a plan to, *inter alia,* to build the foundations of the narrative its client desires to be sold to corporate employees, shareholders, and the public after, for example, a corporation's top leadership team in general or one key individual becomes entangled with a criminal investigation, regulatory malfeasance or a public scandal for engaging in some form of moral turpitude.

134. FTI sets the parameters, milestones, budget and ultimate goals, with the ladder becoming the goals of FTI and their core teams of experts and communications strategists.

135. Other operations and services FTI provide, include, acting as third-party contractors for Insurance Carriers, such as the Carrier Defendants to mitigate payment on insurance claims.

[8] *See generally,* https://www.fticonsulting.com.

Here, FTI uses ‘experts’ to provide a ‘report’ which purportedly disputes the findings of, for example, public adjusters, roofing engineers, medical professionals or other licensed professionals who submit expert analysis reports as to the amount of money an insured should be paid on their insurance claim.

136. Over the last ten to thirteen years, FTI has also been retained by political figures and operatives to plan and implement communication strategies around clandestine actions taken by foreign governments.

137. FTI’s business model, culture and conduct is directed at to accomplishing client goals.

138. Over the last 8 years, FTI has been retained by Large Oil Companies, Roundup Pesticide, and the New York District Attorney who successfully prosecuted President Donald J. Trump and the Trump Organization procuring a February 2024 Final Judgment in excess of Three Hundred Fifty Million Dollars ($350,000,000.00) which is currently on appeal.

139. More precisely, FTI’s online articles, website and social media posts highlight the scores of former national cyber-security agents and intelligence officers who work on its strategic communication strategies, crisis management and reputation stabilization teams, such as the former decorated Special Agents and Special Agents in Charge of Task Forces and Joint Task Forces of the Federal Bureau of Investigation (“FBI”).

140. For over the last 10 years, FTI has worked with, consulted for, planned and executed crisis management operations all over the globe for Fortune 100 companies.

141. For over the last 10 years, FTI claims to have worked with 98 out of the top 100 largest law firms in the world, either providing them litigation support, forensic investigative services, consulting advisory services and crisis management services.

142. For over the last ten years, FTI has hired choice law firms when it has been named as a bankruptcy trustee, or receiver or with respect to its providing of services to its clients.

143. For over the last ten years, FTI has provided preventative cyber-security services to global law firms, insurance carriers, large insurance agencies, and Fortune 500 companies.

144. More specifically, according to its website www.fticonsulting.com and articles it publishes frequently online, part of FTI's alleged services relate to situations where organizations face investigations involving allegations of corporate fraud and misconduct, money laundering, bribery and corruption, trade sanction violations, and other regulatory issues.

145. FTI's website states that where such allegations are made, they must address such allegations or inquiries from regulators with a rapid and appropriately tailored response.

146. More specifically, this includes responding to an incident, uncovering critical facts, communicating with regulators, engaging in remediation efforts, and, ultimately, meeting the requirements of a settlement agreement and repairing reputational damage.

147. FTI had and has the ability mobilize and rapidly deploy a team of cyber-experts with experience in defending against the most sophisticated cyber-attacks, including those perpetrated and funded by hostile nation-states anywhere in the world to support its client's needs.

148. From 2012 through present, FTI's crisis management and communications strategy teams are notorious infamous for their success in achieving their client's ***offensive***, as

well as their defensive, operational goals through the discovery and exploitation of digital (cyber) and non-digital vulnerabilities.

149. FTI's hallmark of its corporate crisis management and strategic communications services involves the manipulation of human decision making and conduct, also known as social engineering.

150. FTI's social engineering commonly begins with researching a human target, and tailoring an email, message or situational event to cause that person to provide otherwise confidential information or Personal Identification Information ("PII") for purposes of achieving operational milestones in pursuit of its clients' ultimate goals.

151. FTI's social engineering experts direct influence upon individuals without their knowledge by feeding them information which is directed at shifting their choices, or their impressions about other individuals they work with or are within their 'sphere of influence.'

152. In this case, FTI and/or the other Threat Actor Defendants' employees, contractors, business associates and/or partners, conspired to commit the above referenced computer, computer network and personal electronic communication device unauthorized intrusions, and/or, did, in fact commit those intrusions, by and through various means and methods, *inter alia,* by installing malware on protected computers, and obtaining, using, maintaining and communicating with computer and internet infrastructure located in the United States or obtained from commercial providers in the United States.

153. FTI, along with some or all of the Threat Actor Defendants' infrastructure included electronic communication accounts (*e.g.* email accounts), social media accounts, computer servers, domain names, computer software and other items.

154. FTI is a publicly traded company, with a NYSE ticker FCN.

155. FTI regularly files required regulatory documents with the SEC.

Defendant Steven Gunby

156. According to FTI's SEC records, Defendant Steven Gunby was elected and hired to be FTI's CEO in 2013 and became its CEO in 2014.

157. Upon becoming CEO, and through the filing of this lawsuit, Steven Gunby has sought reelection to FTI's CEO position and has been elected each year, with his last successful bid to remain as CEO being on or about June 5, 2024.

158. Steven Gunby is also the officer, director and/or owner of other corporations in the United States and Great Britian.

159. In or about March 2024, Steven Gunby is an individual who directly and/or indirectly requested and received FTI's services for his individual benefit.

160. Steven Gunby also directed, participated in, had knowledge or and/or consented to the means and methods used to by FTI, and/or those of the other Threat Actor Defendants to achieve their individual or collective Ultimate Goals they are defined herein.

161. In or about April 30, 2024, or after May 2, 2024, Steven Gunby procured information by and through the unauthorized access to protected computers (as further defined herein below through specific individual and collective unauthorized infiltrations into protected computers belonging to Farrow, Farrow Law, their attorneys and others) that Farrow and Farrow Law had prepared the first court motion which would allege some or all of the newly discovered evidence that FTI, and its clients, Heath Ritenour, John Ritenour and IOA had manipulated judicial proceedings using various methods and means since at least Junne 2020.

162. While this motion to disqualify was substantially detailed, and was filed on March 2, 2024, it was not filed in case as against FTI, Steven Gunby or any executive or employee of FTI and, as such, Steven Gunby knew or should have known that the motion and testimony would likely or highly probative, would not be discovered by and through the normal course of research and/or due diligence by market analysts or FTI shareholders.

163. Notwithstanding, in advance of the filing of the motion and the testimony of Spagnuolo detailing criminal conduct on behalf of FTI to illegally obstruct justice and unlawfully interfere through undue influence upon a judicial proceeding, Steven Gunby did knowingly sell millions of dollars of his personal FTI stock at a time where FTI's publicly traded shares were at or near all-time highs.

164. From May 2, 2024 through the next 14 days, Steven Gunby did direct, order and/or instruct individuals under his personal control to effectuate the sale of his ownership of FTI shares when he knew or should have known that if the information had been made public, the same would have likely devaluated the price of FTI stock.

165. Thus, by selling FTI's stock under those circumstances, Steven Gunby sold FTI stock using insider information which was not readily available to the public and for which he had a duty to disclose to the shareholders of FTI.

166. From 2019 through May 2024, Steven Gunby directed the preparation of regulatory forms 8-K and 10-K and approved, adopted and directed the same to be transmitted over interstate wires to the SEC which contained information Steven Gunby knew or should have known to be false and misleading.

167. This was accomplished such that Defendant Steven Gunby could line his pockets, in part, through remaining as CEO of FTI by fraudulently increasing FTI's profit margins as either FTI did not actual pay any remuneration because the individual did not exist, or it paid these remote workers far less than the qualified employees who had credentials and experience.

The Insurance Carrier Defendants

168. Each Carrier Defendant may only transact insurance business in Florida, and in any other state, under a valid Certificate of Authority or its equivalent.

169. In order to qualify, obtain and maintain a subsisting Certificate of Authority issued by the Florida Department of Financial Services ("FDFS"), each Carrier Defendant was and is required to be in compliance with Florida's Insurance Code ("FIC"), its own charter powers and satisfy the other eligibility requirements of the FIC, e.g. Fla. Stat. §§624.404 and 409.

170. The duties and obligations for maintaining the privilege to transact insurance are ongoing and continuous for any insurer, such as the Carrier Defendants.

171. At all times material hereto, from at least 2013, each Carrier Defendant was and is presently authorized to transact insurance in Florida, and in several other states, as it maintains a subsisting Certificate of Authority issued by the FDFS, or its equivalent.

172. From at least 2013, each Carrier Defendant, in Florida and in each state, it is authorized to transact insurance, has regularly provided financial, compliance and requested information to the FDFS, or its equivalent, for purposes of demonstrating its continuing adherence to the FIC and applicable provisions of the Florida Administrative Code ("FAC") (or their equivalent) for purposes of maintaining its COA.

173. From at least 2013, each Carrier Defendant has actual and/or constructive knowledge of the FIC and FAC, or their equivalent in other jurisdictions, with respect to both compliance and the consequences for noncompliance and/or violations of the same.

174. From at least 2013, each Carrier Defendant has appointed over 500 agents under their respective COA, or its equivalent, with the actual and constructive knowledge of their respective obligations in making appointments.

175. From at least 2013, each Carrier Defendant had actual and/or constructive knowledge that by informing the FDFS, or its equivalent, of its decision to appoint an individual agent, the respective Carrier was certifying that it had completed an independent and thorough investigation of their appointee and deemed them to be following the applicable insurance code and otherwise trustworthy to transact insurance in Florida.

176. With regard to obtaining an Insurance License under the FIC, or its equivalent in another state, a "person" is required written application to the FDFS and pass the applicable written, as well as character examinations with regard to, *inter alia,* their trustworthiness.

177. After receiving a license from the FDFS, the same does not yet permit the individual from transacting insurance.

178. Pursuant to Fla. Stat. § 626.451 of the FIC, or its equivalent in another state, there is a second requirement for an agent to transact insurance, to wit: an insurance carrier, acting under its subsisting COA, must review a licensee for an appointment to be its agent.

179. Under the FIC, or its equivalent in another state, upon receiving an application from a licensee, an insurer must perform an independent investigation into the moral character, trustworthiness and in compliance with the FIC of the potential appointee, after which, the insurer

may appoint if it determines that, in its opinion, the licensee is otherwise in compliance with law and has demonstrated trustworthiness.

180. An individual must have both a license and at least one appointment from an insurer to transact insurance business in Florida, and in other states.

181. An individual must also be reappointed every 24 months by the insurer, at which time, the insurer must conduct another investigation of their appointee for compliance with the FIC, or its equivalent, and as to their character and trustworthiness.

182. Pursuant to its obligations under the Insurance Code, each individual Defendant Carrier operating under its Certificate of Authority is required to engage a comprehensive and independent investigation into each appointee applicant as to their initial appointment, which similarly includes an inquiry into the character, trustworthiness and that otherwise the appointee applicant is in compliance with the provisions of the FIC.

183. After this investigation and inquiry, the FIC requires each of the Carrier Defendants to certify they have completed an independent investigation and also certify that, in the carrier's opinion, they are appointing the insurance agency and insurance agent to act as their agent, being satisfied that they are of good moral character and are in compliance with the provisions of the FIC.

184. Each and every Defendant Carrier not only issued IOA, Heath Ritenour and John Ritenour ("Appointees") an initial appointment, but have since, each in turn, reappointed one or all of the Appointees in not less than three instances of electronic transmissions over interstate wires to the FDFS.

185. Each and every Defendant Carrier's certification as to one or all of IOA, Heath Ritenour and John Ritenour was a fraud upon the State of Florida, and caused damage to the Plaintiffs and others, because each Defendant Carrier failed to comply with their statutorily defined obligations relative to investigating and formulating their certified opinions as to the Appointees fitness, trustworthiness, and compliance with the FIC *and* IOA.

186. Not only did the Carrier Defendants simply fail to investigate Appointees, the abandonment of their statutory obligations to engage a thorough investigate is systemic and pervasive as they routinely fail to investigate their appointees upon appointment and reappointment.

187. More specifically, each and every Defendant Carrier failed to, *inter alia*:

(1) formulate any meaningful investigative process which did anything but a routine background check that never followed up with information which would tend to impugn the Appointees character.

(2) implement universal standards for making certifications of fitness which would deny appointment or reappointment regardless of the amount of business the application had or currently sends to the Defendant Carrier, to the State of Florida.

(3) establish clear and unequivocal guidance and training to compliance employees or investigators such that readily available public information could be researched and evaluated prior to issuing a certification of the Appointees or any appointees.

(4) engage processes for contacting character witnesses, or witnesses which related to information considered concerning to the compliance employees or internal investigators.

(5) promulgate proscribed procedures for alerting management of information which would qualify for additional investigations or inquiries into any appointee applicant or the Appointees specifically.

(6) failed to investigate within each of the Carrier Defendants internal systems to determine if any of their officers, directors, employees, departments, or other agents had entered into back-end contingency agreements or horizontal non-competitive agreements with other carriers related to the Appointees or any other appointee applicant.

(7) engaged a "run" report as to the amount of business being referred to and bound with each Defendant Carrier as to each of the Appointees or other appointee applicants for purposes of making further inquiries based upon the known correlation between large brokerages binding numerous policies on the same lines of insurance and illegal kick-back agreements.

(8) proscribe and implement a clearly noticed policy of non-retaliation for an internal reporting of information which could disqualify any of the Appointees or others like them which drove large amounts of business to the Defendant Carrier.

(9) creating and implementing standard policies which foster compliance with the FIC by each Defendant Carrier and the agents, the Appointees; and

(10) engage in, or create, or design an ongoing investigatory practice which would seek to research or obtain through private submissions information which could disqualify the Appointees or those like them, such that each Defendant Carrier would also be operating in accordance with the FIC and their individual Certificate of Authority.

228. However, regarding re-appointing the Appointees, the Carrier Defendants failed to engage policies, procedures and standards referenced herein above.

229. Each and every Defendant Carrier reappointed the Appointees because of their strategic partnership with the Ritenours and IOA, Inc.

230. Regardless of the sufficiency of their investigations, or the veracity of their certifications, the Carrier Defendants transmitted the Appointees appointments over interstate wires to the FDFS in furtherance of the schemes to derive ill-gotten gains through, as it relates to Plaintiffs, using a cyber-attack to substantially interfere with, and/or eliminate, the advancement of claims against the Carrier Defendants by Farrow and Farrow Law.

231. The Carrier Defendants, through their initial and subsequent appointments of the Appointees, certified their willingness to be responsible for the Appointees' conduct under Florida Stat. 626.451(3).

188. The Appointees conduct herein was within the scope of their respective appointments by the Carrier Defendants and/or was within the scope of an agreement, implied or otherwise, to act or engage in a serious of actions directed to benefit the Carrier Defendants, financially, or some other benefit. .

189. Moreover, to the extent that Heath Ritenour, John Ritenour and IOA, Inc.'s conduct was outside the scope of their respective appointments, the FIC requires nevertheless that the Carrier Defendants' original and subsequent appointments certify that these Defendants be deemed fit, after actually having gone through an appropriate investigation conducted by the Carrier Defendants into the trustworthiness and compliance with the FIC, to be reappointed to have the privilege to transact insurance. However, at the very least, such an investigation was not performed, or was performed with reckless and/or gross negligence as to be tantamount to not having engaged performed such investigation.

724. Moreover, from 2019 to present, the Carrier Defendants had actual and/or constructive knowledge of, or should have known pursuant to their statutory duties pursuant to Fla. Stat. §626.451, or because Appointees made a claim on their Directors/Officers Errors and Omissions policies with some of the Carrier Defendants, that

(A) FTI was retained by Appointees for purposes of a comprehensive plan of "crisis management," communication strategies, expert data analysis, and counter-litigation strategies to rehabilitate Appointees reputations and/or otherwise restore confidence in IOA's stock valuation which was essential for the continuation of Appointees ability to direct insurance policies and insurance premiums on new and renewal policies to the Carrier Defendants, which the Carrier Defendants had profited from for over a decade with regard to TLE business and other insurance business.

(B) FTI would engage an aggressive and unconventional campaign using its advanced social engineering cyber capabilities, as well as, other tactics such as using their personnel to manipulate or create false profiles, internet postings and false professional

accomplishments to allow them to affect the judicial proceedings in which Plaintiff was a litigant in Seminole County, especially the 2020 SLAPP Lawsuit.

(C) FTI, through its actions and conduct on behalf of Appointees, was, in effect, directly and/or indirectly supporting and protecting the Carrier Defendants' profits and revenues they received from the Appointees.

(D) they failed to engage any measure to prevent, mitigate or stop these schemes from commencing or otherwise to engage in conduct and directives to have the same cease at any time from 2019 through present.

(E) the Carrier Defendants have made approximately 15% to 20% more revenue from the insurance premiums from the TLE Account every year through present, and they continue to receive millions more in insurance premiums from Appointees, or others at IOA working at their direction, as a consequence of continuing to reappoint Appointees and as a consequence of favorable results from the litigation targeted by FTI and Appointees.

The Strategic Alliance Defendants

190. As their plan and strategy to achieve their Ultimate Goals, as defined, *infra,* took shape, FTI, Heath, John, IOA, Inc., IOA, LLC, 1188 Partners and JKR, LLC found strategic alliances with Defendants Joe Talor Restoration, Joe Taylor and others (the "Strategic Alliance Defendants") who began to litigate against clients who hired Farrow Law in early 2000.

191. Plaintiffs allege that the individuals and entities who comprise the Strategic Alliance Defendants all had identical or nearly identical Ultimate Goals which they sought to

achieve by entering into an alliance and demonstrated their willingness to participate in tandem and cooperation to achieve those Ultimate Goals with the other members of the alliance.

192. The Strategic Alliance Defendants shared identical and/or nearly identical Ultimate Goals and, they agreed that they would, in furtherance of achieving those Ultimate Goals, participate by sharing work product, strategies, information, costs, revealing settlement confidential settlement discussions, and allow FTI's designated team and/or teams to use their tactics, techniques and tradecraft as needed and requested.

The Aiding and Abetting Defendants

193. From at least August 2019, Defendant Kolaya was and is an attorney for IOA, Inc., Heath Ritenour and John Ritenour who has provided material support, assistance, which included failing to act, that facilitated the Threat Actor Defendants to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

194. From at least August 2020, Defendant Brian Moran was and is an attorney for IOA, Inc., Heath Ritenour and John Ritenour who has provided material support, assistance, which included failing to act, that facilitated the Threat Actor Defendants to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

195. From at least March 2024, Defendant Chris Oprison was and is an attorney for one of the Carrier Defendants and/or FTI Consulting, Inc. who provided material support, assistance, which included failing to act, that facilitated the Threat Actor Defendants to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

196. The Carrier Defendants appointed and reappointed Defendants Heath Ritenour, John Ritenour and IOA, Inc. as their agents pursuant to the FIC, and they provided material

support, assistance, which included failing to act, that facilitated the Threat Actor Defendants to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

197. From at least March 2020, Defendants JTR and Taylor has provided material support, assistance, which included failing to act, which provided and/or facilitated these Defendants to allow them to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

198. From at least July 2022, Defendants Wieder and McClatchy provided material support, assistance, to the Threat Actor Defendants that facilitated the Threat Actor Defendants to commit tortious acts and/or the violations of 18 U.S.C. § 1030 which form part of Plaintiffs' claims.

199. Kolaya, Moran, the Strategic Alliance Defendants, Wieder, McClatchy and the Carrier Defendants compromise the Aiding and Abetting Defendants.

The Law Firm Defendants

200. The Law Firm Defendants intentionally, knowingly, or under circumstances which they should have known, or, through recklessness, gross negligence and/or negligent acts and omission, failed to monitor their office Domain Name System records, or put policies and procedures in place such that their DNS records would be monitored for, *inter alia,* registered 'updates' to such records.

201. By intentionally, recklessly, with gross negligence and/or negligence, failing to monitor their respective DNS records, threat actors and/or the Threat Actor Defendants used a known exploit to procure ownership, admin privileges and/or permissions or some authority to

manipulate the web domains owned by each respective Law Firm Defendant for malicious purposes, which caused Plaintiffs' damages.

The Threat Actor Defendants

232. Collectively, Defendants Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, FTI, Steven Gunby, the Carrier Defendants and the Strategic Alliance Defendants JTR and Taylor consist of the Threat Actor Defendants.

IV. THE APT's OBJECTIVES, SEQUENCES, SCHEMES AND TRADECRAFT

202. From 2019 to present, Plaintiffs allege that the Threat Actor Defendants planned, intended to execute and executed a Cyber-Attack modeled after or substantially designed with the architecture of an APT for purposes of achieving their Ultimate Goals as defined specifically herein.

203. From 2019, the Threat Actor Defendants separately and/ or in association with another or all other Threat Actor Defendants, direct, or indirectly, and/or through the hiring of contractors, subcontractors or through means and methods in which they directed, controlled or it was understood that they directed, controlled or had influence over, individuals and entities, did cause the carrying out of some or all of the cyber and non-digital activities directed at Plaintiffs, their contacts, family members, and others as alleged herein.

204. This involvement to give any direction or approval may have been verbal or written, or any indication of which signified an intent, or an act or omission which was understood to be their intent of consent to carry forward the conduct and activities in pursuit of their ultimate goals, defined herein, *supra.*

205. By referring to the APT, Plaintiffs do not allege that the plans, discussions or operators considered their workings as an APT, Plaintiffs allege that the cyber and non-digital attacks followed the architect and/or model of an APT as defined by, for example, the National Cyber-Security and Infrastructure Security Agency ("NCIA") and F.B.I.

206. Between about June 2019 and ongoing through the filing of this Verified Complaint, the Threat Actor Defendants, together and with others known and unknown, conspired to commit a sprawling array of computer intrusions targeting protected computers in the United States and the Southern District of Florida to unlawfully achieve specific objectives using the form, structure and sequence framework structures of an APT.

OBJECTIVES: The Ultimate Goals of the Threat Actor Defendants

207. Plaintiffs allege that they were the targeted victims of a highly sophisticated, coordinated, prolonged and expensive digital and non-digital attack which was planned, executed, funded and maintained, directly and/or indirectly by the Threat Actor Defendants and other known and unknown individuals and entities for purposes of achieving certain and specific operational goals.

208. Plaintiffs allege that the digital and non-digital attacks which targeted them were and are an APT with the ultimate operational goals (herein defined collectively as "**Ultimate Goals**") to:

(1) substantially interfere with and/or eliminate the prosecution of civil lawsuits against the Threat Actor Defendants, the Carrier Defendants and the Co-Conspirator Defendants by Plaintiffs;

(2) mitigate or eliminate any civil legal consequences related to any of the Defendants claims;

(3) sabotage Farrow Law to effectuate is closure;

(4) cause substantial, catastrophic and/or destroy Farrow and Dr. Jane Doe's careers, reputations, credit and relationships with friends and family; and/or

(5) intentionally use sophisticated digital and non-digital attacks, including creating situational crisis events which were and are designed specifically to create traumatic anchors, environmental stressors, fear, anxiety, exhaustion, and/or physical and/or mental pain, suffering and anguish[9];

(6) inflicting the maximum amount of emotional, financial, reputational, domestic, physical pain and collateral damage as possible as part of the strategic communications corporate crisis management services to thaw and chill other agents, employees and business associates of the Defendants from initiating, prosecuting or continuing to prosecute future litigation against them; and

(7) each Threat Actor Defendant sought an Ultimate Goal of financial benefits and rewards by and through the use of the sophisticated, coordinated, and persistent digital and non-digital attacks against Plaintiffs. Plaintiffs allege that the financial benefits and the methods, means and mechanisms of the renumeration of ill-gotten gains varied, and may

---

[9] All of which was and is specifically tailored to each Plaintiff based upon substantial initial and ongoing research and intelligence gathering, and designed to create automatic traumatic responses which would cause irreversible, permanent and/or substantially prolonged physical and emotional pain and suffering; and as it relates to Infant Doe, to cause developmental regression and/or cause permanent and/or substantially prolonged neurological brain injuries to Infant Doe

have been direct, indirect, intended, expected and/or passive. Plaintiffs allege that any respective Defendants' financial benefit may have been monetary or non-monetary. Plaintiffs also allege that any respective Defendant's direct or indirect financial benefit may have been through knowing or should have knowing they would receive a financial reward by and through the conduct of any other Defendant or group of Defendants, and that they did directly and/or indirectly engage in conduct or omissions such that they would receive the same.

THE SEQUENCE: the Components and Flow of the Cyber-Attack

209. In this case, the Threat Actor Defendants (a/k/a the "TADs" or "TAD Defendants") built their APTs framework around the defined objectives of the Ultimate Goals.

210. The Threat Actor Defendants' conduct and activities directed at achieving their Ultimate Goals were nearly impossible to detect from the inception of their APT in or about 2020.

211. The Threat Actor Defendants' conduct and activities were more challenging to have been detected during the maintenance/persistence sequence framework structures of the APT.

212. As in most of the documented APT Cyber Attacks, the TADs' activities and conduct were discovered, years after initial access into the first protected computer was achieved.

213. Plaintiffs allege that, due to the sophistication of the TADs' conduct and activities, their malicious conduct was not detected until approximately June 2024.

214. As such, Plaintiffs allege first, the results of the years-log digital and non-digital attacks, followed by allegations as to how the results were achieved.

215. In this case, as of the time of the filing of this lawsuit, the results of the cyber-attack are undeniable in that substantially all of the defined **Ultimate Goals** were achieved, to wit:

(1) Farrow Law was effective closed on July 10, 2024;

(2) Farrow and Farrow Law's communications were and have been persistently and substantially severed;

(3) Farrow and Farrow Law have been financially devastated;

(4) Farrow and Farrow Law's reputation have been destroyed;

(5) Farrow and Dr. Doe have suffered and continue to experience trauma and substantial emotional pain;

(6) Infant Doe suffers through symptoms of trauma manifesting in regressive development;

(7) Farrow and Dr. Doe's lives and lifestyles have retracted and regressed due to emotional trauma;

(8) the quiet enjoyment of Farrow, Dr. Doe and Infant Doe's lives has been utterly uprooted and upended, for example, as nearly all planned social events, or modest family trips out of town or even special days which have been planned for Infant Doe have been substantially interfered with and/or ruined by a situational crisis event manufactured by and through the use of what can only be referred to as the Threat Actor Defendants' invisible yet extremely palatable cyber-fence; and

(9) each and every avenue to seek judicial accountability or communications with law enforcement or attempts to engage legal counsel or to communicate through emails to opposing counsels who appeared for other parties since July 2024 have been thawed through the use of the cyber-network the Threat Actors have constructed.

216. The Ultimate Goals were substantially achieved by each Threat Actor Defendant through the filing of Plaintiffs complaint.

217. The Ultimate Goals were accomplished through strategic planning, operational adjustments and adaptation, all of which left digital imprints within Farrow Law's protected Computers, the Farrow Law Network and registered on open sources, such as ICANN.ORG.

218. The Threat Actor Defendants used the APT model, or a substantially similar sequence structure to achieve their Ultimate Goals.

219. In the pursuit of their Ultimate Goals, the Threat Actor Defendants activities and conduct were and are focused on defense evasion, anonymity and obfuscation.

220. The TTPs utilized by the Threat Actor Defendants in pursuit of their Ultimate Goals, were and are sophisticated and required reasonably seasoned operators with various trainings, by example, individuals with cyber-security defensive and offensive tactics.

221. The use of the TTPs by the Threat Actor Defendants in pursuit of their ultimate goals required substantial initial and ongoing financing, which they paid for, in part and/or in whole, or through providing in-kind services.

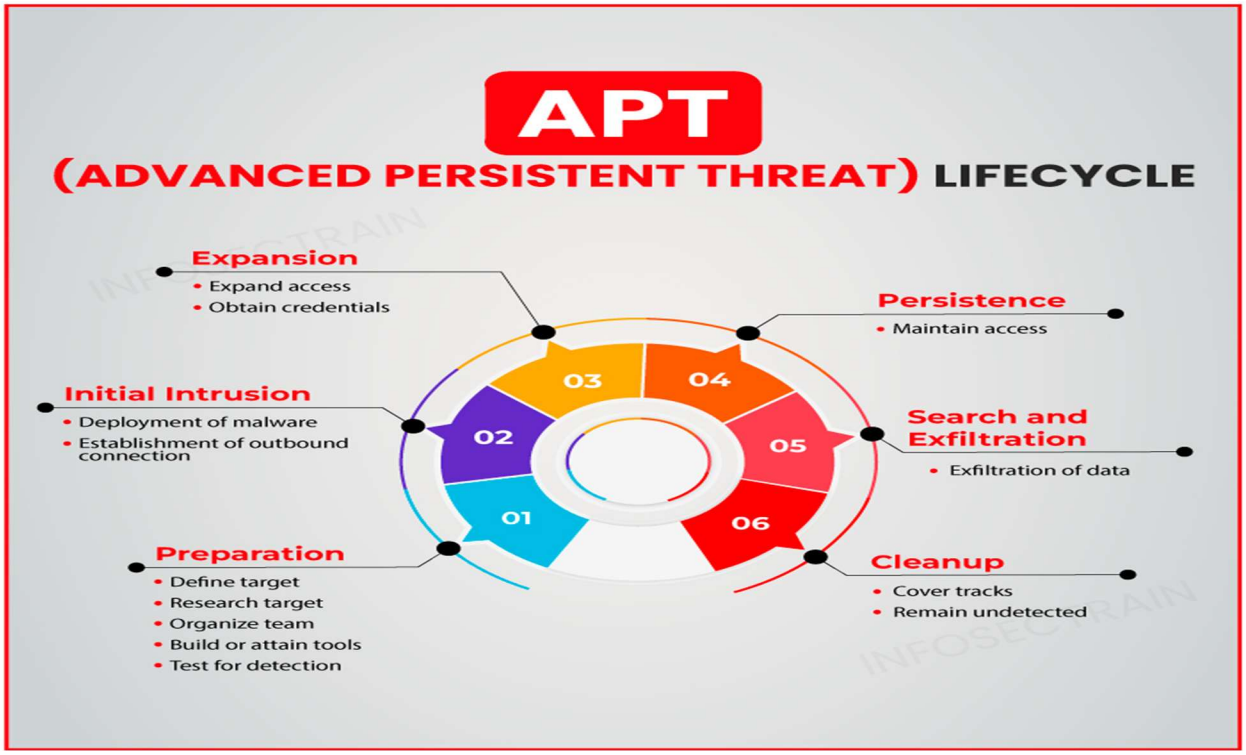
222. The TTPs used by the Threat Actor Defendants for purposes of attempting to, and accomplishing some or substantially all of their Ultimate Goals involved the unauthorized accessing of Farrow, Farrow Law, Dr. Jane Doe and other protected computers used in interstate commerce with the intent to either obtain information, further a fraud and/or damage the computer or its data.

223. The activities and conduct of the Threat Actor Defendants, such as following the APT model and employing a variety of TTPs, caused each individual Plaintiff over $5,000 in one

previous year, and occurred within 2 years of the filing of this lawsuit or was discovered within two years from the filing of this lawsuit.

Accomplishing the Sequence Framework Structures of an APT

224. Plaintiffs allege that the term APT defines the collective conduct of cyber-threat actors over time which track substantially similar activities of other cyber threat actors utilizing at least seven (7), and as many as twelve (12) similar or identical sequence framework structures to achieve their ultimate goals.



225. The Threat Actor Defendants achieved all of the necessary components of an APT.

226. As alleged more specifically hereinbelow, the Threat Actor Defendants planned, executed and achieved all of the sequence framework structures of an APT, for purposes of achieving one or all of their collective or individual Ultimate Goals.

227. The Threat Actor Defendants in this case sourced, employed and/or contracted individuals and/or entities a core team and/or teams and/or freelance cyber-experts, as well as other individuals and/or entities with other expertise, *inter alia,* skill sets and experience in the strategic communication industry to plan, collaborate, implement and/or execute the operations of the APT.

228. The Threat Actor Defendants controlled, directed, ordered, and/or had the ability to exert dominion over the operators of the APT such that the operators, employees and/or contractors' actions were an extension of the activities, conduct and actions of the Threat Actor Defendants.

229. The Threat Actor Defendants and/or the APT Operators worked in concert, with basic and/or sophisticated real-time situational awareness intelligence coordination which provided, for example, feedback and results of, for example, the exploitation, or attempted exploit, of an attack vector.

230. This included the actual sharing of, or the Threat Actor Defendants having direct and/or indirect access to, data and information obtained or retrieved by and through the exploitation and/or attempt exploit of a vector vulnerability.

231. The purpose of sharing ill-gotten and other data and information, or at least providing direct or indirect access to the same, was such to plan and execute future operational activities, to gather intelligence and to share PII to allow other operators to gain unlawful access to protected computers, networks and/or electronic devices such as cell phones to either obtain information, further a fraud and/or damage the computer or its data.

232. In summary, Plaintiffs allege the Threat Actor Defendants accomplished and achieved substantially all the Sequence Framework Structures of an APT in pursuit of their Ultimate Goals, to wit:

233. **Target Selection** – any known APT, as the one created and executed by the Threat Actors in this Case, is not random. Here, the Threat Actor Defendants choose their original targets Farrow and Farrow Law, the attorney and law firm who filed original lawsuit by their client Louis Spagnuolo in May 2019 against Heath Ritenour, John Ritenour and IOA, Inc., alleging they stole IOA Agent commission to line their pockets and to artificially inflate the value of IOA, LLC's stock for personal financial gain.

234. Thereafter, in or about mid-2023, Dr. Jane Doe and Infant Doe were added as targets and they were meticulously selected in part for their strategic value for achieving the Threat Actor Defendant's Ultimate Goals, but also, Dr. Jane Doe was selected as an opportunity presented itself to acquire a financially beneficial position in a project which involved upgrading the hospital and transplant center where Dr. Jane Doe works.

235. **Initial Reconnaissance** - intelligence gathering and extensively researching targets and their associated strategic collateral targets, identifying human and cyber-vulnerabilities and planning strategies for initial access.

236. Here, the Threat Actor Defendants conducted extensive research and gathered substantial intelligence on their targets by: (1) locating, extracting and studying information and date derived from web sites, social media accounts, press releases, publications and blogs belonging to and/or published by Farrow, Farrow Law and Dr. Jane Doe, as well as, those of numerous other selected individuals and entities with connections to Plaintiffs, such as Farrow

Law clients, Farrow Law Staff Members, Dr. Jane Doe, Jackson Memorial Hospital, the Miami Transplant Institute, University of Miami Miller School of Medicine, (2) public records such as previously filed litigation by Farrow and Farrow Law, recorded documents, corporate records, and court records; (3) professional license records; and (4) through directing social engineering activities to Farrow, Farrow Law and Dr. Jane Doe, as well as their business and personal contacts, such as through social media posts, direct messages, posing as 'potential clients' and receiving 'free legal consultations', using phishing and spear phishing emails and text to obtain their Personal Identification Information for strategic purposes and using AI spoofing voice cloned calls in furtherance of their initial and ongoing research since June 2019.

237. **Initial Compromise** – the exploitation of a direct, indirect and blended vector infiltration, such as through highly tailor spear-phishing emails, hyperlinks or text from the target's known trusted sources, exploiting of software vulnerabilities and/or through social engineering. Here, Plaintiffs allege that the Threat Actor Defendants gained initial compromises of protected computer networks, computers and personal devices by using, *inter alia,* spear phishing emails which were designed using the research gathered as to each individual Plaintiff and their personal and business contacts.

238. The spear phishing emails included, *inter alia,* DropBox links and pdfs from opposing counsel under the guise of court filings or document exchanges.

239. These spear phishing emails and text messages also included messages tailored to Farrow and Dr. Doe's business and personal interests, or related to their daily routines which were delivered under the guise of otherwise legitimate sources which, directly or indirectly, carried

malware payloads allowing for initial access vector infiltrations with extremely low to zero probability of detection.

240. **Establishing a Foothold** – Threat Actor Defendants deployed malware through the mechanisms of their initial compromise and subsequent infiltrations to create a backdoor into the network, ensuring they can return even if their initial point of entry is closed.

241. **Lateral Movement** – after gaining a foothold, threat actors move laterally within the network or collateral networks to increase privileges and permissions to more valuable data, systems and/or strategic information which allows the achievement of Ultimate Operational Goals;

242. **Espionage - Exfiltration of Data - Infrastructure Vandalism - Sabotage** – after the threat actors obtain privileges and permissions to access the information, systems, electronic devices and network, their freedoms to maneuver throughout a network are directed to accomplish one or several Ultimate Goals through coordinated and/or compartmentalized micro and/or macro operational mission tasks which, in this case included, *inter alia,*: (1) espionage (monitoring target strategies, tactics and movements for strategic advantages), (2) stealing information, (3) manipulating software and data files; (4) denying access to legitimate users; (5) copying and encrypting confidential business and personal files for exfiltration; (6) sabotaging the Farrow Law Network to cause Farrow Law to effectively close through, *inter alia,* substantial communication interferences, modifying and or rearranging client folders, and causing situational crisis events designed to distract and drain financial and human resources.

243. **Covering tracks** – Throughout the attack, APT actors work to cover their tracks to evade detection, often deleting logs, encrypting stolen data, and using legitimate credentials to blend in with normal network traffic.

THE APT'S TRADECRAFT – the Techniques, Tactics and Protocols

244. The Ultimate Goals of the Threat Actor Defendants' APT governed their use and deployment of certain and specific cyber related Tactics, Techniques and Protocols ("TTPs").

245. That is to say, the Threat Actor Defendants' operational logistics, strategies, architecture, hierarchy of leadership, protocols execution of activities, and the conduct of the Threat Actor Defendants and others working to achieve the Ultimate Goals.

246. In this case, from June 2019 through present, the APT consisted of and continues to consist of numerous digital (cyber) and non-digital (conventional and/or social engineering) schemes directed at Plaintiffs, and numerous other entities and individuals the Threat Actor Defendants and/or their designated team-operators determine strategically advantageous to the operation and the achievement of the Ultimate Goals.

247. Moreover, the TADs conducted the workings of their cyber-operations knowing that, the breath and scope of their operation would require gaining unauthorized access to protected computers, individual electronic communication devices, web domain hosting servers, email servers belonging to Farrow, Farrow Law and Dr. Doe's contacts, such as private organizations, numerous law firms, public organizations, and corporations which served as, for example, vendors of Farrow and Farrow Law.

248. Thus, the TADs conducted their cyber-operations using sophisticated TTPs which were directed at achieving unauthorized access to protected computers, the networks they were connected to, which belonged to Farrow Law and strategically advantageous private and public

organizations and/or individuals such that their unauthorized intrusions would similarly remain undetected.

249. The TADs, for example, used TTPs and other sophisticated strategies such that they could receive and read emails and/or text message communications from Farrow, Farrow Law and/or Dr. Doe, and if strategically advantageous, respond to Farrow, Farrow Law and/or Dr. Doe masquerading and/or impersonating an individual or organization.

250. The Threat Actor Defendants' consistent focus on defense evasion within the Farrow Law Network, was also employed as a protocol such that victims to this communication interference would likely have no means to suspect or detect that the TADs were steering the direction of the communications.

251. Moreover, the TADs planned and executed their cyber-operations to achieve their Ultimate Goals, which included the unauthorized access into protected computers, networks, domain registrars, hosting servers and email servers, such that any infiltration was surgical and hyper-focused, relating only to achievement of their milestones, and sequence framework structures of the APT.

252. Further, the TADs operated and conducted their cyber-operations into hundreds of protected computers and devices without reservation, and achieved their unauthorized access into protected computers, and/or violated the rights of the human beings who operated them using various TTPs with reckless disregard as to the "real-world" and "real-life" consequences.

253. Plaintiffs allege that each manipulation of a person through a social engineering attack, and each instance the Threat Actor Defendants gained unauthorized access by and through the direct and/or indirect actions of the Threat Actor Defendants, they did so from a distance,

remained faceless and nameless to avoid detection, which evidences their sinister and/or malicious intentions.

254. With these open-source records, are corresponding registered activities within Plaintiffs protected computers and other devices, that serve to connect the Threat Actor Defendants to the damages caused to Plaintiffs.

THE APT'S SCHEMES - the Pillers Supporting the Pursuit of Ultimate Goals

255. Here, Plaintiffs allege that the Threat Actor Defendants used approximately 13 TTPs in pursuit of their Ultimate Goals, which form four independent schemes that worked in tandem, and/or specific cyber-tradecraft hacking schemes and non-digital activities since 2019, and these schemes are characterized by:

(1) **UNAUTHORIZED ACCESS TO PLAINTIFFS' PROTECTED COMPUTERS**: the scheme to gain unauthorized access to a protected computer, network, hosting server, and/or email server and/or individual email account belonging to Farrow, Farrow Law and/or Dr. Jane Doe;

(2) **SUPPLY CHAIN ATTACKS**: the schemes to gain unauthorized access to a protected computer, network, hosting server, and/or email server and/or individual email accounts belonging to individuals or entities which belonged to Farrow, Farrow Law and/or Dr. Doe's contacts, vendors, contractors, colleagues, for example, Farrow Law's IT Vendor;

(3) **REMOTE C2 SCHEME**: the schemes to gain strong foothold fortifications and lateral footholds which establish a means to send and receive remote commands, to the target protected computer, device, server or email account;

(4) **DoS SCHEME**: the schemes surrounding the achievement of one or more of the Threat Actor Ultimate Goals subsequent to their Denial of Service ("DoS") Attack upon Farrow Law's Network causing the firm's effective closure on or about July 10, 2024.

TTPs Utilized by the Threat Actor Defendants

256. As the definitions of one or more commonly used TTPs overlap, Plaintiffs hereinafter specifically allege that the TTPs, or Cyber-Tradecraft, or Tradecraft utilized by the Threat Actor Defendants from June 2019 through present, included, *inter alia:*

257. **TRACKING EMAILS/MESSAGES**: The tracking emails sent by the Threat Actor Defendants from at least March 2020 through present, are labeled by deceptive headers and/or subject lines purporting to contain legitimate information from trusted sources.

258. The messages contained an embedded hyperlink that served as a tracking link.

259. If the recipient activated the tracking link by opening the email, information about the recipient, including their location, IP addresses, network schematics and specific devices used to access the pertinent email accounts, was transmitted to a server controlled by the Threat Actor Defendants.

260. The Threat Actor Defendants used and used this method to enable more direct and sophisticated targeting of recipient's' home routers and other electronic devices.

261. **SECOND STAGE MALWARE**: Tracking and Phishing Emails and Text Messages may deliver a sophisticated malware payload, In other words, these emails contained a malicious attachment and/or link designed to install malware on the recipient's protected computer, and that initial malware was designed to facilitate the installation of a second stage of

malware which is uploaded through, in some cases, the exploitation of a vulnerability discovered with the information illegally obtained by the tracking link malware.

262. The Threat Actor Defendants successfully and repeatedly gained access to the Farrow Network, its individual computers (such as Farrow's Lenovo Laptop), and cell phone devices exploiting the intelligence gathered by initial tracking emails such as its individual IP address, owner and location to deploy second stage malware.

263. From approximately January 19, 2021 and at least by March 18, 2021, the Threat Actor Defendants implanted Second Stage Malware which was used to install seemingly otherwise legitimate executable files to side-load malicious malware such as Dynamic Link Library ("DLL") files, which decrypted and execute malware payloads, or implants, on the victim's machines.

264. In so doing, the Threat Actor Defendants' implants established secure connections (fortified footholds) in FLF's Network, Farrow's computer, Dr. Jane Doe's computer and other strategically targeted networks, protected computers and/or devices by and through using accounts or servers controlled by the Threat Actor Defendants to receive and execute commands on the victim machines, as further described, *infra.*

265. **DEFENSE EVASION**: From at least December 2019 through June 2024, the Threat Actor Defendants used TTPs to avoid detection in the Farrow Law Network, as well as other collaterally strategic networks and the protected computers connected therewith using a variety of methods.

266. For example, the Threat Actor Defendants disabled or uninstalled security software and exploited vulnerabilities in trusted processes to hide and masquerade their malware. As further alleged herein, they also used DNS Tunnelling, hid various artifacts, including system files and

administrative task execution to circumvent the disruption of user work environments and prevented legitimate users of the Farrow Law Network and other networks, from changing files or features on the system.

267. In this way, the Threat Actor Defendants hid user accounts, files and directories – all of which allowed them to remain undetected as they navigated, monitored and ultimately exfiltrated and stole confidential information.

268. At the very least, the TADs remained undetected from the commencement of their APT Attack through the effective closure of Farrow Law on July 10, 2024.

269. Moreover, the TADs conducted the workings of their cyber-operations knowing that, the breath and scope of their operation would require gaining unauthorized access to protected computers, individual electronic communication devices, web domain hosting servers, email servers belonging to Farrow, Farrow Law and Dr. Doe's contacts, such as private organizations, numerous law firms, public organizations, and corporations which served as, for example, vendors of Farrow and Farrow Law.

270. Thus, the TADs conducted their cyber-operations using sophisticated TTPs which were directed at achieving unauthorized access to protected computers, the networks they were connected to, which belonged to Farrow Law and strategically advantageous private and public organizations and/or individuals such that their unauthorized intrusions would similarly remain undetected.

271. The TADs, for example, used TTPs and other sophisticated strategies such that they could receive and read emails and/or text message communications from Farrow, Farrow Law

and/or Dr. Doe, and if strategically advantageous, respond to Farrow, Farrow Law and/or Dr. Doe masquerading and/or impersonating an individual or organization.

272. However, the other victims to this communication interference would likely have no means to suspect or detect that the TADs were steering the direction of the communications.

273. Another example of the TTPs, would be to hijack a domain, mirror it and direct certain traffic to their malicious website, yet as in the case with the interference with email communications, the owner of the website, even a law firm, would continue to receive regular communications and web traffic such that it would never appear that the TADs had used their cyber-systems or emails.

274. **Email Hiding Rules** – as part of their Defense Evasion and to support their Man-in-the-Middle Attacks, the threat Actor Defendants used email rules to hid inbound emails in, for example, one of Farrow Law's staff's compromised email boxes, or for example those belonging to counsel for Nationwide Insurance, the Roig Law Firm.

275. In this case, the Threat Actor Defendants gained access to approximately 34 law firms, and over 22 of Farrow Law's client's email accounts and thereafter created inbox rules for various email functions, including moving emails to other folders, marking emails as read or deleting emails.

276. **ADVANCING PRIVILGES AND PERMISSIONS**: From at least March 2020, the Threat Actor Defendants typically sought to convert their initial access into long-term, persistent access using several methods, including, *inter alia,* installing sophisticated Remote Access Trojan ("RAT") malware, "webshells" which provided unauthorized access to victim

networks through compromised web servers, and unauthorized Virtual Private Network ("VPN") software on compromised computers.

277. **Services File Permissions** – From March 2021 through June 2024, the Threat Actor Defendants were successful in executing their malicious malware payloads through hijacking the binaries used by services.

278. In other words, from March 2021, but at least from August 2022, the Threat Actor Defendants exploited known vulnerabilities in the permissions of Microsoft Windows services to supplant the binary that is executed upon service start.

279. As these system processes routinely execute precise binaries as a component of their functionality, or, for example, to perform other actions should the permissions on the file system directory containing a target binary be improperly configured, the Theat Actor Defendants exploited the same by overwriting the target binary using another binary using user-level permissions executed by the original process.

280. And, in several cases, since the original process and thread were running at a higher permission level, the result, i.e. the Threat Actor Defendants' implant replacement binary, also executed under higher-level permissions – which included the critical SYSTEM.

281. **DLL Search Order Hijacking** – from March 2021, the Threat Actor Defendants executed their own malicious payloads of malware by hijacking the order in which DLLs are loaded.

282. Here, the Farrow Law's Microsoft OneDrive Network System used a common method to search for required DLLs to load a program, and by hijacking DLLs loads and modifying the search order, the Threat Actor Defendants not only established strong foothold fortifications,

but they also used this to elevate privileges and permissions within the Farrow Network and other collaterally strategic networks and the protected computers connected therewith.

283. **COMMAND AND CONTROL SERVERS ("C2 SERVERS")**: The Threat Actor Defendants, *inter alia,* worked to and gained control over "domain controllers", a/k/a Command and Control Servers ("C2 Servers") servers which were and are used to control the malware and communicate with compromised protected computers.

284. This access was used to facilitate widespread access to computers that are members of the corporate domain.

285. Upon information and belief, The Threat Actor Defendants used, directly or indirectly, at times material hereto, from at least March 2020, the following, without limitation, C2 Servers:

- **X.NS.JOKER.COM;**
- **Y.NS.JOKER.COM;**
- **Z.NS.JOKER.COM;**
- **AUTHNS1.QWEST.NET;**
- **AUTHNS2.QWEST.NET;**
- **NS1.SITEGOUND.NET;**
- **NS2.SITEGROUND.NET;**
- **UDNS1.ULTRADNS.NET,**
- **UDNS2.ULTRADNS.NET;**
- **RESOLVER1.QWEST.NET;**
- **EWARTTECHNOLOGIES.NET**
- **DIGICERT.COM**
- **WINDIX.COM**
- **WORLDNIC.NET**

286. **APPLICATION LAYER PROTOCOL: DNS TUNNELING** – From approximately March 2021, and at least from August 2022 through July 2024, the Threat Actor

Defendants, *inter alia,* established footholds within the Farrow Network, and used the Domain Name System ("DNS") application layer protocol to avoid detection.

287. In this way, the Threat Actor Defendants communicated with C2 Servers and sent commands to the remote system embedded in existing protocol traffic between the server and Farrow Law. The DNS protocol serves an administrative function in computer networking and DNS traffic is commonly permitted prior to network authentication.

288. Moreover, DNS packets contain several 'fields' and headers in which data can been concealed.

289. In this case, the Threat Actor Defendants' sophistication and experience allowed them to hide their communication with the Farrow Network and other networks and protected computers connected to those networks such that their communication and remote commands could be executed in the targeted victim's protected computer without being detected as the same mascaraed as normal expected traffic.

290. The purpose of this TTP employed by the Threat Actor Defendants was especially significant with respect to the 34 law firms whose networks, hosting servers and/or email servers were used for malicious purposes, and using DNS tunnelling was one, but not exclusively, a means to manipulate, by example, communications between Farrow, Farrow Law and Dr. Doe with third parties.

291. **BLUEBORNE CYBER ATTACK: APT MANUVERS OVER BLUETOOTH** – From at least August 2022, the Threat Actor Defendants used Farrow, Farrow Law and Dr. Doe's protected computers, and/or electronic devices and/or Bluetooth features in their motor vehicles, by example, to exfiltrate over Bluetooth rather that one of their C2 Channels.

292. In this way, due to the proximity of Farrow and Dr. Doe's protected computers to Bluetooth devices, even a home Bluetooth music speaker, and in light of the fact that these devices were not as secured as the primary internet channel at their residence or at Farrow Law's office, also, since they were routed through a different enterprise network, the Threat Actor Defendants sent commands to transmit encoded information from the infected system over a Bluetooth protocol which allowed them to avoid detection and creating a redundant channel for purposes of executing APT maneuvers and the sequence framework structure of exfiltration.

293. **COMMAND AND CONTROL DEAD DROPS ("C2 DEAD DROPS")**: The Threat Actor Defendants also used more advanced tradecraft, including command-and-control web pages which the conspirators created using legitimate websites, and which cybersecurity professionals refer to as "C2 Dead Drops."

294. These web pages, including "profile" pages on legitimate websites, were surreptitiously encoded with the internet protocol ("IP") addresses of C2 Servers.

295. 2 Dead Drops using websites that were and are otherwise commonly used in the legal community and/or of interests to Farrow and Farrow Law, and/or their staff, business associates and colleagues.

296. In this case, the Threat Actor Defendants used, *inter alia,* sanyiabooth.org, lawsinflorida.com, intelligenceonline.com, and 18judicial.org as C2 Dead Drops.

297. **COMMAND AND CONTROL DOMAINS ("C2 DOMAINS")**: The Threat Actor Defendants also registered and/or acquired malicious domains, a/k/a command and control domains (C2 Domains). These C2 Domains were and are pre-selected domain names which

impersonate legitimate domain names and are used to control malware and communicate with the Threat Actor Defendants' C2 Servers.

298. For example, the Threat Actor Defendants preselected and acquired domain names nearly identical to Farrow Law's IT Vendor, and otherwise impersonated legitimate domains of the 18th Judicial Circuit of Florida, at least three 'opposing counsel' law firms with active litigation with Farrow Law, Jackson Memorial Hospital and others which facilitated their communication with the malware they installed so as to accomplish the theft of information, destruction of evidence and effectively close Farrow Law and/or otherwise achieve their Ultimate Goals.

299. **STOLEN CODE SIGNING CERTIFICATES**: The Threat Actor Defendants' tradecraft also included other sophisticated methods, including using stolen code signing certificates to cryptographically "sign" malware, which fraudulently cloaked malware to be legitimate software authored by legitimate software providers.

300. **SUPPLY CHAIN ATTACKS**: Their tradecraft also included supply chain attacks carried out using a variety of advanced techniques, including the use of encrypted malicious payloads that would only be decrypted if they were installed on computers operated by the targets of their APT, to wit: Farrow, Farrow Law and Dr. Jane Doe. An example of the Threat Actors Using a Supply Chain Attack was through their compromising of protected computers and the network of Farrow Law's IT Vendor.

301. **SITTING DUCK ATTACK**: Commencing in 2019, one of the Threat Actor Defendants vector infiltrations of FLF's Network and those of strategic collateral networks, had been the utilization of the "Sitting Duck" Domain Cyber Attacks.

302. Sitting Duck Attacks allow the claiming of a web site domain, or a named server domain, without having access to the owner's account at the Domain Name System ("DNS") provider or registrar.

303. In Sitting Duck Attacks, cyber threat actors exploit configuration deficiencies at the registrar level, as well as, *inter alia,* insufficient ownership verification by DNS providers.

304. Sitting Duck Cyber Attacks have been and continue to be easier ways for cyber-threat actors to hijack domains than any other method.

305. From 2019 through present, the Threat Actor Defendants have utilized Sitting Duck Attacks by exploiting the necessary conditions of the attack which they, upon information and belief, discovered through research online sources.

306. More specifically, the Threat Actor Defendants, from 2019 through present, researched and discovered the website domains Farrow and Farrow Law, their staff, business associates, legal colleagues, opposing counsel and even their own attorneys have, use and/or interact with, as well as the hosting server domains which have been assigned to those web sites domains.

307. The Threat Actor Defendants identified over two hundred (200) domains (which have been discovered through the filing of this complaint) which the registered domain used or delegated authoritative DNS servers to a provider other than the registrar, or the authoritative name server could not resolve queries because it lacked the information about the domain (lame delegation) and/or the DNS provider allowed for claiming a domain without verifying ownership or even requiring access to the owner's account.

308. Once the Threat Actor Defendants exploited the vector, they were able to change administrative credentials, ownership details or the authoritative servers which host the domain, and in some instances, use their advanced administrative permissions to extend the attack into the email servers of these collateral targets.

309. Once there is a change made as to administrator, ownership or to which servers the domain points to, the official DNS records of the domain record an "update" which can be found through scores of open sources, with the official records being stored with "ICANN.ORG."

310. The Threat Actor Defendants in this case used Sitting Duck attacks at the commencement of the APT.

311. Additionally, in the substantial majority, over 90% of instances where one of these website domains, server hosting domains or email servers were updated, the same reflected that the same was for just less than a year - which does not reflect an extension of domain ownership.

312. In some cases, such as with several of the Carrier Defendants' attorneys of record in the 2024 federal case, the Threat Actors exploited 'lame' domain designations to interfere with Farrow's communications with opposing counsel – especially the few whom wished to resolve the claims against their client in June 2024.

313. In the case of interference with opposing counsel or any vendor, client or even Farrow's own attorneys, the sitting duck attack allowed the Threat Actors to intercede in email communications, utilizing what is referred to as the Man-In-the Middle Attack – being capable of receiving, reading, blocking or responding to an email as if they were either Farrow or an opposing counsel or a vendor.

314. In other cases, the sitting duck attack, allowed the Threat Actors to clone a website, such as Farrow Law's IT Vendor's site, to make it impossible to communicate with them especially in May, June and July 2024, and also fake the vendor's website such that requests for help actually go nowhere and, additionally, the website provided false information related to telephone numbers and email addresses.

315. **MAN-IN-THE-MIDDLE ATTACKS**: The Man-in-the-Middle Attack ("MitM") is a form of cyberattack which exploits weak web-based protocols, allowing threat actors to insert themselves between individuals or entities in a communication channel, and in this case, the Threat Actor Defendants used this form of attack to steal data, PII, interfere with communications, create situational crisis events to cause emotional distress and drain human and financial resources, and maliciously use unauthorized access to protect networks and computers in furtherance of the Ultimate Goals.

316. In this case, the Threat Actor Defendants utilized, directly or indirectly, at least three (3) identifiable MitM methods in pursuit of their Ultimate Goals.

317. Based upon the review of Farrow's Lenovo computer, and the outlook application, upon information and belief, all or substantially all of Farrow and Farrow Law's clients' communications were compromised through a form of MitM Cyber Attack as of June 2024.

318. **MitM Email Hijacking**: The Threat Actor Defendants used various means and methods to obtain the login credentials of email accounts belonging to, *inter alia,* Farrow Law's employees, clients, opposing counsel, judicial staff, Florida Bar employees, investigators and Staff attorneys and thereafter used their access for malicious purposes such as to advance privileges and

permissions within the respective organizations' network, individual computers and individual communications devices such as cell phones, iPads and android tablets.

319. **MitM Wi-Fi Eavesdropping**: Wi-Fi Eavesdropping commonly occurs by threat actors to lure victims into connecting to a nearby wireless network using, for example, a legitimate sounding name such as a nearby business, educational institution or 'free' hotel guest Wi-Fi connections.

320. In this case, on or about at least December 2022, the Threat Actor Defendants used the MitM Wi-Fi Eavesdropping Attack using unauthorized access to their respective computers, cell phones and emails to set up Wi-Fi hotspot accounts for their personal vehicles.

321. Between at least 2022 through August 2024, Farrow and Dr. Doe's cell phones routinely connected to these Wi-Fi hotspots, as did the protected computers in their home and the 'smart' devices, such as the 'Owlet' baby monitor in their home using Bluetooth connections (see Blue Bourne Attack description hereinbelow).

322. With respect to the Owlet baby monitor, the same recorded video and audio of Infant Doe from August 2022 through approximate June 2024, and was able to pick up and record audio from around Farrow and Dr. Doe's home which included, *inter alia,* their conversations.

323. **MitM DNS Spoofing**: This attack vector primarily relates to the utilization of the Sitting Duck Attack exploit of, *inte alia,* misconfigurations of a web-domain and its hosting servers. Also known as DNS cashe poisoning, DNS Spoofing occurs when threat actors cause updates to a domain's DNS through manipulations of ownership and/or admin records, and allows for the diversion of legitimate online traffic to a face or spoofed website built to resemble a website the user would likely know and trust.

324. Here, the Threat Actor Defendants used the MitM DNS Spoofing, *inter alia,* to create situational crisis and/or circumstances under which Farrow and/or Farrow Law's staff, or other users would be convinced to take specific action.

325. More specifically, in this case, the MitM DNS Spoofing of Florida's ePortal Authority resulted in Farrow and Farrow Law being prompted to pay court costs for the issuances of summons to the Carrier Defendants in the 2024 Family Circuit Case over and again, only for the same to be rejected by Florida's eFiling portal for the payment of summons by the Clerk of the 11th Judicial Circuit, which prevented Farrow, Farrow and Dr. Doe from obtaining issued summons to serve various defendants; as well, DNS Spoofing was used by the Threat Actor Defendants to have Farrow and Farrow Law submit repeated requests for support from their IT Vendor in June and July 2024 with those requests being submitted into a spoofed website and never received by their IT Vendor.

326. **ZERO DAY CYBER ATTACKS**: From at least March 2020, the Threat Actor Defendants used the Zero-Day Privilege Escalation Exploits cited herein – i.e. vulnerabilities in a computer system the Threat Actor Defendant hackers became aware of prior to, for example, a CVE being issued by NCIA and/or efforts by a vendor to patch (or fix) the vulnerability.

327. Moreover, the Threat Actor Defendants used Zero-Day attacks as the same intentionally exploited a "real-world" vulnerability, that is to say, Zero-Day attacks seized on the reality that, unlike a large corporation or governmental agency, Plaintiffs did not have the teams or departments which employed "white-hat" hackers, or conducted "RED-TEAM - - BLUE TEAM" Pen-Testing exercises searching for undiscovered software vulnerabilities.

328. In short, the Threat Actor Defendants knew that using Zero-Day attacks further diminished the extremely low chance that their massive and persistent operation would be discovered before they achieved their Ultimate Goals, and using an attack vector which avoids detection by the most sophisticated cyber-security systems lessened the possibility of 'getting caught' even further while paradoxally the implantation of this malware through a Zero-Day exploit created strong foothold fortifications which progressively advanced permissions.

329. **PREVIOUSLY IDENTIFIED CYBER-EXPLOITATIONS**: In this case, the Threat Actor Defendants also exploited previously identified security vulnerabilities with respect to their profound shift in operational recalibrations after February 2024, such as Sitting Duck Cyber Attacks, and previously issued NCIA CVEs.

330. In this way, the Threat Actor Defendants avoided using their own or otherwise distinctive identifying malware which, upon information and belief, included the exploitation of security vulnerabilities identical or substantially similar to CVE2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE2019-1653, CVE-2020-10189 and others.

331. **SOCIAL ENGINEERING**: Sitting Duck, Man-in-the-Middle, and Zero-Day Cyber-Attacks, along with Social Engineering, successfully and unlawfully allowed the Threat Actor Defendants to steal Personal Identification Information ("PII"), including login credentials belonging to individuals who had administrative access to FLF's Network and others deemed strategically valuable to the Threat Actor Defendants.

332. After procuring this information, the Threat Actor Defendants persistently and routinely and unlawfully used their expanded access to accomplish the goals of the intrusion, such

as the theft of data, through persistent repetition of the above named digital and non-digital means and methods.

333. The Threat Actor Defendants achieved, through an array of methods, permissions to create new user accounts on FLF's Network which were 'birthed' with shared admin privileges and permissions, allowing the Threat Actor Defendants Command and Control status as early as late 2020 or mid-2021.

334. These compromises typically resulted in the installation of widely available Remote Access Trojan ("RAT") malware within FLF's network or the networks of its lawyers, opposing counsel, the Florida Bar and Florida's eFiling portal allowing for the carrying on of persistent unlawful conduct without any meaningful probability of detection.

335. The Threat Actor Defendants also used FTI to register fraudulent communications and social media accounts.

336. The Threat Actor Defendants also used those accounts to conduct target research and to engage in other activities to support their hacking.

V. QUALIFICATIONS OF THE THREAT ACTOR DEFENDANTS:

- **The Theat Actor Defendants Were and Are the Individuals and Entities Who Had and Have the Core Team of Trained Operatives, Experience, Sophistication and Motivation to Plan, Execute, Operate and Persistently Maintain the APT Attack**

337. APTs are specifically classified by several identifying qualifiers, however, only two are fundamental.

338. As to those two qualifiers, the ability to source the operators, teams and contractors who could technically achieve perpetrating the operational plan, maintain persistent movement

through the sequence framework structures of an APT and the financial ability to fund a long-term persistent attack.

The Technical Qualifications of the Threat Actor Defendants

339. FTI's website, its published articles and the profiles of some of FTI's team, specifically identify that it has the experts who work in 'core' teams, are well-trained, experienced, well-funded, organized, and capable of utilizing a range of techniques, tactics and procedures ("TTP Tradecraft") with respect to a plethora of technologies, social engineering, psychological operations, data extraction and sabotage.

340. FTI touts that it has former intelligence, law enforcement or national security officers, agents and/or assets who have field experience and intensive trainings in deploying offensive and defensive actions in real world situations related to APTs and SAPTS.

341. FTI's own claims and statements specifically spell out that their core teams can be deployed anywhere in the world as part of a rapid response squad of crisis managers to create, architect, and execute complex strategies with embedded multi-level redundancy to stabilize a corporate execute crisis.

342. FTI's also represents that it is able to establish and implement strategic communications and do whatever is necessary to "**hunt threats**" such that they are neutralized.

Cybersecurity Capabilities & Offerings

A STRATEGIC APPROACH TO INTELLIGENCE-LED CYBERSECURITY

An intelligence-led, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

FTI Consulting's cybersecurity business is engineered to synthesize cutting-edge, intelligence-led capabilities around a trusted core of comprehensive offerings. This enables clients of any size to address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs to address cyber threats.

We build a safer future by helping organizations understand their own environments, harden their defenses, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident. Our seasoned experts bring deep technical and practical experience to the delivery of these solutions. Our industry experience across forensic investigations, strategic communications, expert testimony, and managed network defense operations, empowers FTI Consulting to meet a full range of technical needs across the globe.

FTI CONSULTING'S CORE CAPABILITIES & OFFERINGS

ASSESS and Understand Your Environment:
Managing cybersecurity risk begins with developing an organizational understanding of your business environment and its assets. We conduct assessments that inform the development of strategies to manage and mitigate cybersecurity risk to your systems, assets, data, and capabilities.

DEFEND Your Assets and Infrastructure:
The deployment of network safeguards is critical. We identify, implement, and manage defensive best-practice processes including access control, awareness and training, data protection policies, network maintenance, and deployment of protective technologies. Through these defensive measures, we ensure the delivery of your critical services and operations.

IDENTIFY Threats Rapidly and Proactively:
Timely discovery of impacts to your network can be a key factor in minimizing damage. By implementing continuous security monitoring and advanced detection processes on your networks, FTI Consulting experts can detect anomalies and other security-related events rapidly and proactively.

RESPOND to an Incident Holistically:
Once you detect a cybersecurity incident, you must take action. We provide complete cyber incident response options that include planning, analysis, mitigation, system refinements, and ancillary mission support functions, such as strategic communications and reputation management.

RECOVER Operations Quickly and Sustainably:
Restoring capabilities or services that have been impaired is often your top priority when you face a cybersecurity incident. We develop recovery plans that ensure long-term improvement, limit the potential lasting impacts of cyber incidents, and prevent damage from future incidents. With our recovery assistance, you can get back to business as usual, as soon as possible.

FTI CONSULTING | CYBERSECURITY

343. Here, the Threat Actor Defendants successfully achieved the operational goals of SAPT by eliminating Farrow and Farrow Law as a threat in July 2024.

344. FTI claims to have numerous former national security officials as Managing Directors with specific experience with APTs:

FTI CONSULTING

FTI Consulting Bolsters Cybersecurity Practice Globally with Three Appointments

Nathan Mousselli, Chris Pluhar and Dawit Kim Deepen Cybersecurity Incident Response and Complex Investigations Capabilities

Washington, D.C., May 5, 2021 — FTI Consulting, Inc. (NYSE: FCN) today announced the appointment of three professionals to its Cybersecurity practice, continuing the firm's global investment in its capabilities to help companies, law firms and governments with proactive and reactive cybersecurity measures.

The new appointments include Nathan Mousselli, who joins as a Managing Director in New York, Chris Pluhar, who joins as a Senior Director in Los Angeles, and Dawit Kim, who joins as a Director in Singapore. Collectively, the experience of this group will enhance the incident response and complex investigations capabilities of the Cybersecurity practice.

Mr. Mousselli is an expert in cybersecurity, digital forensics and incident response. He is a former special agent with the U.S. Department of Homeland Security ("HSI") in the New York Cyber Division, where he provided expert testimony in addition to leading and supervising computer and network forensics, incident response, national security, child exploitation and financial sector investigations.

Mr. Pluhar has over 25 years of U.S. government service, with expertise in technical investigations; large-scale, complex multiagency cases; and international investigations. He joins FTI Consulting from the Federal Bureau of Investigation, where he served as a supervisory special agent and led complex cyber investigations with a national security and advanced persistent threat focus.

345. Other "Managing Director's" profiles on FTI's website, such as 'Managing Director' Sara Sendek specifically state they have experience 'navigating a variety of complex cyber incidents involving data theft and extortion….and advanced persistent threats ("APTs")":

346. Another example of a FTI Managing Director having experience with advanced persistent threat actors is David J. Youssef:

347. Managing Director Harald Hertel is claimed to have "managed cyber incident readiness and response projects, including an advanced persistent threat ("APT") case for more than nine months…"

348. In 2018, one of FTI's most prominent experts on APTs, and a former FBI Special Agent, prepared an expert report which was filed in federal court.[10]

349. In this expert report, this FTI expert provides a compressive analysis as to how FTI was able to detect, track and follow an APT threat actor who targeted Sec. Hillary Clinton's campaign manager such as to provide their clients with a substantial defense to a lawsuit filed against them for defamation by the alleged threat actors.

350. This expert report provides the means, methods, tactics, tools, and sources FTI experts purportedly use to identify an APT threat actor.

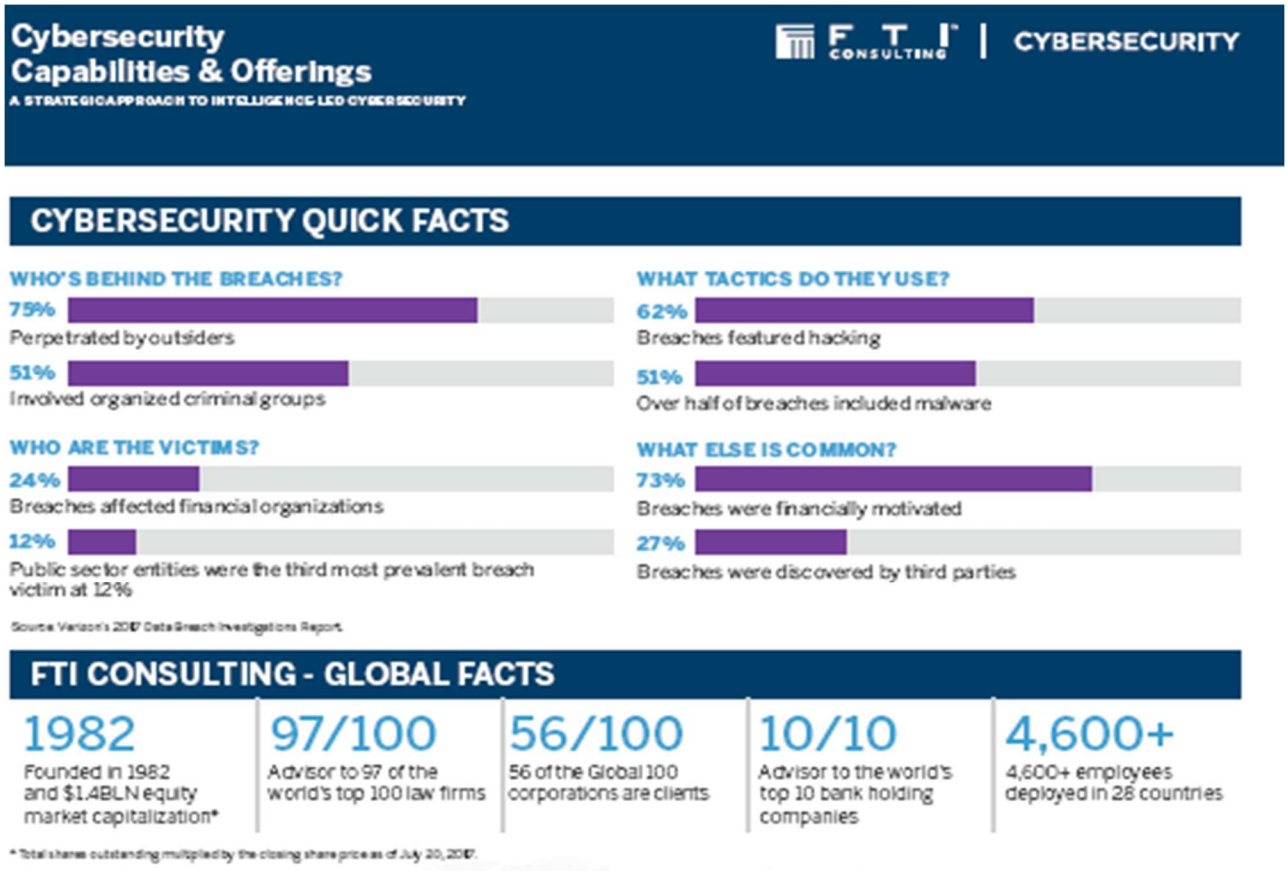
351. The expert report also demonstrates FTI's knowledge of numerous types of vector infiltrations used by APTs from 2012 through 2018, and how FTI experts could, once retained, locate or identify within a reasonable degree of certainty, as to who was behind an APT, what servers the APT threat actors used, the level of sophistication of the operatives, and, as well, provide scores of open source websites which provide information as to hackers and threat actors shared by official government agencies, or private security firms.

352. On July 25, 2024, after FTI had been the subject of two emergency motions alleging that Farrow and Farrow Law were experiencing massive coordinated cyber-attacks coming from multiple directions, and that FTI was highly likely to be the central perpetrator, FTI did not deny Farrow and Farrow Law's allegations that it was behind a comprehensive cyber-interference

[10] A copy is appended hereto marked Ex "D".

campaign, nor did it state it had engaged in any investigation itself to defend against Farrow and Farrow Law's allegations.

353. FTI's publications from over five years ago claim that over half of the major cyber-attacks throughout the globe emanate from organized criminal organizations:



The Threat Actor Defendants' Financial Qualifications

354. From 2019 through Present, the Threat Actor Defendants paid, funded, and incurred the financial costs for their APT, in whole or in part, and at various times for the common purpose of achieving the Ultimate Operational Goals as defined herein.

355. From 2019 through 2024, IOA, Inc.'s posted and reported on its website that its yearly revenues averaged approximately $230MM.

356. From 2019 through 2024, Heath Ritenour received over $3MM as insurance commissions from the TLE Account, exclusive of other revenue from other insurance account which he is either the lead producer or co-producer.

357. From 2019 through 2024, John Ritenour received over $1.5MM as insurance commissions from the TLE Account, exclusive of other revenue from other insurance account which he is either the lead producer or co-producer.

358. In 2024, Heath Ritenour received over $1MM as insurance commissions from the TLE Account,

359. In 2023, John Ritenour received over $1MM as insurance commissions from the TLE Account, exclusive of other revenue from other insurance account which he is either the lead producer or co-producer.

360. From 2019 through 2024, FTI's reported profits averaged over $1Billion per year, and its total market capitalization for those years averaged approximately $4Billion ending with close to $9Billion in 2024.

361. From 2019 through 2024, Defendant Steven Gunby's has been FTI Consulting's CEO and during that time his base annual salary averaged over $3,400,000 per year. In 2024, Gunby's based annual salary was over $6,000,000 per year.

362. In May 2024, according to records filed by Gunby with the Security and Exchange Commission, Gunby sold over $10,000,000 in FTI stock.

363. The Threat Actor Defendants Heath Ritenour, John Ritenour, IOA, Inc. FTI Consulting, Inc., and Steven Gunby directly or indirectly, financially contributed to the APT digital and non-digital activities and attacks against Plaintiffs.

VI. THE APT TIMELINE

February 2019 through March 2023- Target Selection, Research Gathering, Sourcing Social Engineering Identities, Testing Vulnerabilities, Initial Access and Fortifying Footholds

Target Selection -

364. On May 9, 2019, Farrow and Farrow Law filed a lawsuit on behalf of Spagnuolo in Broward County Circuit Court against IOA, Inc. its co-founders, John Ritenour and Valli Ritenour, and one of Defendant John's companies, 1188 Partners, LLC ("1188 Partners") ("2019 Spagnuolo Case").

365. The Lawsuit alleged that the Ritenours, IOA, Inc., and 1188 Partners defrauded Spagnuolo out of substantial past and continuing insurance commissions related to a very large account ("TLE Account"), and that the theft of Spagnuolo's monies, along with those of other IOA Agents, was in furtherance of an ongoing PONZI Scheme conducted by Heath Ritenour and John Ritenour with respect to IOA, LLC's private stock valuations.[11]

366. Within weeks of the 2019 Lawsuit being filed, in June 2019, Defendant John Ritenour caused one of the key witnesses for in the 2019 Spagnuolo Case to be intimidated for purposes of interfering with, thawing or dissuading the witness from participating further in the

[11] The 2019 Lawsuit alleged that the Ritenours had created the classic PONZI scheme, with new purchasers of IOA stock buying at the highest price, while the agreement to purchase the stock prohibited liquidation until the individual retired, quit working for IOA or was terminated and even then, the payout was over a period of 5 years.

lawsuit as the witness had provided a statement corroborating Spagnuolo's factual allegations which was attached to the original complaint.

367. Prior to, and after the commencement of the 2019 Spagnuolo case, Defendant Kolaya represented the Ritenours, IOA, Inc., and a limited liability company John Ritenour used for purposes of collecting commissions from the TLE Account.

368. By at least late June 2019, Farrow and Farrow Law were the targets of an offensive campaign and strategy being developed and planned by FTI and Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, 1188 Partners and/or JKR Professional, LLC ("JKRP, LLC").

369. In or about March 2020, Farrow and Farrow Law became targets of Strategic Alliance Partners Joe Taylor Restoration, Inc., and Joseph Clifford Taylor ("Taylor") (collectively the "JTR Partners") after Farrow and Farrow Law had undertaken the representation of the two former employees of JTR after they were sued in Palm Beach Circuit Court for alleged violations of their employment agreements.

370. From March 2020 through present, the IOA Defendants and the JTR Partners are and have been aligned with respect to carrying out digital and non-digital activities as against Farrow and Farrow Law, as well as, as against Dr. Doe and Infant Doe after they became selected Targets in or about March 2023.

Researching Targets, Gathering Intelligence, Initial Social Engineering Campaigns and Development of Stolen and/or Fictious Social Media Profiles

371. FTI's and its corporate crisis management and strategic communications services involve the manipulation of human decision making and conduct, also known as social engineering.

372. Plaintiffs allege that FTI's social engineering research, development and testing began with respect to them, their associates, colleagues, family members and staff, by at least September 2019.

373. The Threat Actor Defendants initial social engineering campaigns used Tracking Emails, Phishing Emails, Spear Phishing Emails, and/or by sending spear phishing social media messages on Facebook to some of Farrow's friends and followers.

374. Upon information and belief, Farrow and Farrow Law and/or its staff opened a pdf and/or a link in or about November 2019, which delivered a highly undetectable malware payload in or about December 2019.

375. By January 2020, the direct and indirect messages sent to Farrow, Farrow Law and others increased substantially, yet remained undetected.

376. In and around July 2019, during the research and intelligence gathering sequence framework structure of the APT, in addition to research their Targets, the Threat Actor Defendants located strategic social media identities which they would use in future social engineering activities for procuring PII from Farrow and Farrow Law's staff, family, friends and colleagues.

377. In or about 2019, FTI had procured, as part of its regular way of conducting its business, scores of old social media accounts which are available for purchase online that have established connections, followers and verified credentials.

378. As it relates to this case, FTI and the other Threat Actor Defendants purchased, acquired or stole through procuring the PII of the original owner, LinkedIn and other social media profiles which had been opened for at least 5 years and in most cases over longer periods of time for purposes of creating the illusion that the fictitious profile was a legitimate human working in a

particular field or trade by erasing the original creator's profile and building a new one designed for social engineering purposes.

379. On September 26, 2019, an Amended Complaint was filed in the Spagnuolo Lawsuit which included allegations, *inter alia,* of felonious witness tampering and/or harassment, wire fraud and mail fraud as predicate acts to a Civil Racketeering Conspiracy and regular way of conducting the affairs of that certain Racketeering "RICO" enterprise.

380. On November 8, 2019, Attorney Joshua Clark and the Law Offices of Joshua Clark, P.A. filed the case styled: *TNC Holdings US, LLC and J. David Naughton IV v. Insurance Office of America, Inc., et. al.,* In the Circuit Court for the Eighteenth Judicial Circuit In and For Seminole County, Florida Case No: CACE2020CA001019 ("Naughton Lawsuit"). Farrow and Farrow Law would substitute in as counsel for Plaintiffs in the Naughton Lawsuit in June 2020.

381. On or about January 24, 2020, Farrow and FLF caused to be filed the case styled: *Roy Caswell v. Insurance Office of America, Inc. et. al.*, In The Circuit Court For The Seventeenth Judicial Circuit In and For Broward County, Florida: Case Number: CACE20001518 ("Caswell Lawsuit").

382. On February 26, 2020, FLF and Farrow caused to be filed *Woodrow Power, on behalf of himself and others similarly situated, v. Insurance Office of America, Inc. et. al.*, In The Circuit Court For The Seventeenth Judicial Circuit In and For Broward County, Florida, Case Number: CACE20003595 ("Power Lawsuit").

383. As each of the above litigation matters were filed, the Threat Actor Defendants restructured and/or recalibrated operational activities and milestones, and, where necessary, repeated a sequence framework structure such as research and intelligence gathering.

384. Farrow and Farrow Law remained as defined targets of the APT from the 2019 through present.

385. In June 2019, FTI was hired by Heath, John, IOA, LLC and IOA, Inc. to implement a strategy which would eliminate Farrow and Farrow Law as their first primary targets, which would, in turn eliminate the prosecution of the Spagnuolo Case.

386. From July 2019 through March 2020, FTI carried on, on behalf of their clients, substantial research of Farrow and Farrow Law, and selected clients, such as Spagnuolo, through the location, extraction and study of Farrow Law's website, YouTube Channel, online records of two radio shows Farrow had been a co-host, Farrow's Facebook page, and information from open sources such as court records, corporate records and property records.

387. As well, from August 2019 through December 2020 and beyond, the Threat Actor Defendants' social engineering/strategic communications research and activities included numerous scripted communications to all of IOA's employees presenting false narratives consisting of denials of the claims made against them, and discrediting Farrow and Farrow Law.

388. Documents provided to Farrow and Farrow Law in March 2021, identified FTI as being retained by IOA as early as March 2020.

389. Further, the Ritenours and IOA's documents provided to Farrow and Farrow Law specifically detail some of the research and intelligence gathering that FTI performed from March 2020 through March 2021.

Introduction

FTI Consulting, Inc. ("FTI") was retained by Moran Kidd Lyons Johnson Garcia, P.A. ("Moran Kidd") on behalf of its client Insurance Office of America to investigate Louis Spagnuolo ("Spagnuolo"), Charles Goldman, ("Goldman") and Charles Reynolds ("Reynolds") and to conduct social media analytics to attempt to establish connections between the subjects' profiles in order to understand the flow of information in the subjects' negative feedback loop strategy.

FTI has also preserved online information extracted from Spagnuolo, Reynolds, Goldman and VRA Risk America's LinkedIn profiles as well as VRA Insurance's inactive website and has conducted public records research into Proton Mail's email service.

Testing Vulnerabilities, Initial Infiltrations and Foundations of Digital and Non-Digital Foothold Fortification Activities of the APT

390. By January 2020, the Threat Actor Defendants, directly and/or indirectly, had created and/or stolen and/or misappropriated the likenesses of over 10 fictious online profiles of individuals which would support or could support the Threat Actor Defendants in achieving their Ultimate Goals.

391. The creation of fictious expert profiles on its website or on LinkedIn by FTI, were accomplished as a regular way of conducting business with respect to their crisis management and strategic communication services.

392. In February 2020, the Threat Actor Defendants tested one of their fictitious online profiles, which they had cultivated since July 2019, that being Ms. Sanyia Booth.

December 2019 – March 2022 – Examples of Social Engineering Judicial Proceedings

Sanyia Booth and sanyiabooth.org

393. In this case, in 2019, FTI and the IOA Defendants discovered through their research gathering, a woman named Sanyia Booth who had had gone through a unique litigation history in the 18th Judicial Circuit in and for Seminole County, having six independent legal matters opened from 2015 to 2017 related to ongoing family issues with her former husband, Carl Booth.

394. Ms. Booth herself, was purported a mother of two daughters, and schoolteacher.

395. In April 2015, less than 48 hours after Ms. Booth allegedly called the police and reported a domestic violence incident at her home in Seminole County, Florida which resulted, allegedly, in the arrest of her then husband, Lt. Comr. Carl Booth, Mr. Booth filed a petition for dissolution of marriage which was randomly assigned to the Hon. Jessica Recksiedler.

396. The dissolution cases were dismissed for lack of jurisdiction.

397. In the other 'civil' cases, one of which was assigned to Judge Susan Stacy.

398. In 2018, Judge Stacy entered one substantive order on Ms. Booth's motion to disqualify and entered an order dismissing a case for lack of prosecution in or about 2018.

399. In fact, upon information and belief, Ms. Booth it does not appear that Ms. Booth was ever before Judge Stacy in open court at any time.

400. After being dismissed for lack of jurisdiction – in two separate cases – by Judge Recksiedler, court records indicated the Booth divorce was decided in North Carolina.

401. By late 2018, Ms. Booth had gone through and been discharged from a no asset Chapter 7 Bankrupcy, claiming to be out of work and making less than $500 per month in income.

402. After her discharge in early 2019, Ms. Booth completely disappeared, her driver's license expired and there are no records of her currently living in the United States.

403. From June 2019 through February 2021, there are two social media accounts associated with her name, one on change.org dated July 6, 2019, and the other a twitter account.

404. While some evidence exists that Ms. Booth may have had other social media accounts, none of them had any content, especially none which matched the content posted on change.org and her purported twitter account.

405. Change.org – On July 6, 2019, the one and only post purportedly attributable to Ms. Booth appeared and is registered.

406. That July 6, 2019 post was created nearly two years after the filing or prosecuting any substantive issues in the Booth litigation matters, and while it rants about injustices, it does not mention herself as a directed victim or as herself being an actual litigant.

407. The July 6, 2019 post does not mention, whatsoever, Judge Recksiedler or Judge Stacy, the two Seminole County Circuit Court Judges who presided or were at least assigned one or more of the seven case filings between 2015 and 2017.

IMPEACH JUDGE MICHAEL DENNING OF WAKE COUNTY, NC FOR FORGING $49,321.75 ATTORNEY FEE ORDER

Started July 6, 2019

408. The Twitter Account - the twitter account has no postings prior to July 2019.

409. After approximately July 6, 2019, Ms. Booth's purported twitter account which has substantial ongoing posts with content primary ranting against the inequities of the judicial system.

410. Between July 2019 and February 5, 2020, Ms. Booth's twitter account contains over 1800 posts, none of them mention Judge Recksiedler or Judge Stacy.

411. Yet, on February 5 and again on February 9, 2020, Ms. Booth's twitter account posts a few derogatory posts containing video links, one of Judge Recksiedler being admonished live before the Florida Supreme Court, and the other of a television interview of Judge Stacy running for judicial office.

412. With those videos, the twitter commentary purportedly written and published by Ms. Booth is highly negative and derogatory.

413. Upon information and belief, the five postings on February 5 and 9, 2020, were redirect links which directed traffic to a C2 Domain and/or a C2 Server which the Threat Actor Defendants set up to deliver malware payloads.

414. Upon information and belief, the Threat Actor Defendants posted the links of a news interview of Judge Stacy and one of Judge Recksielder before the Florida Supreme Court which contained malware payloads designed to infiltrate computers belonging to employees of the 18th Judicial Clerk's Office, Judge Stacy, Judge Recksielder and their judicial staff in anticipation of the filing of Heath Ritenour, John Ritenour and IOA, Inc.'s lawsuit against Farrow and Farrow Law, all of their three clients, and Josh Clark, Clark, P.A. and their client David Naughton.

415. The postings directly and indirectly by the Threat Actor Defendants were also part of the testing vulnerabilities, and gaining initial access to networks and the individual protected computers connected to those networks.

416. After February 9, 2020, the negative posts about Judge Recksielder and Judge Stacy stop – however, there are a few sporadic postings from February 9, 2020 through February 14, 2021 after which all social media postings purportedly by Ms. Booth end.

417. On February 14, 2021, all of Ms. Booth's social media postings end, with her last post stating she was cooking her husband, Carl Booth's, favorite meal, and implying the two are still married.

418. On March 8 and 9, 2020, respectively, the Threat Actor Defendants registered johnritenour.net and heathritenour.com.

Using Legal Process for Malicious Social Engineering Campaigns

419. In March 2020, the Threat Actor Defendants caused not one, but two SLAPP lawsuits to be filed against Farrow and Farrow Law.

420. On March 24, 2020, Heath Ritenour, John Ritenour and IOA, Inc. filed their SLAPP lawsuit in Seminole County Circuit Court dated March 24, 2020 ("2020 Seminole SLAPP Case").

421. Two days later, on March 26, 2020 in Palm Beach County Circuit Court ("2020 Palm Beach SLAPP Case").

422. Before filing these matters, counsel for the IOA Defendants and the JTR Partners agreed, consented to, had knowledge that these two SLAPP lawsuits would work in tandem for malicious purposes other than for which they were designed, such as the purposes of accomplishing sequence framework structure milestones of the APT, and/or to accomplish one or substantially all of their Ultimate Goals.

423. More specifically, these Defendant groups agreed to coordinate these matters, share information and use FTI's plans and strategies for using this litigation as part of the APT for, *inter alia,* spear phishing emails of pdfs and document links which contained and delivered malware payloads.

424. With respect to the 2020 Seminole SLAPP Case, the same was unprecedented in that it was filed against the four plaintiffs of the Spagnuolo, Naughton, Caswell and Power Cases, two law firms and the two lead counsels from those firms representing those plaintiffs.

Initial Infiltrations into Protected Computers through Social Engineering TTPs

- **The sanyiabooth.org Social Engineering Campaign**

425. On March 28, 2020, two business days after the filing of the 2020 Seminole SLAPP Case, and the random assignment to Judge Stacy, the Threat Actor Defendants registered sanyiabooth.org.

426. Upon information and belief, Sanyiabooth.org was and is a C2 Domain or a C2 Dead Drop.

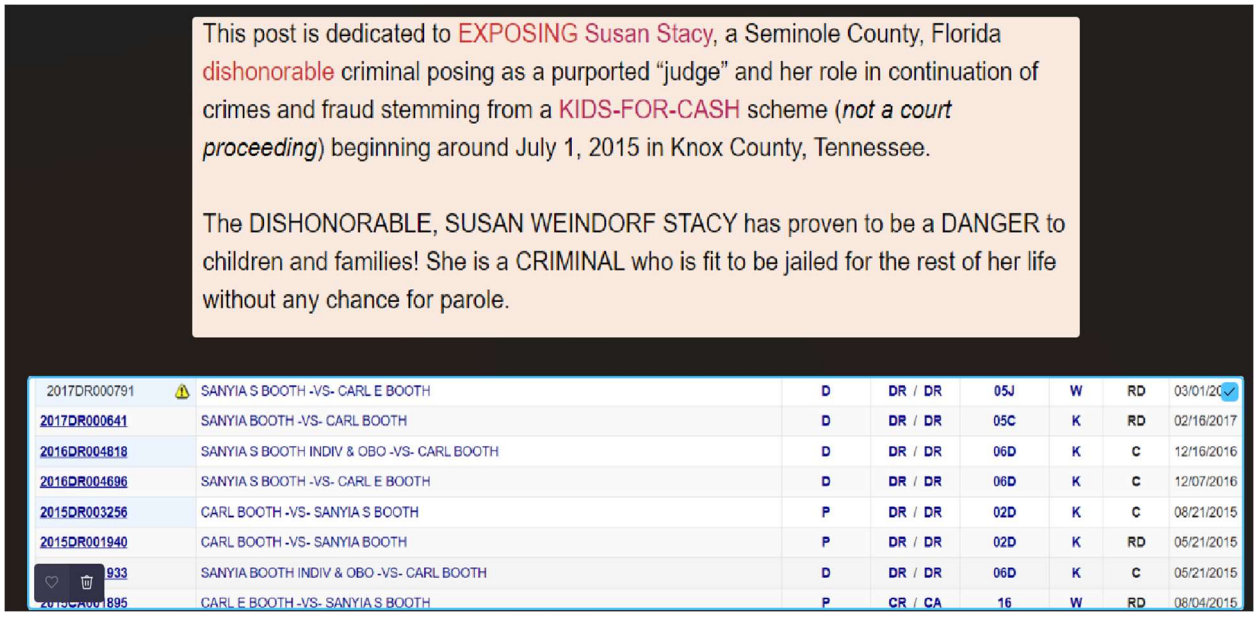
427. By early 2019, the seven or eight litigation matters listed on the 18th Judicial Clerk's Website relating the Booths' family litigation were all dismissed.

428. In total, Judge Stacy was assigned to two cases, and therein, Judge Stacy entered two orders of dismissal for lack of prosecution, and one denying a motion to disqualify in or about 2018 which was purportedly filed by Ms. Booth.

429. From March through June 2020, Heath Ritenour, John Ritenour and IOA, Inc., file several motions seeking to quash subpoenas issued by Farrow and Farrow Law, and multiple motions for extension of time to respond to numerous requests for discovery.

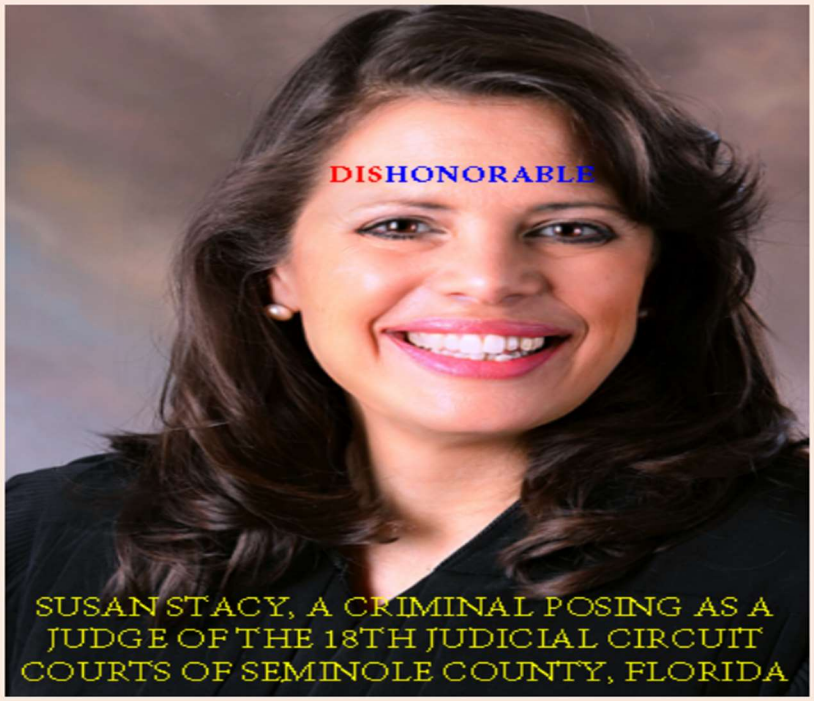
430. From March through June 2020, the sanyiabooth.org first blog page was being carefully crafted by the Threat Actor Defendants to feature and target Judge Stacy, while mimicking Farrow, Farrow Law, but especially, their client, Spagnuolo's social media posts using similar fonts, colors, and other features such as numerous hashtags.

431. When the first blog page was published on June 29, 2020, the day Farrow and Farrow Law filed a Motion to Dismiss the 2020 Seminole SLAPP Lawsuit, and it states in part: "**This post is dedicated to EXPOSING Susan Stacy, a Seminole County, Florida dishonorable criminal posing as a purported 'judge'…**."



432. On June 29, 2020, the statement is followed by the following featured photograph of Judge Stacy, which is copied below with the writing placed on her face by the Threat Actor Defendants as part of their scheme to lure very specific individuals to this website between June 2020 and March 2022.

FLORIDA JUDICIARY!



Susan Stacy, a DISGRACE to the Florida judiciary, EXPOSED in a KIDS FOR CASH scheme out of Knox County, Tennessee!

433. The Threat Actor Defendants employes a comprehensive array of technologies and infrastructure components, which prioritize anonymity and untraceability. The website is built on the WordPress ("WP") platform and was securely hosted through Automatic, a service associated with wordpress.org.

434. The Threat Actor Defendants displayed a high level of expertise constructing sanyiabooth.org by employing, *inter alia*: (1) wordpress.org (as opposed to the user friendly

wordpress.com); (2) Gravatar Profiles; (3) Giphy; (4) Unsplash; (5) Pexels; (6) BatCache; and (7) IE SiteMode.

435. **JAVASCRIPT PLUGINS**: The Threat Actor Defendants displayed a high level of expertise constructing sanyiabooth.org by utilizing JavaScript ("JS") Plugins such as, *inter alia*: (1) IE Pinning; (2) jQuery; (3) jQuery Masonry; (4) images Loaded; (5) Lightbox; and (6) JavaScript Modules.

436. **PINGBACK SUPPORT**: The Threat Actor Defendants demonstrated their focus on constructing the sanyiabooth.org website to have a covert operational framework by using Pingback Support to handle its notifications for the website.

437. **LEGAL LITIGATION DISCOVERY SOFTWARE**: The Threat Actor Defendants demonstrated and used litigation discovery software "Really Simple Discovery" to maintain anonymity, prevent traceability and ensuring meticulous data concealment.

438. **METADATA SCRAPING**: The Threat Actor Defendants intentionally eliminated all metadata as to each image on the sanyiabooth.org website to preserve anonymity and thaw tracking efforts using various Apple iMac operational systems through 2020.

439. **PROXY and JETPACK SITE ACCELERATOR CDN Usage**: The Threat Actor Defendants focus on robust privacy measures is further evidence by the strategy deployment of a proxy and the utilization of a CDN functionality, which further enhances privacy while safeguarding against tracking or surveillance attempts.

440. Upon information and belief, the cyber-tradecraft within the website's architecture which allowed it to act as a C2 Dead Drop and/or a C2 Domain which facilitated the exploitation

of social engineering to obtain unauthorized access to protected computers belonging to Farrow and Farrow Law, and unauthorized access to other protected computers.

441. Additionally, the Threat Actor Defendants used sophisticated geo-fencing technology with the sanyiabooth.org website, and further hid the location of same through various techniques, such as the title of the website within its source code that would prevent search engines from locating the June 29, 2020 blog page.

442. The purpose was to direct the content of the website to a specific individual or group of individuals as part of their utilization of social engineering.

443. More specifically, to geo-fence the sanyiabooth.org website, directing it to Judge Stacy and employees of the 18th judicial circuit, for purposes of social engineering very specific individuals to visit the webpage.

444. Upon visiting the website, the Threat Actor Defendants obtained information such as locations, IP addresses, and using a variety of means and methods, such as embedding malicious code into the photos, pdfs and videos to deliver malware payloads allowing unauthorized access to protected computers such that, *inter alia,* the Threat Actor Defendants could issue commands directed at fortifying network footholds.

445. Moreover, the June 29, 2020 sanyiabooth.org webpage was designed and crafted to manipulate the course of judicial proceedings.

Malicious Conduct and Social Engineering to Procure Wrongful Injunctions

446. More specifically, while no request was made in the 2020 Seminole SLAPP Case for injunctive relief, on December 8, 2020, after a global mediation failed to achieve a resolution of all pending litigation, Heath Ritenour, John Ritenour and IOA, Inc., filed an unverified motion

for injunction alleging, in part, that Spagnuolo created a website, and uses his social media accounts to post about the ligations proceedings, using hashtag that draw the Ritenour and IOA's clients to reading press releases about the 2019 Spagnolo Case and the 2020 SLAPP lawsuits.

447. Additionally, the injunction motion alleged that Spagnuolo's social media posts are made by and through other social media profiles, and that they contain consistent font sizes, and red, white, blue and yellow colors, and use hash tagging.

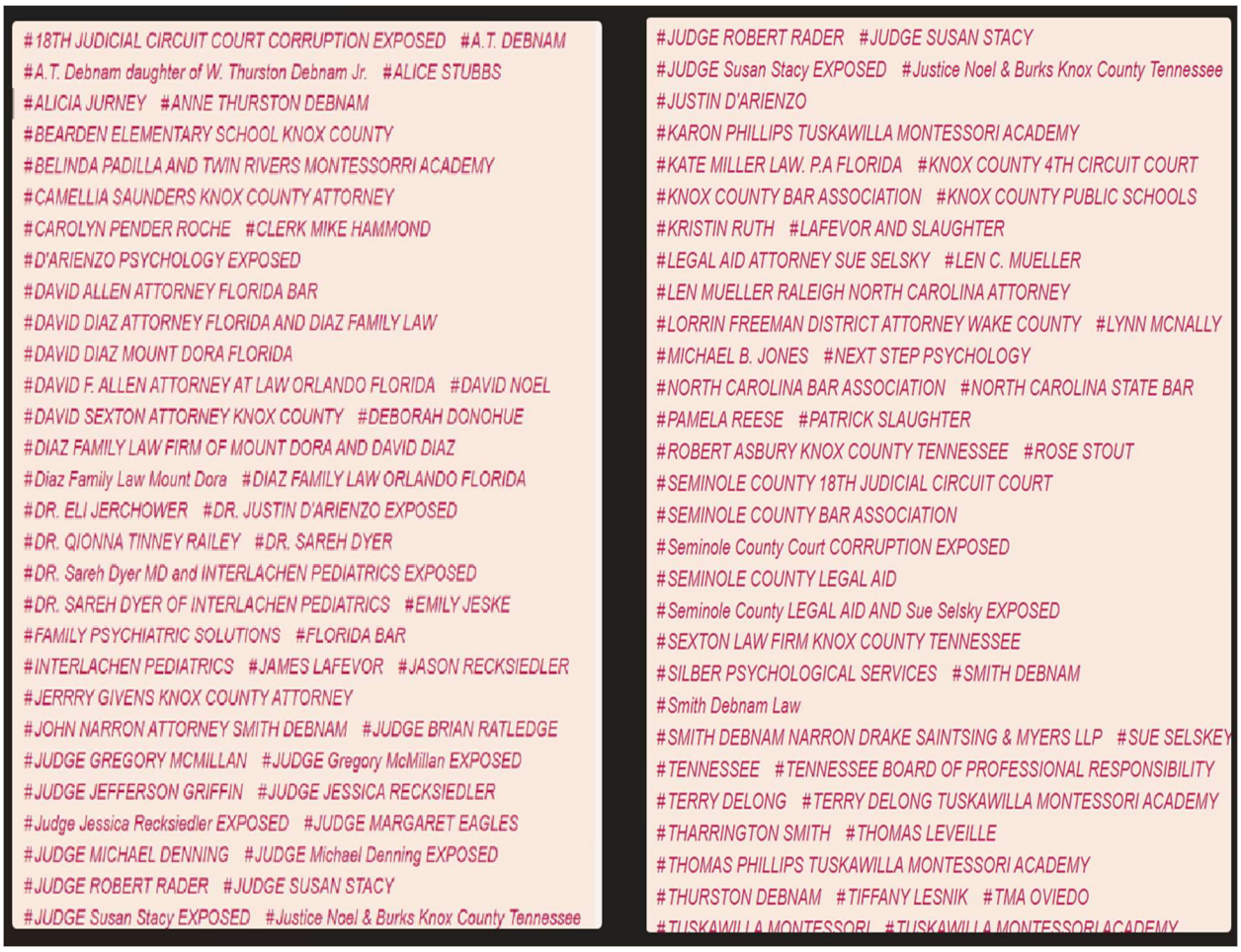
448. Upon information and belief, the Threat Actor Defendants created the sanyiabooth.org website, and directed to Judge Stacy, and Judge Recksielder after extracting Farrow, Farrow Law and Spagnuolo's social media postings and using the identifying features testified to by FTI's fake witness to infer Farrow and/or his client were culpable for attacking her online.

449. On March 9, 2021, in an oral ruling at a three-day video conference hearing, that the **font size, font color and capitalizations of letters** were enough circumstantial evidence to rise to the level of a substantial likelihood on the merits it was Spagnuolo behind sending and posting materials which purportedly interfered with the IOA Defendants business relationships.

450. Further, Judge Stacy found it was **the use of hastaggs** which created the exclusive demonstration of irreparable harm warranting injunctive relief in the 2020 Seminole SLAPP Case

451. At the bottom of the 400 printed pages of the June 29, 2020 blog post are nearly 70 hastaggs with names of other judges within the 18th Judicial Circuit, Florida and out of state attorneys and a Montessori academy.

452. However, clicking any one of these links returns to Judge Stacy's photograph at the top of the 400 paged blog, but it also delivers a malware payload.



APT Adaptation – Farrow and Farrow Law Seek Witnesses and Information

453. By July and August 2020, the Threat Actor Defendants were facing an innovative investigation tool in which Farrow and Farrow Law created and posted Notice to Witness Videos seeking witnesses and/or information in defense of the 2020 SLAPP Cases, and the prosecution of the client's claims.

454. In response, the Threat Actor Defendants created and rapidly deployed a Dump-Pump-Up & Drain ("DPUD") Scheme.

455. In the DPUD Scheme, between September and December 8, 2020, both the IOA Parties and JTR Partners, at the direct of, and./or with the consent of FTI, filed separate motions seeking urgent injunctive relief which collectively resulted in over fourteen thousand (14,000) pages of documents being served via pdf or DropBox links between December 8, 2020 and March 2, 2021, (i.e. the Document Dump)[15].

456. These pdfs and links contained payloads of malware or embedded malicious code that was designed establish and strengthen foothold fortifications in the Farrow Law and other networks and the protected computers connected thereto (i.e. the Pump).

457. The malware and second stage malware strategically accelerated the Threat Actor Defendants upward advancement of privileges and permissions (i.e. the "Up" Aggressive Advancement), while simultaneously forcing APT Targets Farrow and Farrow Law to expend massive amounts of resources (i.e. the "Drain") which substantially reduced any meaningful possibility of detecting such aggressive conduct.

458. As further alleged herein, records retrieved from Farrow's Lenovo Laptop and other protected computers registered the fruits of the DPUD Scheme, especially subsequent to March 17 and 18, 2021.

---

[15] On February 22, 2021 and March 2, 2021, in the 2020 Seminole SLAPP Case, both of the respective "Dropbox links" served upon Farrow and Farrow Law by Heath, John and IOA's counsel, Brain Moran, consisted of over 11,000 pages of documents, of which, over 10,000 were extracted from online sources by FTI, saved to FTI's network, organized by FTI and delivered by FTI directly or indirectly to Farrow and Farrow Law containing malware payloads which had an extremely low probability of discovery, but would allow the Threat Actor Defendants to map FLF's Network of Files, Shared Staff Files and Other General Firm Files.

APT –FTI and the IOA Defendants Use a Fictitious Identity and Fake Expert Witness to Manipulate Judicial Proceedings

459. By design, the IOA Parties and the JTR Partners' also used similar playbooks with respect to the prosecution of their urgent injunction motions, which included presented knowingly false documentary evidence and/or false testimony.

460. With respect to the IOA Parties injunction hearings, the Threat Actor Defendants called a fake expert witness to testify remotely on March 2, 2021, claiming to be a FTI Senior Managing Director going by the name of Kevin Leung.

461. Through Mr. Leung, thousands of pages of documents were admitted into evidence, and his 'expert' testimony was directed to connect the proverbial dots – to wit: that Spagnuolo was responsible for the posting about Heath Ritenour, John Ritenour and IOA, Inc. due to the postings having the same font size, colors and hash tagging.

462. However, similar in nature to some of FTIs more infamous conduct around 2018 and 2019, Kevin Leung's only connection between himself and the purported 13-year career he had had at FTI before testifying on March 2, 2021, was his LinkedIn Page which was created in April 2020, the same month and year he began extracting Farrow, Farrow Law and Spagnuolo's social media postings.

463. Yet, Mr. Leung's testimony as an expert for FTI did not set off any alarm bells, and the same was by design.

464. On his LinkedIn page, Mr. Leung claimed to have the title of Senior Managing Director, which is FTI's top employee designation, and the same stated he worked out of FTI's

New York Office and initially for one of FTI's related companies, FTI Technologies named Kevin Leung.

465. Mr. Leung claimed to be Heath, John and IOA's expert witness and also a purported investigator of Farrow and Farrow Law, its clients and others as further alleged, *infra.*

466. In April 2020, a LinkedIn profile was created and built out to reflect it belong to Kevin Leung.

467. Yet, no one named Kevin Leung ever worked at FTI, nor its New York office or anywhere else in the world since 2007 or ever.

468. No person named Kevin Leung ever graduated from St. John's University at or around 2000 through 2010, or at any time.

469. The only other Kevin Leung in the United States has which has any social media is an individual purportedly who served in the military, yet bears no resemblance to the photo of Mr. Leung on LinkedIn.

470. FTI's main website, and that of which Mr. Leung had a purported email, makes no mention of Mr. Leung whatsoever, and has never listed him as an employee, or a "director."

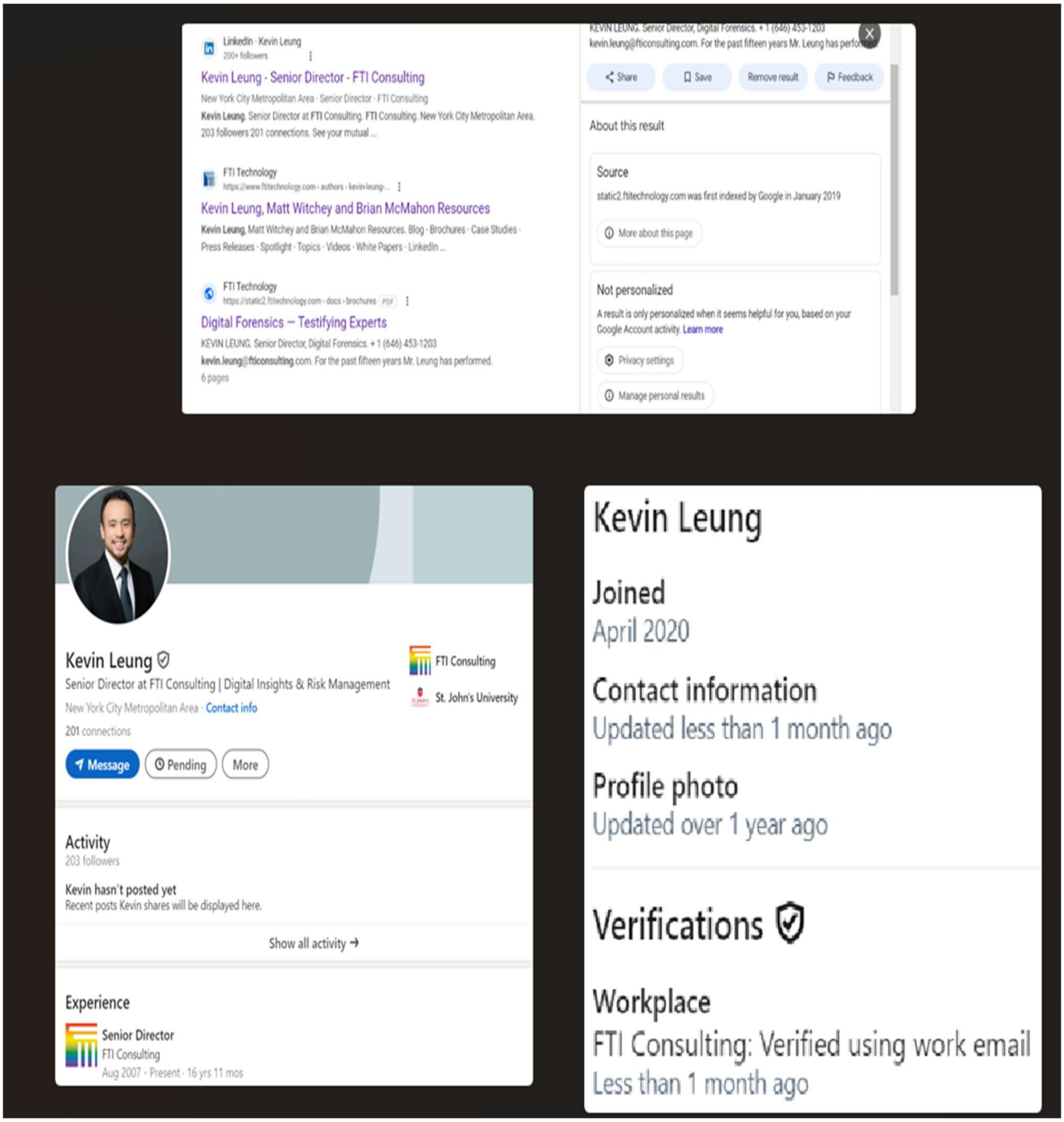
471. The only reference to Mr. Leung's relationship to FTI outside his LinkedIn profile, which was not discovered until March or April 2024, was a single article about cyber-technology which he purportedly co-authored and a pdf profile of Mr. Leung with other alleged FTI directors.

472. However, the same was not posted on FTI's main website, it was located at ftitechnology.com, or some variation thereof. And, even then, that connection between Mr. Leung and FTI was not published until 2022, almost a year after he testified on March 2, 2021.

473. Moreover, at least one of the 'co-authors' of this 'article', Brian McMahon, is an individual who also never worked for FTI as an employee, or a director, and his photo, name and purported credentials are part of the Threat Actor Defendants' attempt to create the illusion that Mr. Leung not only worked for FTI, but to reinforce his fake credentials, he writes and publishes cyber-technology articles with other FTI "directors."

474. Finally, the article which is credited to Leung in the headline generated by an internet search, does not actually mention him.

475. In short, at day's end, to research Mr. Leung's credentials, Farrow and Farrow Law, or anyone else for that matter, was required to click on a hyperlink which redirected to C2 Domain or C2 Dead Drop which, at the very least, infects embedded malicious code track locations and IP addresses.


LinkedIn · Kevin Leung
200+ followers
Kevin Leung - Senior Director - FTI Consulting
New York City Metropolitan Area · Senior Director · FTI Consulting
Kevin Leung. Senior Director at FTI Consulting. FTI Consulting. New York City Metropolitan Area. 203 followers 201 connections. See your mutual ...
FTI Technology
https://www.fticonsulting.com › authors › kevin-leung-...
Kevin Leung, Matt Witchey and Brian McMahon Resources
Kevin Leung, Matt Witchey and Brian McMahon Resources. Blog · Brochures · Case Studies · Press Releases · Spotlight · Topics · Videos · White Papers · LinkedIn ...
FTI Technology
https://static2.fticonsulting.com › docs › brochures PDF
Digital Forensics – Testifying Experts
KEVIN LEUNG. Senior Director, Digital Forensics. + 1 (646) 453-1203
kevin.leung@fticonsulting.com. For the past fifteen years Mr. Leung has performed.
6 pages
KEVIN LEUNG. Senior Director, Digital Forensics. + 1 (646) 453-1203
kevin.leung@fticonsulting.com. For the past fifteen years Mr. Leung has performed.
Share
Save
Remove result
Feedback
About this result
Source
static2.fticonsulting.com was first indexed by Google in January 2019
More about this page
Not personalized
A result is only personalized when it seems helpful for you, based on your Google Account activity. Learn more
Privacy settings
Manage personal results
Kevin Leung
Senior Director at FTI Consulting | Digital Insights & Risk Management
New York City Metropolitan Area · Contact info
201 connections
FTI Consulting
St. John's University
Message
Pending
More
Activity
203 followers
Kevin hasn't posted yet
Recent posts Kevin shares will be displayed here.
Show all activity →
Experience
Senior Director
FTI Consulting
Aug 2007 - Present · 16 yrs 11 mos
Kevin Leung
Joined
April 2020
Contact information
Updated less than 1 month ago
Profile photo
Updated over 1 year ago
Verifications
Workplace
FTI Consulting: Verified using work email
Less than 1 month ago

476. Nevertheless, whomever Mr. Leung is or is not, through the documents provided to Farrow and Farrow Law during the DPUD Scheme evidence the Second APT sequence framework structure of research and intelligence gathering commenced at least April 10, 2020 through March 2021.

Web Data Collection Report

Page Title

Chuck Goldman | LinkedIn

URL

https://www.linkedin.com/in/chuck-goldman-292a7716/

Collection Date

Fri Apr 10 2020 17:51:33 GMT-0400 (Eastern Daylight Time)

Collected by

Kevin.Leung@fticonsulting.com (Kevin.Leung@fticonsulting.com)

IP Address

208.184.134.36

Browser Information

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36

Digital Signature (SHA256 / PKCS#1v1.5)

782005ce21b1f22150b989461c8f011eed2acc3aca2379c023ea8048e0a3ae8eb66d3a63016
497866b4301e208deedb8ed33474b4ac7b625632d8fec2da18954a9073861464bcd43ed80b5
df0446b75af440218d98886d1ccec3dceed56e66bd5fe5dff710de54f21df0fee37dacaf168
307d7c524707351a8fa3533982d61c823d176b0a065d123a1d882b8036280821339f89a7549
fe77613ef6dcb082f89a9284523a90309020d02aaaa43d764035bdfdc91967a5d93f0c97d3f
e3b89c8de92b0a3f393e4a142c5af0df902d67f234462fd8d3ccc5daa9004f02d93bb5df9fd
f2b5fa1322ea6b0d96a8419fb28a78ea75186a5a7b1f53cdd8c8635467eb65

477. On either the exact day of data extraction from Spagnuolo, Farrow and Farrow Law's social media and websites logged by FTI such as April 10, 14, 17 and 20, 2020, or within the same week or weeks, the source code for heathritenour.com, johnritenour.net and sanyiabooth.org evidence that they were all being developed in tandem.

478. In or about January 2020, at around the same time, they created a fictitious profile of another FTI Expert Janet Nweke, who would also purport to be investigative research for FTI and the other Threat Actor Defendants.

Web Data Collection Report

Page Title
John Ritenour | Insurance Office Of America

URL
http://www.johnritenour.com/

Collection Date
Wed Aug 05 2020 11:27:25 GMT-0400 (Eastern Daylight Time)

Collected by
Janet.nweke@fticonsulting.com (Janet.nweke@fticonsulting.com)

IP Address
24.168.16.57

Browser Information
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36

479. There is no information on FTI's website regarding Ms. Nweke, and all social media associated with this person indicates she works as a model in New York.

480. Neither Mr. Leung nor Ms. Nweke were actual Experts, or Senior Managing Directors of FTI. In fact, to the extent that these individuals exist, other social media profiles of persons with similar names and photos reveal that Mr. Leung served in the military which is not mentioned in or on his LinkedIn profile.

LAWYER AND LAWFIRM VULNERABILITY EXPLOITATION SCHEME - 2020 through present - Delivering Malware Through Exploiting Lawyer and Law Firm Communications

481. By December 2020, through the execution of their DPAD Scheme or otherwise, the Threat Actor Defendants initial research discovered, identified and tested a vector vulnerability which was inherent in the usual and customary interactions between opposing counsels in a litigation proceeding.

482. More specifically, the Threat Actor Defendants had knowledge and experience in litigation discovery document exchanges, review, the process by which lawyers and law firms extract and mine data from electronically stored and the manner in which documents are assembled and served upon opposing counsel, court clerks, judicial staff and other third parties in response to, for example, discovery requests and otherwise in advance of hearings and trials.

483. This knowledge and experience included an understanding that, as a matter of routine behavior due, and/or logistical unavoidability, emails with pdf attachments and/or links purporting to serve court related documents which purportedly emanating from opposing counsel, co-counsel or the court itself have a very high probability that they will be trusted, opened and their attachments downloaded.

484. The Threat Actor Defendants intended to, attempted to and did, in fact, exploit this vulnerability by sending Farrow, Farrow Law, its legal counsel, and other law firms and lawyers emails containing links and or attachments containing malware payloads for purposes of infiltration the Farrow Law and other Networks and the protected computers connected to such networks, which, in at least 34 instances, belonged to lawyers and law firms having collateral or

strategic associations, for purposes of achieving operational millstones, one or more sequence framework structures of the APT and/or one or more Ultimate Goals.

485. More specifically, from September 2020, the Threat Actor Defendants planned to use, attempted to use and did, in fact, send emails containing links, Dropbox links or pdf attachments under the case headings of the litigation by and between Heath Ritenour, John Ritenour and IOA, as well as their co-conspirators, Joe Taylor Restoration and Joe Taylor and others, to Farrow, Farrow Law and other lawyers and law firms under circumstances which they knew or should have known contained malware or malicious software code.

486. From 2019 through July 2024, Farrow and Farrow Law, or collaterally targeted lawyers and law firms' networks and the protected computers connected to those networks, received emails directly or indirectly from the Threat Actor Defendants containing links and pdf attachments, and download their contents, some of which contained embedded malware and/or malicious code which was used to gain, maintain and advance privileges and permissions while remaining undetected.

487. From 2019 through at least July 2024, using the pretext of active litigation or, court related proceedings or related to a Florida Bar inquiry to send emails, links and/or pdf documents to deliver malware and/or malicious software code for purposes of gaining unauthorized access to, or to steal information from or for purposes of sabotaging the network system or computer, was a regular way of conducting the activities of the Threat Actor Defendants.

488. This conduct and activity were successful in stealing confidential information, such as documents and evidence stored in Farrow Law's network or on Farrow's Lenovo computer related to the litigation involving the Threat Actor Defendants.

489. This conduct and activity allowed the Threat Actor Defendants to cause substantial interference with Farrow and Farrow Law, and its clients, vendors, staff, legal counsel, opposing counsels and courts of law which was unjustified and having no legitimate legal purposes

490. The conduct and activity of sending litigation related emails, which was used for maintaining persistent access to Farrow Law's Network, its computers and other networks and computers, was also used to steal information and sabotage Farrow and Farrow Law's network, computers and other devices.

491. In other words, very early into the research and intelligence sequence structure framework, the Theat Actor Defendants had a vector infiltration which could exploit the trust placed by one attorney or firm and its opposing counsel, and thus, could establish initial, secondary and persistent foothold fortifications, as well as lateral foothold fortifications in the Farrow Law Network, its computers and other collateral targeted law firms' protected networks.

492. As well, the malware payloads delivered in December 2020, February 22, 2021 and March 2, 2021 respectively, were directed at exploiting network vulnerabilities for purposes of mapping and advancing privileges and network permissions.

493. In each case, by infecting the FLF Network with malware designed to allow the Threat Actor Defendants to access more files and more sensitive information, which resulted in the Threat Actor Defendants' ability to monitor the progress of work product, Farrow's personal life activities and confidential case strategies and tactics.

494. As well, by having gained access through unlawful infiltrations through an FLF employee opening up a pdf or link from opposing counsel, the Threat Actor Defendants also had access to Farrow, FLF and all FLF employee's files and calendars.

January 2020 through July 2024 – Fortifying Strongholds Using Schemes of Known and Zero Day Exploits

495. Beginning in 2019 through June 2024, the Threat Actor Defendants executed the sequence framework structures of testing and deployment[16]/exploitation of vulnerabilities.

496. Plaintiffs allege that from 2019 through present, the Threat Actor Defendants successfully and persistently infiltrated FLF's Network and the computers/networks of Farrow and Farrow Law's clients, lawyers, and vendors using litigation proceedings such as the 2020 SLAPP Lawsuits to send spear phishing emails with pdfs and links containing malware payloads.

497. Each successful unauthorized exploitation of a vulnerability which infiltrated any computer, network, cell phone, personal or business email account and/or organization associated with Farrow and Farrow Law from 2019 through August 2023 was accomplished for the primary purposes of achieving the Ultimate Operation Goals as defined herein, *supra* by:

(1) maintaining foothold positions in FLF's Computer Network;

(2) establishing lateral foothold positions in strategic collateral computer networks of FLF's clients, attorneys and vendors; and

[16] Deployment, also known as Maneuvers or "Fires", are attempts to attack the target network system, internal network devices connected thereto or therewith such as employee PCs, mobile phones, tablets etc. using a direct exploit (i.e. by introducing code), using a known or discovered vulnerability an indirect exploit (having someone else—usually unwittingly—introduce code that exploits a known or discovered vulnerability) or some combination of the two to enter a system or network.

(3) advancing privileges and permissions within each network until the same was sufficient to exfiltrate information and/or to manipulate the network's configuration to allow the Threat Actor Defendants to conduct malicious activities.

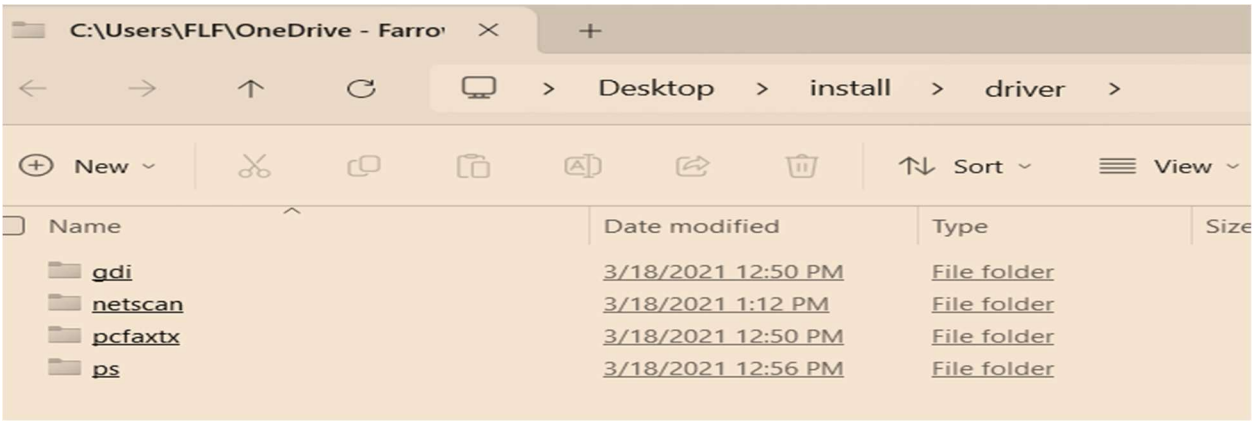
498. The specific malicious activities achieved by the Threat Actor Defendants' conduct between 2019 and present included: (1) obtaining individual credentials to receive, read and respond to emails, block network users from access to files which they were authorized to have; (2) filter email communications by creating 'rules' in Microsoft Outlook which would reject, delete or send outgoing emails to a 'drafts' folder; and (3) creating unauthorized user profiles within FLF's Network which had some shared administrator permissions.

499. From at least December 2019, this conduct is evidenced by and through modifications to over 30 Microsoft Software Programs that occur within a matter of a day to 15 days after the receipt of an email containing a pdf document or a link containing malware from Heath, John, and IOA's attorneys, or attorneys for Joe Taylor Restoration and Joe Taylor.

500. In each instance, the software registering a modification was later identified by in A CVE issued by NCIA, indicating that the exploitation of the software vulnerability was a zero-day attack.

501. A few examples of these modifications which were caused by the Threat Actor Defendants by exploiting a software vulnerability vector to gain unauthorized access to FLF's Network for purposes of enhancing network privileges and permissions are provided hereinbelow, followed by the respective issued CVE describing the software containing the vulnerability and what threat actors have been able to accomplish by exploitation of the vector access.

502. On March 17 and18, 2021, the malware delivered by one or both subject drobox links of February 22, 2021 and March 2, 2021 allowed the Threat Actor Defendants to modify Farrow Law's Network Microsoft Installer to gain network privileges, however, consistent with all case studies regarding APTs, this infiltration point had a very low possibility of detection and raised no red flags.[17]



503. On September 10, 2024, NCIA issued used CVE-2024-38014 related to Microsoft Windows installer Privilege Management Vulnerability which states in relevant part:

[17] In fact, this same vector infiltration point was exploited again by the Threat Actor Defendants on July 3, 2024 as they were exfiltrating tens of thousands of pages of documents and sabotaging FLF's Network, however, the same was not discovered by Farrow until approximately September 2024.

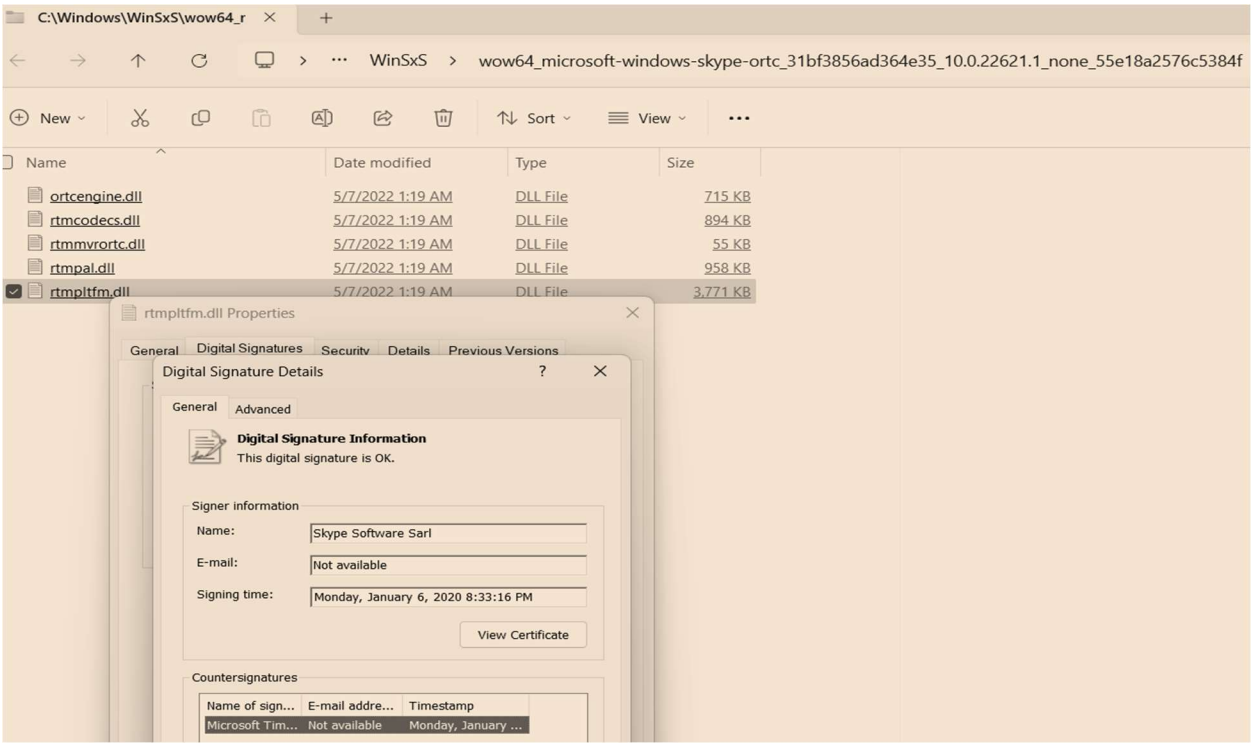
504. In August 2021, Defendant Kolaya served Farrow and Farrow Law pdf documents in advance of a hearing in the 2019 Spagnuolo Case upon Defendant Heath Ritenour, John Ritenour and IOA's Motion to Transfer the case to Seminole County Circuit Court.

505. On August 17, 2021, on the same day of receiving those materials, or within days of receiving and opening those materials, Farrow Law's Network and computers registered the Thread Actor Defendants' malware payload attempting to gain a foothold, first by denying access and issuing a Trace-Level-Warning at approximately 4:00 am, some 8 hours later, through achieving success just after 1:30 pm on the same day.

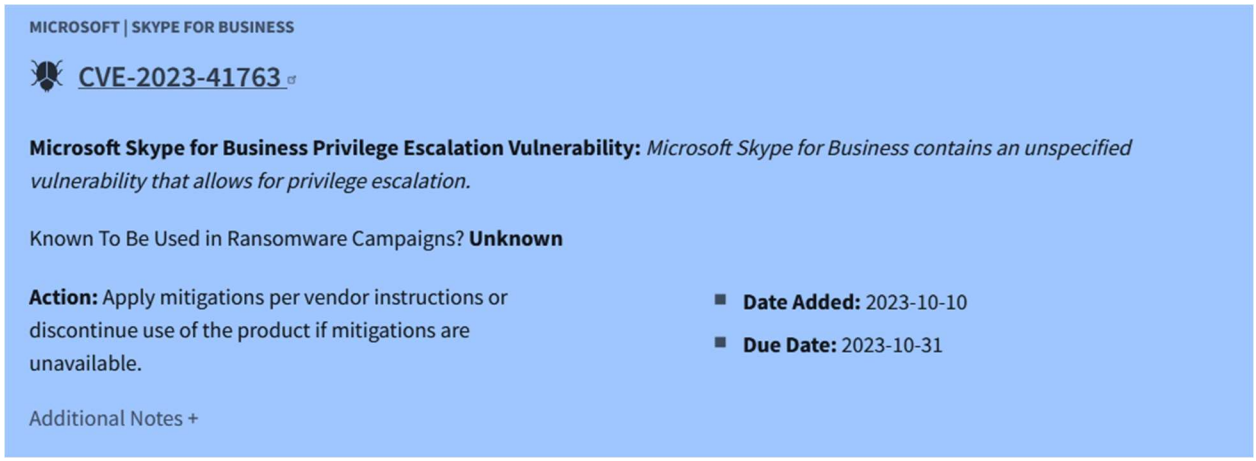
```
08/17/2021-04:59:14.985 TRACE_LEVEL_WARNING     Access denied to protected file [\Device\HarddiskVolume3\ProgramData\WRCore\CoreService
\WRCoreService.json] by process 0000000000000B08[C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain] elevated:
true (0x00000001)->NT AUTHORITY\SYSTEM, Reason: DesiredAccess too broad [0x00100080] [A4B43A4AEDA26E553621245FE11F4864,
DF078D86F0245E3660F52FCFE0CE7783, 448]
08/17/2021-09:09:15.256 TRACE_LEVEL_WARNING     Access denied to protected file [\Device\HarddiskVolume3\ProgramData\WRCore\CoreService
\WRCoreService.json] by process 0000000000000B08[C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain] elevated:
true (0x00000001)->NT AUTHORITY\SYSTEM, Reason: DesiredAccess too broad [0x00100080] [A4B43A4AEDA26E553621245FE11F4864,
DF078D86F0245E3660F52FCFE0CE7783, 448]
08/17/2021-13:08:15.746 TRACE_LEVEL_INFORMATION The WRCore driver is made unloadable... [280E8A05A8B91EDAB4742757499FF570,
D3F5AFA78314A4CD0538B910A872B139, 337]
08/17/2021-13:08:15.747 TRACE_LEVEL_WARNING     Allowing access to protected file [\Device\HarddiskVolume3\Windows\System32\WRDll.x64.dll]
by process 0000000000000CF0[C:\Windows\system32\msiexec.exe /V] elevated: true (0x00000001)->NT AUTHORITY\SYSTEM, because it meets trusted
installer requirements. [A4B43A4AEDA26E553621245FE11F4864, DF078D86F0245E3660F52FCFE0CE7783, 435]
08/17/2021-13:08:15.747 TRACE_LEVEL_WARNING     Allowing access to protected file [\Device\HarddiskVolume3\Windows\System32\WRDll.x64.dll]
by process 0000000000000CF0[C:\Windows\system32\msiexec.exe /V] elevated: true (0x00000001)->NT AUTHORITY\SYSTEM, because it meets trusted
installer requirements. [A4B43A4AEDA26E553621245FE11F4864, DF078D86F0245E3660F52FCFE0CE7783, 435]
08/17/2021-13:08:15.747 TRACE_LEVEL_WARNING     Allowing access to protected file [\Device\HarddiskVolume3\Windows\System32\WRDll.x64.dll]
by process 0000000000000CF0[C:\Windows\system32\msiexec.exe /V] elevated: true (0x00000001)->NT AUTHORITY\SYSTEM, because it meets trusted
installer requirements. [A4B43A4AEDA26E553621245FE11F4864, DF078D86F0245E3660F52FCFE0CE7783, 435]
08/17/2021-13:08:15.747 TRACE_LEVEL_WARNING     Allowing access to protected file [\Device\HarddiskVolume3\Windows\System32\WRDll.x64.dll]
by process 0000000000000CF0[C:\Windows\system32\msiexec.exe /V] elevated: true (0x00000001)->NT AUTHORITY\SYSTEM, because it meets trusted
installer requirements. [A4B43A4AEDA26E553621245FE11F4864, DF078D86F0245E3660F52FCFE0CE7783, 435]
```

506. By May 1, 2022, Farrow and FLF had requested a meet and confer with Defendant Attorney Tim Kolaya with respect to outstanding discovery which had been promised to be delivered in November 2019.

507. Within days of that request, there were a plethora of updates to FLF’s Network, with one particular modification to Microsoft Skype for Business on May 7, 2022 at 1:19 a.m.



508. On October 10, 2023, the NCIA issued CVE-2023-41763 which provided a warning that the Microsoft Skype for Business contained a vulnerability allowing for privilege escalation, which was, in fact, exploited by the Threat Actor Defendants who ultimately achieve full administration command and control of FLF's Network:



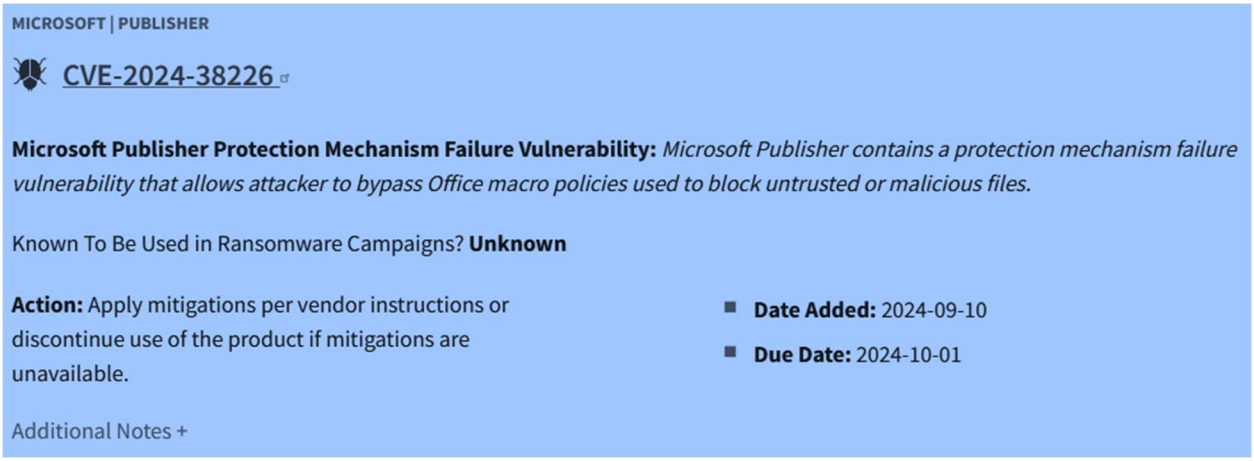
509. From September 2022 through December 2022, Farrow and FLF worked on a Second Amended Complaint in the 2019 Spagnuolo Case after he located over a thousand emails evidencing his relationship with John Ritenour and IOA, and establishing that Heath, John and IOA make false claims over interstate wires regarding the fact that Spagnuolo was an IOA Agent and was entitled to approximately 57% of the insurance commissions from the TLE Account from its procurement.

510. By December 1, 2022, the Threat Actor Defendants had the ability to access files available to FLF employees and, one of the files was the Microsoft Word draft of the Second Amended Complaint in the 2019 Spagnuolo Case.

511. In November and December 2022, Heath, John and IOA had served Farrow and FLF through their other counsel, Brian Moran, with pdf documents in advance of hearings scheduled for January 2023 in the 2020 SLAPP case.

512. On December 5, 2022, FLF's Network registered modifications to numerous software applications, one of which was Microsoft Publisher.

513. On September 10, 2024, the CSIA issued CVE-2024-38226 warning of a 'Microsoft Publisher Protection Mechanism Failure Vulnerability' which provided:


MICROSOFT | PUBLISHER

CVE-2024-38226

Microsoft Publisher Protection Mechanism Failure Vulnerability: *Microsoft Publisher contains a protection mechanism failure vulnerability that allows attacker to bypass Office macro policies used to block untrusted or malicious files.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-09-10
- **Due Date:** 2024-10-01

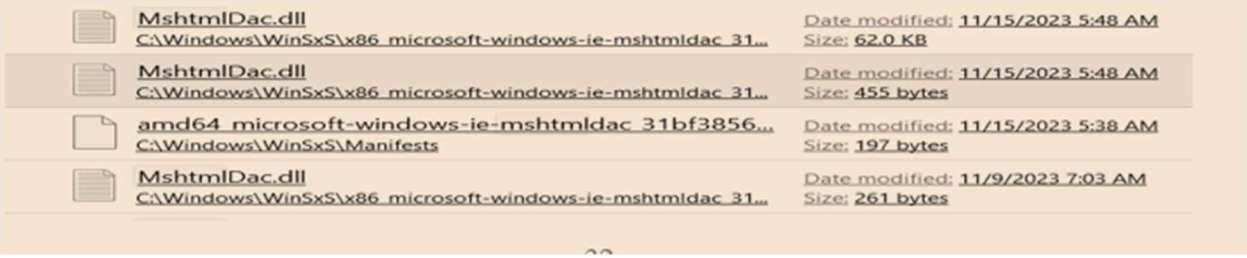
Additional Notes +

514. The modifications to FLF's Network relative to the Microsoft Publisher were caused by the Threat Actor Defendants and, via interstate wire transfer, infiltrated FLF's Network to gain unauthorized enhanced network privileges and permissions.

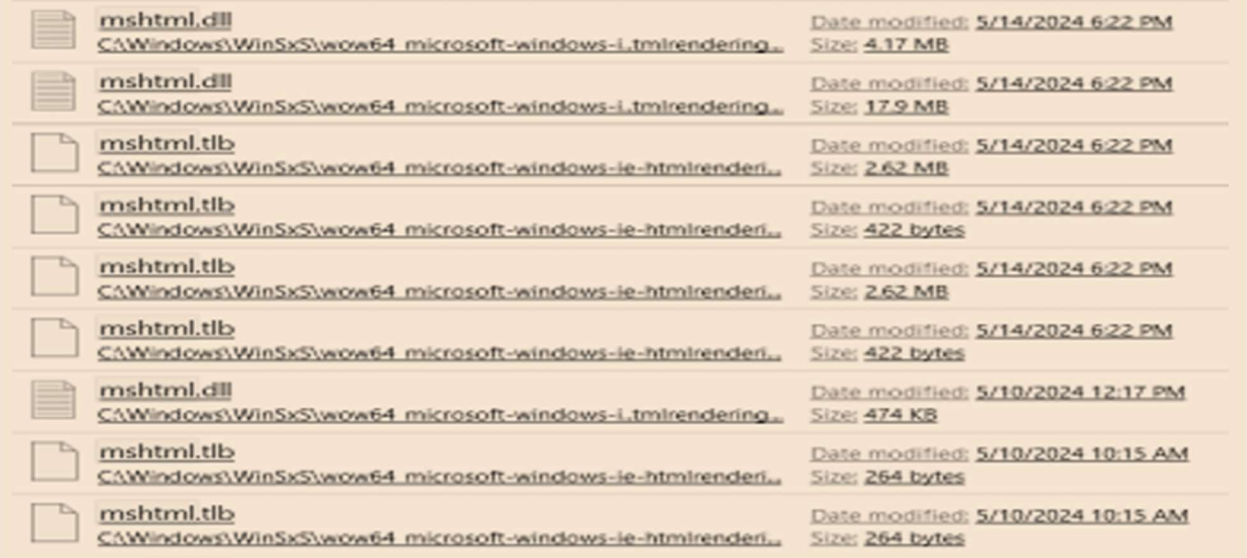
515. From September 2023 through November 8, 2023, Farrow and FLF worked on a comprehensive Motion to Dismiss the 2020 SLAPP Lawsuit as being in violation of Florida's Anti-SLAPP statute.

516. On November 8, 2023, the Anti-SLAPP Motion was filed and the same was followed by the receipt of pdf documents served upon Farrow and FLF by Heath, John and IOA's counsel, Defendant Moran for hearings for November 28, 2023.

517. The very next day, on November 9 2023, and again on November 15, 2023, modifications were made to FLF's Microsoft Windows MSHTML Platform.



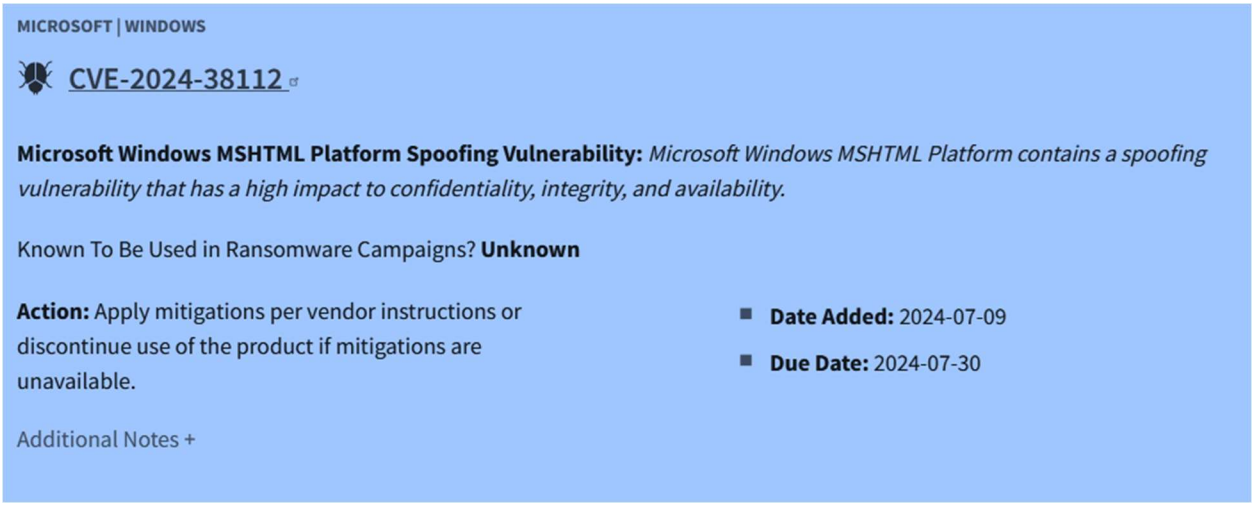
518. Further modifications of FLF Network's Microsoft Windows MSHTML Platform occurred on May 10 and 14, 2024, days after Farrow and Farrow Law filed a verified motion in the 2020 Seminole SLAPP Case outlining the discovery that Heath, John, IOA, and Brian Moran presented a fictitious expert at the March 2021 injunction hearings and evidence that these Defendants had known about, created and otherwise utilized the June 29, 2020 sanyiabooth.org webpage to manipulate the judicial proceedings.



519. Other modifications of FLF Network's Microsoft Windows MSHTML occurred on June 7, 2024, the day after Farrow and Farrow Law filed an Amended Injunction Motion in 2024 Federal Case seeking the immediate suspension and/or limitation of Heath, John, IOA and 11

National Insurance Carrier's licenses pursuant to Florida's Criminal RICO Statute 'Civil Remedy' provision, Fla. Stat. 895.05(6).

520. On July 9, 2024, the CSIA issued CVE-2024-38112 which warned of a 'Platform Spoofing Vulnerability' and provided:



March 2023 – the APT Undergoes Operational Recalibrations

521. By early March 2023, the landscape of the litigation between the Threat Actor Defendants, Farrow, Farrow Law and their Clients had changed dramatically since March 2021.

522. The two injunction orders originally issued and procured by fraud respectively by the Palm Beach Circuit Court [against FLF's clients] and the Seminole County Circuit Court had been substantially overturned and remanded by the 4th and 5th District Courts of Appeal largely for being overly broad and in violation of the 1st Amendment of the United States Constitution.

523. By June 2023, in the Palm Beach Circuit Court Case, Threat Actor Defendant JTR had conceded on the record (which was memorialized by Court Order) that critical evidence submitted in support of its injunction was false and that it had prosecuted its injunction motion as to one of FLF's clients without having standing. JTR never sought the entry of another injunction order.

524. As well, by end of July 2023, the Seminole Circuit Court's Amended Injunction Order of April 2023, as with the Original of April 2021, found no evidence to have warranted any injunction against Caswell, Naughton or Power, and the Caswell, Naughton and Power Cases, as well as Heath, John and IOA's claims against those individuals in the 2020 SLAPP Lawsuit had been amicably resolved and the cases dismissed.

525. In March 2023, Farrow and Farrow Law, on behalf of Spagnuolo, filed a Second Amended Complaint in the 2019 Spagnuolo Case. In April 2023, Heath, John and IOA elected to remove the case to the Federal District Court for the Middle District of Florida citing federal question jurisdiction.

526. The SAC detailed, *inter alia,* that Spagnuolo's relationship with John Ritenour and IOA was significant, and scores of documents evidenced Spagnuolo was an IOA Insurance Agent and he and John Ritenour spent considerable time meeting with Spagnuolo's business contacts such as the Miami Dolphins, Boys & Girls Club, Exotic Car Dealers and The Learning Experience Pre-School's C-Level Executives.

527. Threat Actor Defendants' purposely and intentionally had concealed these emails from their production of documents which was nearly three years late and delivered, along with a malware payload, in August 2022.

528. Through the filing of the SAC in March 2024, Heath, John and IOA's strategic communications strategy developed with the guidance and assistance of FTI, was that Spagnuolo was a 'one time referral source' and never an IOA Agent.

529. In a sharp rebuke of the strategic communications narrative created in conjunction with FTI in 2019 that Spagnuolo was a 'one time referral source', the SAC cited Spagnuolo's IOA email address, signature block and authorization to use the IOA logo, as well as, detailed over 33 high-net worth business contacts Spagnuolo brought to IOA, and that John Ritenour had requested in writing that he personally attend the meetings Spagnuolo had arranged to land his contacts as IOA insurance clients.

March 2023 – Dr. Jane Doe and Infant Doe are Added as Targets of the APT

530. After the filing of the SAC in March 2023, Heath Ritenour received inquiries related to the evidence presented which directly contradicted the strategic communications narrative created in collaboration with FTI in 2019 regarding Spagnuolo's business relationship with IOA.

531. According to one IOA insider, Heath, John and IOA were 'neck deep in shit" immediate before the annual shareholder's meeting of 2023.

532. After the filing of the SAC in March 2023, the Theat Actor Defendants' APT was enhanced significantly evidenced by: (1) Dr. Jane Doe and Infant Doe were added as targets; and (2) the APTs operators began to substantial utilize Sitting Duck Cyber Attacks to rapidly advance achievement of the APT's Ultimate Goals.

VII. MARCH TO JULY 2024 - APT HYPERDRIVE

533. In early January 2024 through present, especially after February and March 2024, the Threat Actor Defendants' use of all vector attacks exponentially increased.

534. Importantly, from mid-January 2024 through July 2024 all, or substantially all, of the means and methods utilized by the Threat Actor Defendants exponential increased in utilization and frequency, corresponding in time to not only each other, but directly to pre-filing confidential communications, post-litigation events, and relevant non-litigation events directed to accomplish the Ultimate Goals.

535. More specifically, as alleged hereinbelow, the specific vector attacks which registered a massive explosion of activity from April through July 2024, included *inter alia:* (1) the Sitting Duck Attacks; (2) Farrow's Cell Phone Data Vulnerability; (3) Modifications to FLF's Network using administrative permissions and the collecting of specific file information related litigation involving JTR, Taylor and separately involving Heath, John, IOA, FTI and the insurance carriers; (4) spearing phishing emails directed at Farrow; (5) Installation of Unauthorized Software; (6) Application Repackaging; and (6) social engineering.

January through March 10, 2024

536. At the beginning of January 2024, Farrow and Farrow law received approximately 40 pages of discovery evidence relative to the 2019 Spagnuolo Lawsuit.

537. Within these 40 pages was evidence which established a critical misrepresentation that Heath, John and IOA had maintained since 2019.

538. Specifically, John Ritenour had represented in January 2019 that he would no longer be receiving any commission from the TLE Account because he was retiring.

539. However, after four years of delaying this discovery, not only had John Ritenour been receiving substantial commissions from the TLE Account, but he had opened JKR, LLC to receive the money such as to disguise the same from Spagnuolo and from discovery relative to the 2019 Spagnuolo Case.

540. In February and March, 2024, Farrow and Farrow Law began to research claims against the Carrier Defendants relative their appointment and reappointments of Heath Ritenour, John Ritenour and IOA.

March 10, 2024 through April 2024

541. By March 10, 2024, the Threat Actor Defendants had established strong foothold fortifications allowing them to monitor Farrow Law's Network and unauthorized access to the protected computers connected to same.

542. By March 10, 2024, Farrow and Farrow Law were preparing the draft original complaint in what would become the 2024 Federal Case.

543. At and around March 10, 2024, the Threat Actor Defendant had, since December and January 2024, began to escalate their conduct and activities as further alleged herein. The overwhelming majority of those activities were not discovered until after Farrow Law's effective closure on or about July 10, 2024.

544. At and around March 10, 2024, while Farrow and Farrow Law did not connect the observable activities to a concerted pattern of interference, they began to experience substantially increased situational events which were designed to drain resources and interrupt workflows, yet nevertheless, required attention of Farrow and Farrow Law's Staff.

545. An example is a March 10, 2024 email received from a former client which Farrow and Farrow Law represented but chose not to undertake further representation of him after a series of discussions.

546. Nevertheless, sometime after their last discussion, Farrow received a Bar Complaint[18] which Farrow responded to, and the Florida Bar Closed the file after receiving Farrow's response.

547. Farrow received this Bar Complaint well-after his last conversation with this former client wherein they discussed the client's most-recent additions to the scores of wounded or homeless stray dogs he had an incredible talent to find, nurture back to health and find homes for in the South Florida community.

548. Yet, in sharp contrast to their last conversation 18 months previously, the March 10, 2024 email states:

Jay Farrow

From: EDWARD CRESPO <musicandmore20@gmail.com>
Sent: Sunday, March 10, 2024 5:10 PM
To: Jay Farrow
Subject: What You Did Will NEVER Be Forgotten!
Attachments: Jay Lewis Farrow on Quora.pdf

Did you really think it was over? GUESS AGAIN! Although the SOL protects you from civil proceedings... it does NOT protect you from ME and my First Amendment rights! I've decided that it's time people knew exactly what kind of lawyer you really are! My AVVO review of you was the first step. This is the second step and there WILL be more! Good thing I saved all the court records and all our emails! I'm sure you enjoyed spending the money I paid you...FOR NOTHING!

[18] FLF and Farrow assert that this client's Bar Complaint, similar to the March 10, 2024 email, pdf and negative consumer post was directly and/or indirectly part of one of the Threat Actor Defendants' schemes to achieve their operational goals using unauthorized breaches into the Florida Bar Computer Network which will be alleged in a separate section, *infra,*

549. The pdf attached to the March 10, 2024 email contained the negative post and states:

> In Florida, the vast majority of lawyers DON'T GIVE A SHIT about VIOLATING the Bar Rule which prohibits them from taking on MORE cases than they can COMPETENTLY handle, (as long as the prospective client has the money to PAY them, of course). Investigators aren't much different. It's always about the MONEY!
>
> A perfect example is lawyer, JAY LEWIS FARROW of FARROW LAW, PA., whom I hired to represent me in an FDCPA / FCCPA case against Bank of America and its third party debt collectors, Aldridge Pite, LLP. I paid Jay Farrow over $7,500 in attorney's fees at $500 a month! The case was a "Slam-Dunk" for me, I had them dead-to-rights for violating both the state and federal debt collection laws, but Jay Farrow FUCKED UP my case and LOST me all my federal claims by FAILING to engage in a settlement discussion with Bank of America at the outset! He was "too busy" with OTHER cases! In regards to my remaining state claims, Jay Farrow THREW ME UNDER THE BUS by walking away from my case and refusing to file the state claims, like he promised me he would! JUST ANOTHER LYING, INCOMPETENT, FUCKING FLORIDA LAWYER who violated the Bar Rules and got away with it! He KEPT all the money I paid him in exchange for his sloppy, substandard, incompetent representation! The Bar Complaint I filed against him was, of course, summarily DISMISSED by the so-called "disciplinary" branch of the Florida Bar!
>
> I wonder HOW MANY people like me have filed valid, well-supported Bar Complaints against errant Florida lawyers like JAY LEWIS FARROW, only to have their intelligence INSULTED by the Florida Bar who always gives the SAME BULLSHIT EXCUSE THAT THE LAWYER DIDN'T VIOLATE ANY OF THE BAR RULES!
>
> Anyone who reads this and has had the same bad experience, PLEASE comment on this post! Thank you!

550. The March 10, 2024 email purportedly from this former client, the posted negative review and the pdf attached to the email was prepared by, directly or indirectly, by the Threat Actor Defendants using information which could only be accessed with a FLF Network Administrator Permission as it was in the FLF Administrator files which contained a copy of the alleged Florida Bar Complaint and Farrow's response.

551. Another example of creating a situational event to drain resources occurred on or about the same day as the receipt of the March 10, 2024 email referenced above, and related to the Threat Actor Defendants Heath Ritenour, John Ritenour and IOA had served an illegal subpoena on one of its vendors.

552. This event required immediate attention and drained resources.

553. On or about March 12 and 18, 2024, Farrow and Farrow Law filed a motions for sanctions for bad faith discovery conduct after discovering that Heath Ritenour, John Ritenour, IOA and Brian Moran served a subpoena upon one of Farrow and Farrow Law's business vendors which had a New York Case Caption, however, no New York Lawsuit had been filed and the actual subpoena requests had been objected to in the 2020 SLAPP Lawsuit without final resolution.

March 15, 2024 – the 2024 Federal Case

554. On March 15, 2024, Farrow and Farrow Law filed a federal lawsuit against several Insurance Carriers pursuant to the Florida and Federal Racketeering Statutes styled *Louis Spagnuolo v. American Casualty Company of Reading PA et al.,* United States District Court, Southern District of Florida, Case Number: 24-cv-60422-SMITH-HUNT (2024 Federal Case").

555. In the 2024 Federal Case, Farrow Law's client alleged that the Defendant Insurance Carriers participated in and profited from a criminal enterprise by, *inter alia,* using and retaining the benefits from Heath Ritenour, John Ritenour and IOA's deceptive conduct related to the RISK SCORE scam, stealing from agents such as Farrow Law's client and overbilling customers.

March 21, 2024 – Farrow and Farrow Law Discover Substantial New Evidence Related to Manipulating Judicial Proceedings

556. Subsequent to the filing of the 2024 Federal Lawsuit, on or about March 21, 2024, Farrow and Farrow Law discovered new evidence that substantial evidence existed that IOA, Heath Ritenour, John Ritenour, had conspired with FTI to enrich themselves using the TLE Account to bid rig insurance policies, and on the same day, discovered a concerted campaign to perpetrate fraud upon the court.

557. **At 5:06 am on March 21, 2024**, Farrow sent an email to one of his staff outlining in detail the discovery of how Heath, John and IOA had manipulated not just a discovery production, but also how these Defendants' bid rid insurance premiums for the large account which was procured by Spagnuolo back in 2014. This email stated as follows:

> Look at this letter stating that premium to client is $6702, then on spreadsheet they mislabled the policy number instead of a -04 they put -05, the premium billed claimed by ioa on their spreadsheet was 2149, with only a $191 premium billed, however, the spreadsheet says estimated premium of 8500 with no estimated commission. This is egregious and it goes on and on. Even the first example I sent last night, I found that they doubled the premium the next year. Look at the Hardford. None of these match at all, and one of the spreadsheets that we have been working off only goes fro 2019 through 2020, with so much information missing that makes it impossible to add up the figures, but one of the spreadsheets says over 6.7 million in premiums with 1.8 million in commissions billed. I check some of the numbers and they match the premium billed and commission billed, however, if there are bullshit numbers like a 6700 premium that was actually billed, and the spread sheet says only 2100, then its all fraudulent discovery...but what it does show is that the commissions reflected are far lower than premiums billed and that IOA is making up numbers to manipulate back end fees. The premiums billed to customers are real, but IOA's internal numbers show lower premiums were billed, the estimated premiums are always lower than actual premiums supposedly paid, which shows that the premiums billed are reflective of the lines. If you manipulate the spreadsheet to look at type of policies, you will see that most lines go to one company.

558. **On March 21, 2024**, Approximately three hours after Farrow sent an email to one of his staff outlining the discovery of newly discovered evidence, he received an email from what appeared to be a local newspaper which he was not subscribed and which did not send him 'periodic' news alerts – whatsoever.

Jay Farrow

From: Sun Sentinel Special Delivery <sunsentinel@nws.sun-sentinel.com>
Sent: Thursday, March 21, 2024 8:21 AM
To: Jay Farrow
Subject: SPECIAL REPORT: Florida's infant mortality crisis

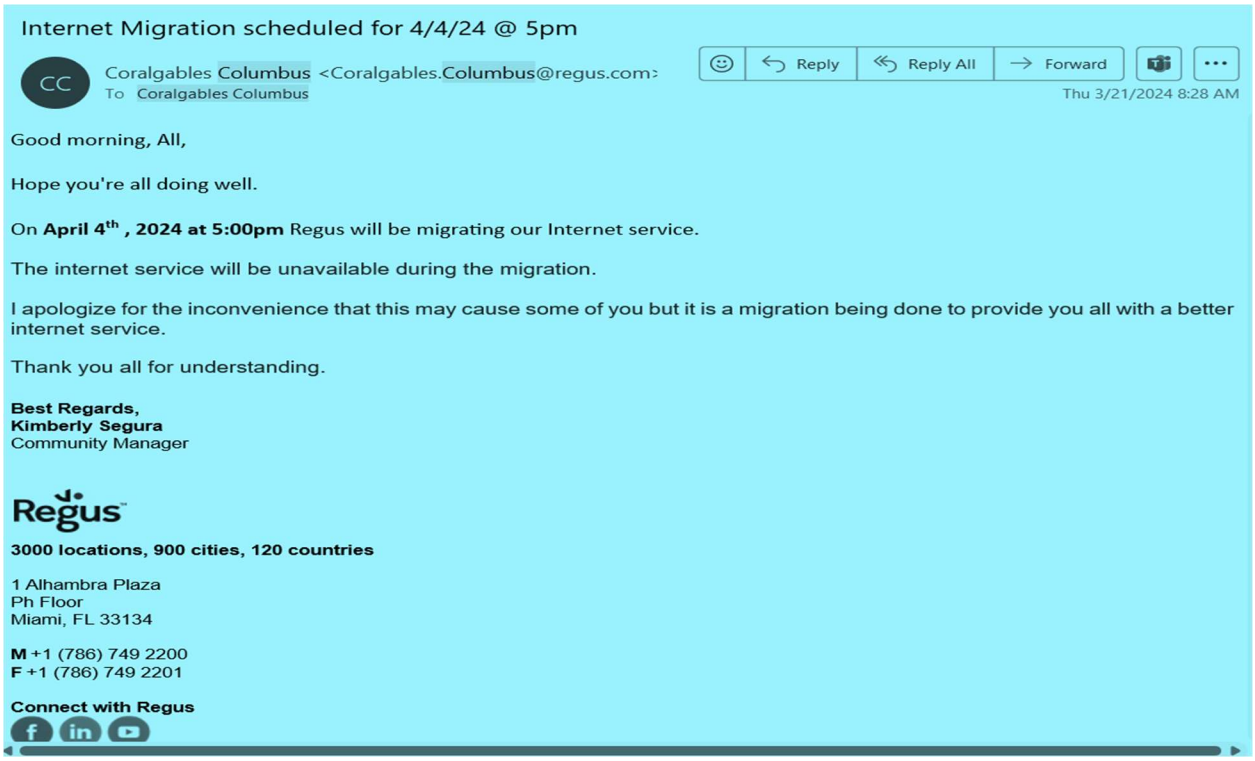
559. **MARCH 21, 2024: FARROW DISCOVERS SANYIABOOTH.COM**: On March 21, 2024, as well, Farrow discovered the sanyiabooth.org June 29, 2024 blog page while

conducting a search into Judge Stacy's online procedures without clearing a search related to Heath Ritenour.

560. Upon information and belief, the sanyiabooth.org website was and is a C2 Domain, and/or a C2 Dead Drop.

561. The result prompted an image of the blog page, which Farrow clicked on and discovered the photo of Judge Stacy, the hastaggs, the particular font size and colorings which mirrored Spagnuolo's social media posts.

562. **On March 21, 2024, seven minutes after receiving the INFANT MORTALITY Crisis warning from the Threat Actor Defendants**, again hours after Farrow sent an email to his staff regarding newly discovered evidence, at 8:28 AM from Farrow Law's landlord, Regus management purportedly to provide notices that on April 4, 2024, "Regus will be migrating our Internet service." The Regus email stated in relevant part:



Internet Migration scheduled for 4/4/24 @ 5pm

CC Coralgables Columbus <Coralgables.Columbus@regus.com>
To Coralgables Columbus

Reply | Reply All | Forward

Thu 3/21/2024 8:28 AM

Good morning, All,

Hope you're all doing well.

On **April 4th , 2024 at 5:00pm** Regus will be migrating our Internet service.

The internet service will be unavailable during the migration.

I apologize for the inconvenience that this may cause some of you but it is a migration being done to provide you all with a better internet service.

Thank you all for understanding.

Best Regards,
Kimberly Segura
Community Manager

Regus

3000 locations, 900 cities, 120 countries

1 Alhambra Plaza
Ph Floor
Miami, FL 33134

M +1 (786) 749 2200
F +1 (786) 749 2201

Connect with Regus

563. The Regus email was sent, directly or indirectly, by the Threat Actor Defendants for malicious purposes.

564. More specifically, the Threat Actor Defendants used at least two vector infiltrations of the Regus Network and achieved unauthorized access to the protected computers connected therewith, one of these vector exploits was through a Sitting Duck Attack which triggered a registered update to Regus' website domain's DNS records, and the other was through purportedly a 'migration' of its network's IP address to different servers.

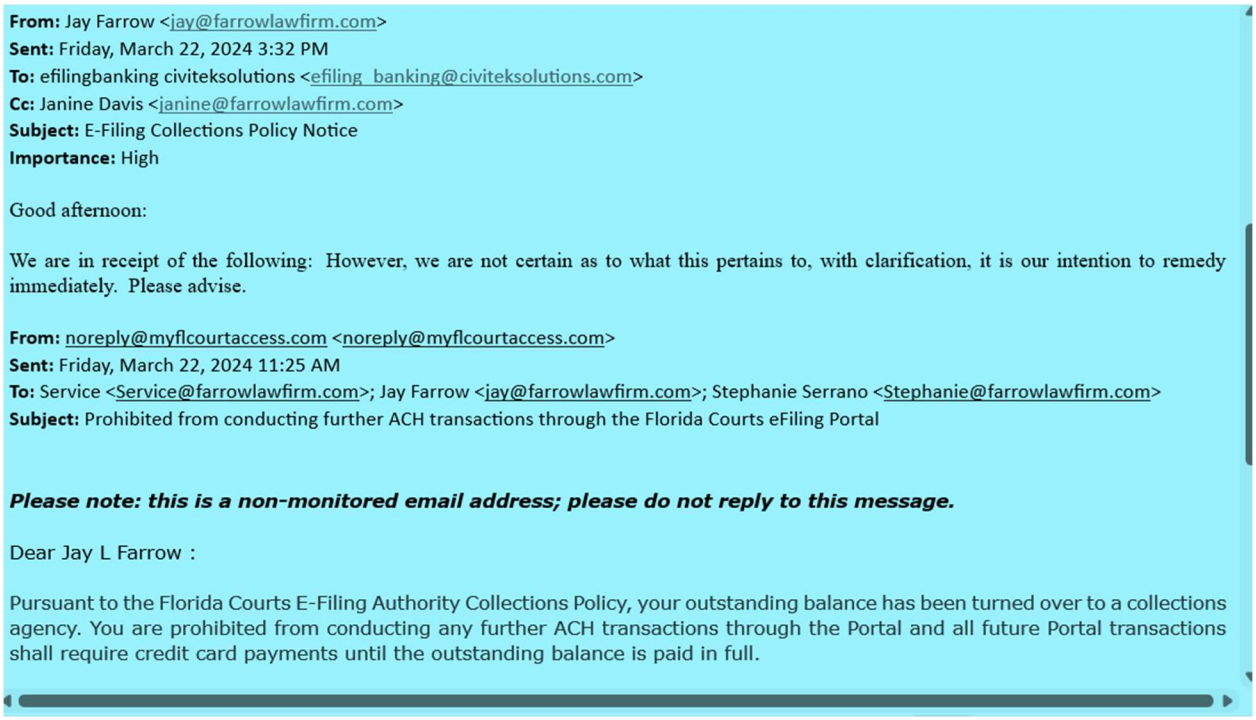
565. The infiltrations into the Regus network allowed the Threat Actor Defendants to infiltrate the Routers which supplied the Penthouse Offices at 1 Alhambra Plaza, in Coral Gables, with malware which they remotely controlled and used as a steppingstone to access the protected

computers belonging to the protected computers of over twenty other tenants who offices were adjacent to those of Farrow Law.

566. The Threat Actor Defendants conspired to and/or did commit these unauthorized infiltrations into protected computers referenced hereinabove for purposes of maintaining footholds in FLF's Network, computers and Farrow's cell phone, as wells as, lateral footholds in networks, computers and devices in strategic proximity.

567. **On March 22, 2024 at 3:32 p.m.**, the Threat Actor Defendants demonstrated that by that date and time, they were able to send an email from Farrow's business email address evidencing their access to Farrow Law's email accounts, such as jay@farrowlawfirm.com.

568. That is to say, the email cited below and incorporated herein, established that by at least March 22, 2024, the Threat Actor Defendants had unauthorized access into and were using Farrow's user account in the Farrow Law Network, and that they also had shared administrator permissions within Farrow Law's Network as of March 22, 2024.



From: Jay Farrow <jay@farrowlawfirm.com>
Sent: Friday, March 22, 2024 3:32 PM
To: efilingbanking civiteksolutions <efiling_banking@civiteksolutions.com>
Cc: Janine Davis <janine@farrowlawfirm.com>
Subject: E-Filing Collections Policy Notice
Importance: High

Good afternoon:

We are in receipt of the following: However, we are not certain as to what this pertains to, with clarification, it is our intention to remedy immediately. Please advise.

From: noreply@myflcourtaccess.com <noreply@myflcourtaccess.com>
Sent: Friday, March 22, 2024 11:25 AM
To: Service <Service@farrowlawfirm.com>; Jay Farrow <jay@farrowlawfirm.com>; Stephanie Serrano <Stephanie@farrowlawfirm.com>
Subject: Prohibited from conducting further ACH transactions through the Florida Courts eFiling Portal

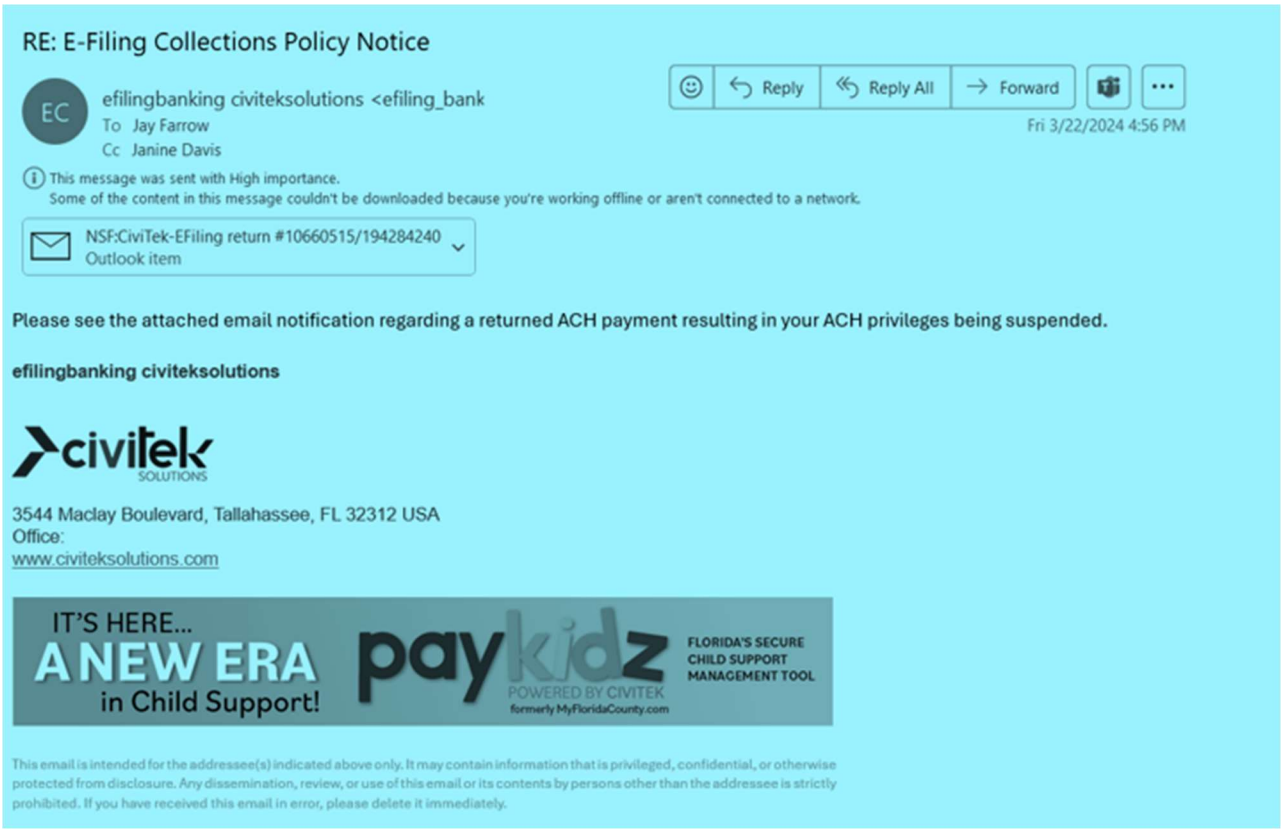
Please note: this is a non-monitored email address; please do not reply to this message.

Dear Jay L Farrow :

Pursuant to the Florida Courts E-Filing Authority Collections Policy, your outstanding balance has been turned over to a collections agency. You are prohibited from conducting any further ACH transactions through the Portal and all future Portal transactions shall require credit card payments until the outstanding balance is paid in full.

569. Analysis of this response dated March 22, 2024 from jay@farrowlawfirm.com to efilling_banking@civiteksolutions.com, evidences the Threat Actor Defendants using a variation of the MitM Attack.

570. In this March 22, 2024 response, which was sent approximately an hour after the Threat Actor Defendants sent an unauthorized email from jay@farrowlawfirm.com to efiling_banking@civiteksolution, the Threat Actor Defendants respond [to themselves essentially] with an email containing an attachment which was opened by either Farrow or one of Farrow Law's staff which delivered a malware payload into FLF's Network.


RE: E-Filing Collections Policy Notice

EC efilingbanking civiteksolutions <efiling_bank
To Jay Farrow
Cc Janine Davis

Reply | Reply All | Forward

Fri 3/22/2024 4:56 PM

This message was sent with High importance.
Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.

NSF:CiviTek-EFiling return #10660515/194284240
Outlook item

Please see the attached email notification regarding a returned ACH payment resulting in your ACH privileges being suspended.

efilingbanking civiteksolutions

civitek SOLUTIONS

3544 Maclay Boulevard, Tallahassee, FL 32312 USA
Office:
www.civiteksolutions.com

IT'S HERE...
A NEW ERA
in Child Support!

paykidz
POWERED BY CIVITEK
formerly MyFloridaCounty.com

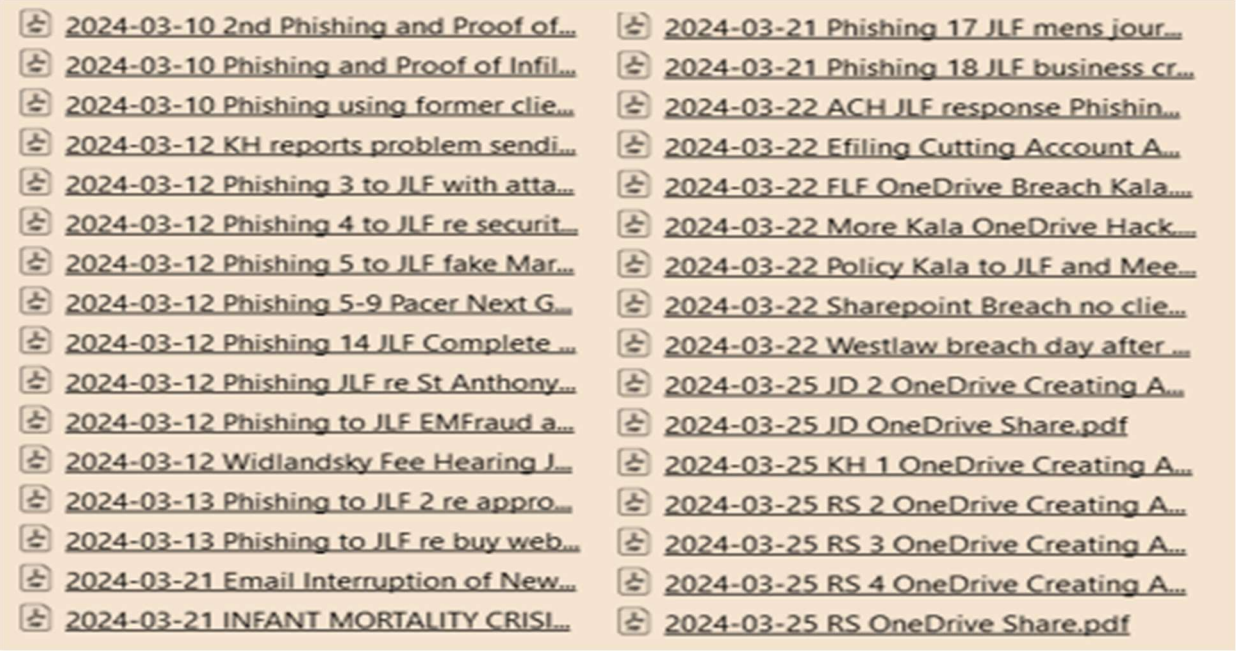
FLORIDA'S SECURE CHILD SUPPORT MANAGEMENT TOOL

This email is intended for the addressee(s) indicated above only. It may contain information that is privileged, confidential, or otherwise protected from disclosure. Any dissemination, review, or use of this email or its contents by persons other than the addressee is strictly prohibited. If you have received this email in error, please delete it immediately.

571. Moreover, the March 22, 2024 spear phishing emails directed to cause situational events requiring immediate or urgent attention, became a daily occurrence.

572. As the demonstrative below illustrates, between March 10, 2024 and March 25, 2024, there were over thirty (30) spear phishing emails directed at Farrow alone, may of the causing the same result, interferences with Farrow Law's workflows, schedules and which drained resources.

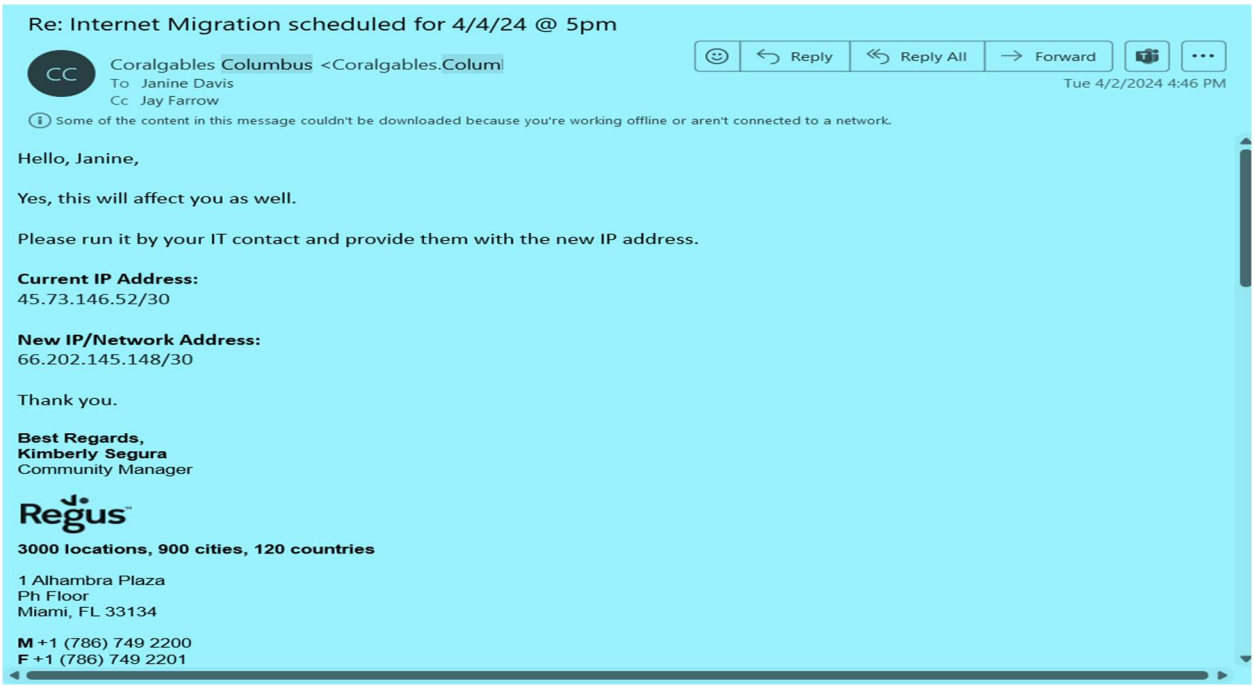
573. Upon information and belief, many of these spear phishing emails originated from the same IP address blocks which were used also by Defendants Kolaya, Moran, and their law firms, which resulted in spear phishing emails to resolve to IP addresses which would pass through the Farrow Law Network's anti-spam software as coming from a trusted source.



574. On April 2, 2024, emails sent directly or indirectly by the Threat Actor Defendants to Farrow and Farrow Law again related to its landlord, Regus', purported email migration, caused interferences with workflows and the expenditure of resources to conduct inquiries into if or how this 'migration' would affect Farrow Law's operations.

575. By example, on April 2, 2024, FLF's administrator contacted the firm's IT vendor who believed this 'migration' would not affect FLF's IP address or its network.

576. Upon receiving the response from the firm's IT vendor, on April 2, 2024, FLF's administrator emailed Regus and asked if this migration would change or alter Farrow Law's IP address, and the purported response stated it would and instructed her to pass along the new IP address to the firm's IT professionals.



Re: Internet Migration scheduled for 4/4/24 @ 5pm

CC Coralgables Columbus <Coralgables.Colum

To Janine Davis

Cc Jay Farrow

Reply | Reply All | Forward

Tue 4/2/2024 4:46 PM

Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.

Hello, Janine,

Yes, this will affect you as well.

Please run it by your IT contact and provide them with the new IP address.

Current IP Address:
45.73.146.52/30

New IP/Network Address:
66.202.145.148/30

Thank you.

Best Regards,
Kimberly Segura
Community Manager

Regus

3000 locations, 900 cities, 120 countries

1 Alhambra Plaza
Ph Floor
Miami, FL 33134

M +1 (786) 749 2200
F +1 (786) 749 2201

577. Notably, the April 2, 2024 response from Regus containing the IP address and the 'new' IP address was only sent to Farrow and Farrow Law, however, none of the other businesses and tenants received this information in March or April 2024, or through December 2024.

578. Moreover, the IP addresses listed above are not those of regus.com or Regus Management.

579. Upon information and belief, many of these spear phishing emails originated from the same IP address blocks which were used also by Defendants Kolaya, Moran, and their law firms, which resulted in spear phishing emails to resolve to IP addresses which would pass through the Farrow Law Network's anti-spam software as coming from a trusted source.

Remote Access, Monitoring, Surveillance and obtaining C2 Administrator Status

580. During this time period, between at least February 2023 and June 2024, the Threat Actor Defendants' abilities to remotely access the Farrow Law network and the individual

protected computers connected thereto allowed them to monitor work progress, calendar entries and the status of Farrow Law's financial affairs.

581. On or about April 8, 2024, Farrow and Farrow Law contacted Attorney Charles Meltz who represented Heath, John and IOA with regard to some of the litigation between them and Spagnuolo. The purpose of the call was to share with Mr. Meltz preliminary findings of Farrow and Farrow Law's investigation post-March 21, 2024.

582. On April 9, 2024, following Farrow's proffer of the newly discovered evidence and investigation findings to Heath, John and IOA's attorneys, all of FLF's staff received an email directly and/or indirectly by the Threat Actor Defendants purportedly from "Microsoft" request they change their passwords.

583. The April 9, 2024 emails caused immediate substantial interference with FLF's employees' workflows by requiring inquiries to the firm's IT professionals, as well as the sending of a firm-wide email which reported that the IT professionals instructed the was a spoof and which caused the firm's administrator to send an email to all employees and to speak with them in person.

BOGUS email from "Mircosoft"

Janine Davis

To Jay Farrow; Kala Hartle; Stephanie Serrano; Kate Shannon; Legal Assistant; Tanesha Blye; meera@koodielaw.com Tue 4/9/2024 1:53 PM

Reply Reply All Forward

This message was sent with High importance.

Hello all –

I just got an email from "Microsoft" asking to change my password because it was expiring. According to IT it is a bogus email. If you receive something similar, please delete and disregard.

Thank you!

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the cor...

Janine Davis
Non-Attorney
Client-Attorney Liaison
Chief Operating Officer
Farrow Law Firm
t: 954.252.9818
e: janine@farrowlawfirm.com
w: farrowlawfirm.com
a: 1 Alhambra Plaza - Floor PH - Coral Gables, FL 33134

CONFIDENTIALITY NOTICE: This electronic mail transmission has been sent by a law office. It may contain information that is confidential, privileged, proprietary, or otherwise legally exempt from disclosure. If you are not the intended recipient, you are hereby notified that you are not authorized to read, print, retain, copy or disseminate this message, any part of it, or any attachments. If you have received this message in error, please delete this message and any attachments from your system without reading the content and notify the sender immediately of the inadvertent transmission. There is no intent on the part of the sender to waive any privilege, including the attorney-client privilege, that may attach to this communication. Thank you for your cooperation. Please consider the environment before printing this e-mail.

584. On April 11, 2024, Farrow and Farrow Law prepared a motion to vacate an order entered on December 13, 2023 for fraud upon the federal court presiding over the 2019 Spagnuolo Case.

585. On April 12, 2024, the next day, Mr. Kolaya filed a motion to dismiss in the 2019 Spagnuolo Case in the Seminole County Circuit Court being presided over by Judge Spryenski and served Farrow Law and Farrow with the same.

586. At that time, the motion to dismiss contained highly developed arguments as to complex legal issues, was four months late and served hours after Farrow notified Kolaya of a motion detailing he and his client's fraud upon a federal court.

587. Upon inspection of the motion to dismiss' metadata which revealed it was not authored by Kolaya or his firm, was embedded with signing certificates, email certificates and other encodings which contained a malware payload.

588. As of April 13, 2024, Farrow had not detected that any pdf had delivered malware or that he, his law firm, wife and infant son were the targets of an APT. Yet, while undetected, this pdf, upon information and belief, contained a malware payload evidenced by modifications to Farrow Law's network as further alleged herein.

589. Nevertheless, the information which the metadata did reveal prompted Farrow to send Kolaya and his partner a correspondence inquiring about embedded code from the law firm of Greenberg Traurig.

April 13, 2024

SENT EMAIL TRANSMISSION
Timothy Kolaya, Esquire tkolaya@sknlaw.com
Ryan Stumphauzer, Esquire rstumphauzer@sknlaw.com
Stumphauzer Kolaya Nadler & Sloman PLLC

Re: Company Name: Greenberg Traurig
GTTagline: MIA 181,508,188v1 10-19-10
EMAIL_OWNER_ADDRESS: AAA2RgG6J6jCJ12/q/hxuMmsQLUybDl+ra70VVergpzQGk=
MAIL_MSG_ID1:aCAARdlFdK/mCW0R398lsQVDT0PRlNQh1hFsk5VoeCz6pmV6Qh/OHfm
V6IvArimdvIbVcjhaXkUZmDqLv/I7gDHZ8vPeaogZWz/2WrsC/juZVsIdfQwEHpI5Sb7tlzCdkwM
AGhJ1OUFxe4oeecMM/lylAg

Tim – Its one thing to make material misrepresentations during the course of a federal litigation to advantage your Client's position, and another to have utilized various means and methods which landed you and your firm as named defendants in a count regarding aiding and abetting Insurance Office of America, Inc., Heath Ritenour, John Ritenour and Valli Ritenour. However, when I discover that your firm is using software keys, email certificates and other seemingly proprietary organizational information in the latest of your attempts to obstruct, delay and then send a motion to dismiss to the state court judge after intentionally not responding to the Complaint for four months, I'm going to reiterate to you that I never thought you would find yourself in the spot you are in with these folks.

The information referenced above I will leave to you to research what it technically means, although I'll give you a head start in that all of those letters and numbers, the name of Greenberg Traurig as the company, that email owner and responder certificates and the "GTTagline" belong to your former law firm.

I hope you have come to know me as wanting to do the right thing, so I'm sure there's a plausible explanation for why this was in the metadata of the motion to dismiss someone at your firm conjured up today, because as I said, there is going to be a season of accountability and certain and swift consequences for direct or indirect misrepresentations to the Court. Like sending this Motion to Dismiss in for consideration under the Court's Rules to await a decision without a hearing.

590. On April 15, 2024, Defendant Kolaya wrote Farrow an email in response to the April 12 correspondence raising the concern about the embedded confidential metadata in Defendant Kolaya's April 12, 2024 motion to dismiss.

591. In Defendant Kolaya's email, he stated in relevant part that he was not "going to waste [his] time looking into [Farrow's] metadata concerns".

From: Timothy Kolaya <tkolaya@sknlaw.com>
Sent: Monday, April 15, 2024 9:52 AM
To: Jay Farrow <jay@farrowlawfirm.com>; Ryan Stumphauzer <rstumphauzer@sknlaw.com>
Cc: Stephanie Serrano <Stephanie@farrowlawfirm.com>; Janine Davis <janine@farrowlawfirm.com>; Kala Hartle <kala@farrowlawfirm.com>
Subject: RE: Greenberg Traurig Metadata Inquiry

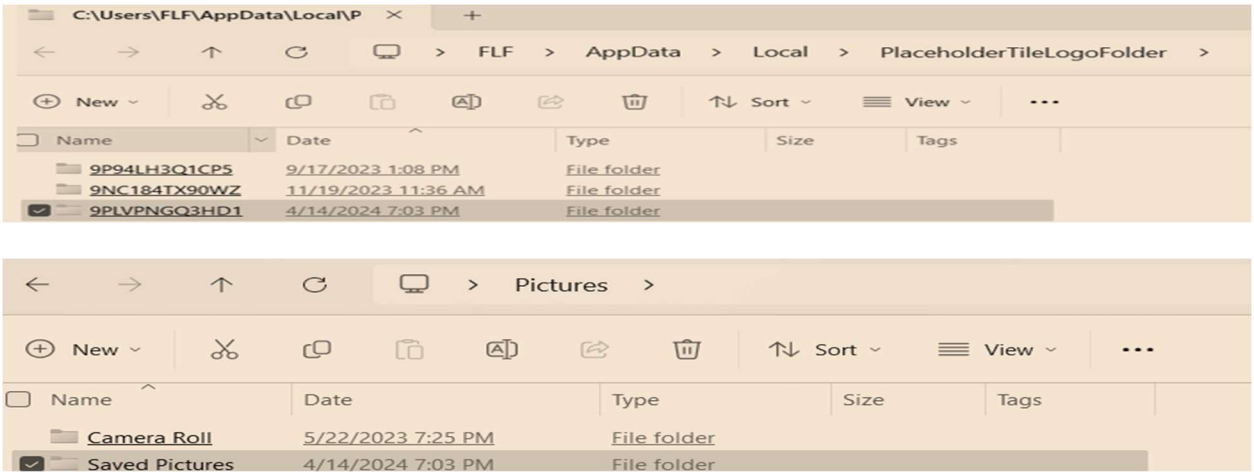
Jay –

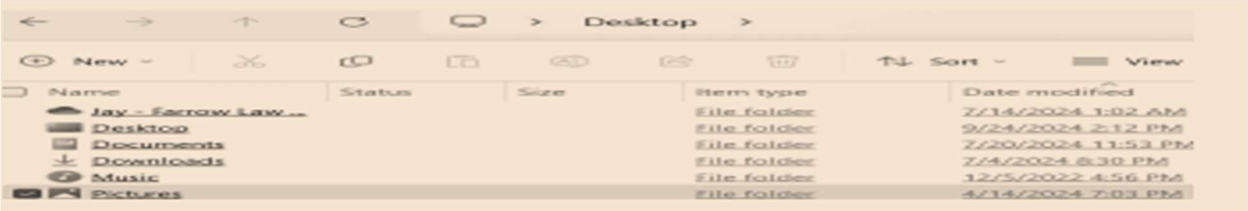
You are getting sidetracked on completely irrelevant issues. As I am sure you know, I left Greenberg Traurig in March 2019. I assure you that nobody at Greenberg Traurig has had any involvement in this case since that time.

I am not going to waste my time looking into your "metadata" concerns. I assume, like me, that you do not create every pleading or filing you prepare from scratch. Rather, when I have a new case, I typically open up an old Word document from a different case, save it as a new file, change the caption and title of the document, and then edit that document as needed.

When I left Greenberg Traurig in 2019, the firm transferred to me the case files (including old Word documents that were created using Greenberg Traurig's computers) for all of the clients that asked that I continue to work on their cases at my new firm. To the extent there is metadata indicating that somebody at "Greenberg Traurig" was the original author of the document I filed on Friday (or somehow identified in a metadata field), I am confident it is because of the process I described above.

592. Upon information and belief, Defendant Kolaya's April 12, 2024 email contained a malware payload, reflected, at least in part, by the installation of new program folders within 24 hours of Farrow opening the pdf motion from Mr. Kolaya.





APRIL 13, 2024 - Farrow Confidentially Discloses Results from Investigating New Evidence of March 21, 2024 and the Threat Actors' Digital Activities are Exponentially Registered on Five Separate Systems

593. On April 15 and 16, 2024, Farrow reached out to Mr. Meltz on behalf of Heath, John and IOA, and wrote an email to FTI directed at Steven Gunby, and two other C-Level FTI executives for purposes of scheduling a further discussion regarding the evidence discovered and his investigation.

594. Specifically, on April 16, 2024, Farrow emailed FTI's CEO Steven Gunby, FTI's CLO Curtis Lu and two others in the same email and specifically stated:

> …I wrote an email to Ms. Joanne Catanese at the recommendation of a colleague of mine, [Name Omitted], Senior Program Manager, Development Data Group, Development Economics at the World Bank. The purpose of my earlier email and of this correspondence is to schedule a call with one of you and Mr. Kevin Leung. The urgency of this matter cannot be understated as we have recently discovered evidence related to a case in Florida wherein FTI Counseling, Inc. prepared an "Investigative Report" and testified with regard to its findings with the report being introduced as evidence.

595. None of the recipients of the April 16, 2024, email responded from FTI, however, delivery receipts were received as to at least CEO Gunby and Attorney Lu.[19]

[19] In December 2024, Farrow discovered that this email has been deleted from view on his hard drive, whereas other emails sent and received on that date remain.

596. While CEO Gunby and his CLO Curtis Lu did not respond, the email receipts that establish that Steven Gunby and Curtis Lu opened the April 16, 2024, email is corroborated by the receipt of an email the following day by IOA, Heath Ritenour and John Ritenour's lawyers requesting that Farrow and Farrow Law cease communications with their 'expert."

Panic and Desperation Fuel Accelerated Timeline for Achievement of Effective Closure of Farrow Law P.A.

597. Importantly, through April 16 and even through May 2, 2024, Farrow endeavored to only share the newly discovered evidence and his investigation thereupon directly with Heath, John, IOA, FTI, and Gunby for purposes of attempting to receive feedback and such to possible avoid the filing of additional litigation with respect to the new evidence.

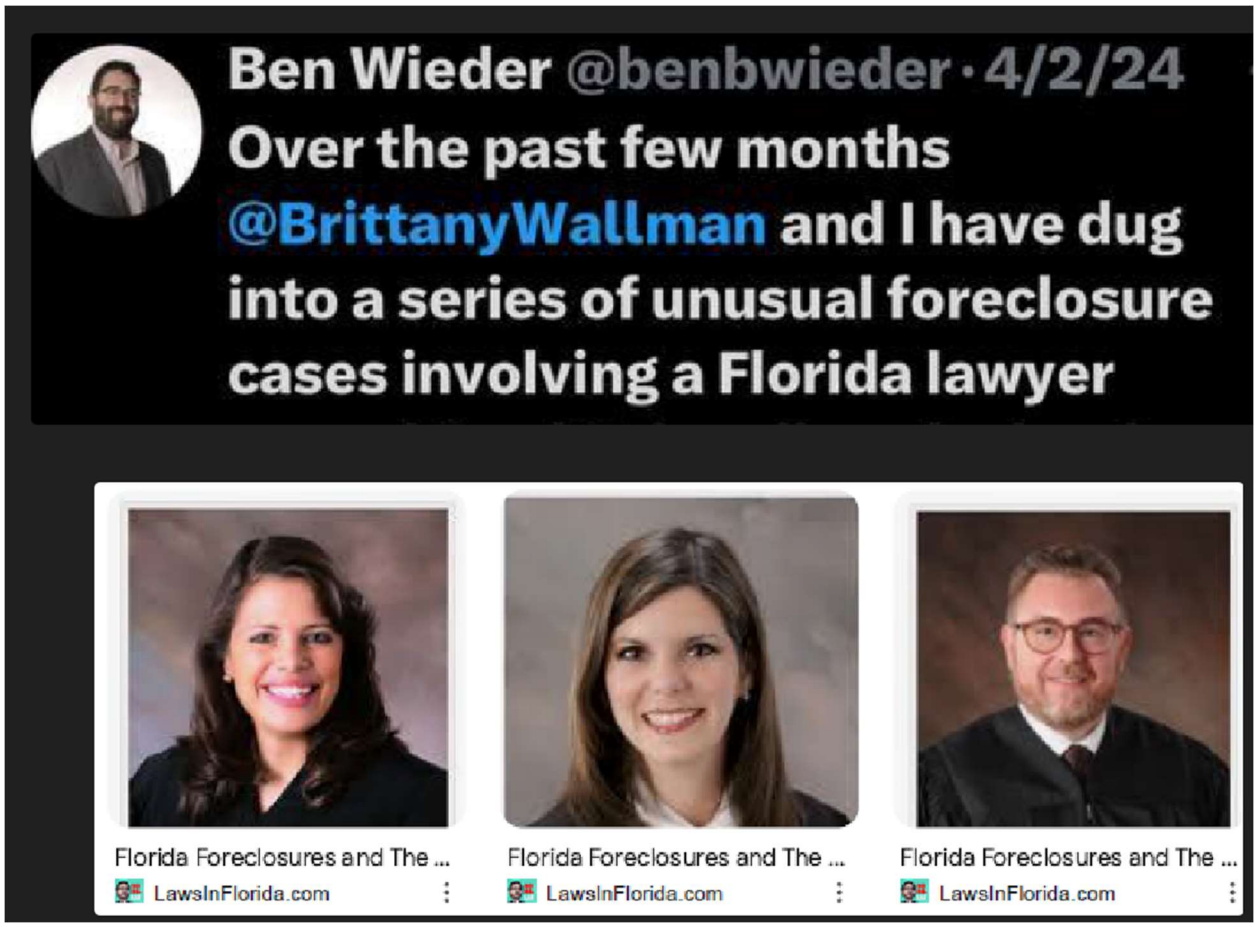
598. On or about April 24, 2024, Farrow discovered that 18th Judicial Circuit Judge Spryenski who was assigned to the Original 2019 Spagnuolo Case after its transfer from Broward Circuit Court became the third Seminole Circuit Court Judge to be defamed online directly and/or indirectly by the Threat Actor Defendants.

599. Here, on April 24, 2024, Farrow and Farrow discovered, that Judge Spryenski was featured on a website joined with Judge Susan Stacy and Judge Recksielder, both of whom were the subject of attacks on the sanyiabooth.org website.

600. Upon information and believe, the lawsinflorida.com website is a C2 Domain and/or a C2 Dead Drop.

601. In this article, purportedly research, written, published and/or contributed to by a purported journalist, "Ben Wieder", the three Seminole Circuit Court Judges are associated with a

2018 foreclosure scheme which allegedly occurred in Miami-Dade County wherein homes were 'stolen' by a Florida lawyer working with some Florida judges.



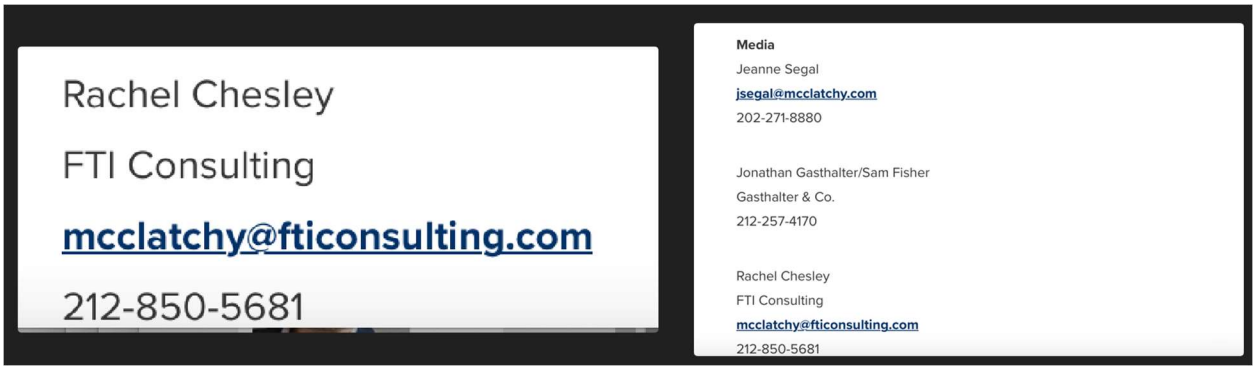
602. As with Sanyia Booth, Wieder's online profiles were stolen and//or created by the Threat Actor Defendants as part of their APT.

603. More specifically, Wieder's online profiles claim he works for various media outlets, such as the Miami Herald's Washington, D.C. Bureau, and also for McClatchy, a large news and media company which owns numerous newspapers throughout the United States, including the Miami Herald.

604. In 2019 or 2020, McClatchy went through a financial crisis and a bankruptcy, and hired FTI to provide services to it during that time.

605. As of December 2024, FTI touts that one of FTI's Senior Managing Directors, Rachel Chesley, works closely with McClatchy, especially handling its media relations.

606. In fact, McClatchy has its own FTI email, which is also one of Chesley's contact emails, to wit: mcclatchy@fticonsulting.com.



607. McClatchy is one of FTI's main outlets where it can publish stories through 'reporter' content portals of newspapers owned by McClatchy, which are routinely published by the subsidiary newspapers owned by McClatchy without meaningful review or editor scrutiny.

608. One of these newspapers is the Miami-Herald.

609. As of April 24, 2024, Farrow and Farrow Law discovered that not one, but two Circuit Court Judges in Seminole County who were presiding over two separate lawsuits involving the Threat Actor Defendants, Farrow and Farrow Law and their client Spagnuolo had articles presented negative and untrue statements against them online.

610. This discovery of April 24, 2024, which occurred days after Farrow wrote to Defendant Kolaya inquiring as to the metadata embedded in a court filing served upon Farrow on

April 12, 2024, prompted Farrow to write an email to Kolaya bringing this newly discovered attack on both Judge Spryenski and Judge Stacey.

611. As of the end of April 2024, Farrow did not file any legal filings containing the newly discovered evidence of frauds upon multiple courts, or related to the two websites negatively attacking two Seminole Circuit Court Judges.

612. More specifically, as alleged herein below, the unobservable massive seismic increase in the Threat Actor Defendants' conduct and activities in pursuit of their Ultimate Goals began after the filing of the March 15, 2024 Original Complaint in the 2024 Federal Case, and *before,* FTI was added as a party.

613. Thus, the only individuals with any knowledge of the newly discovered evidence that FTI had remote workers lacking expert credentials, that FTI, Heath Ritenour and IOA produced one of these fictitious experts at an evidently hearing, used an out of court campaign to manipulated judicial proceedings and that FTI had created false online profiles and websites to unlawfully influence judicial proceedings and to support Heath Ritenour and IOA's crisis management and strategic communications strategies, were, as of April 16, 2024 - Farrow, his staff/team, and Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, and FTI, Steven Gunby and his team.

614. On or about April 30, 2024, Farrow and Farrow Law were unaware that FTI, IOA, the Ritenours and/or other parties which were collaborating, consulting with, and/or having their own legal fees paid by IOA and Heath Ritenour, had already hacked into Farrow Law's Network, and the protected computers connected thereto, and were able to remotely monitor the work Farrow and Farrow Law were preforming for their clients.

615. By at least April 30, 2024, the Threat Actor Defendants had also gained unauthorized access to protected computers belonging to Farrow and Farrow Law's clients, lawyers vendors and contractors, and had used that access to receive, read and/or send emails from Farrow Law's office staff to these individuals and entities, and to also receive, read and/or send emails from these individuals and entities to, at the very least, Farrow and Farrow Law's staff using the MitM Cyber Attack.

616. By at least April 30, 2024, in order to accomplish the ability to receive, read and/or send emails from entities and individuals to Farrow and Farrow Law's staff, the Threat Actor Defendants had used unauthorized access into protected computers used in interstate commerce to compromise email servers of these collateral victims, and/or spoofed IP addresses and/or engaged in DNS Hijacking.

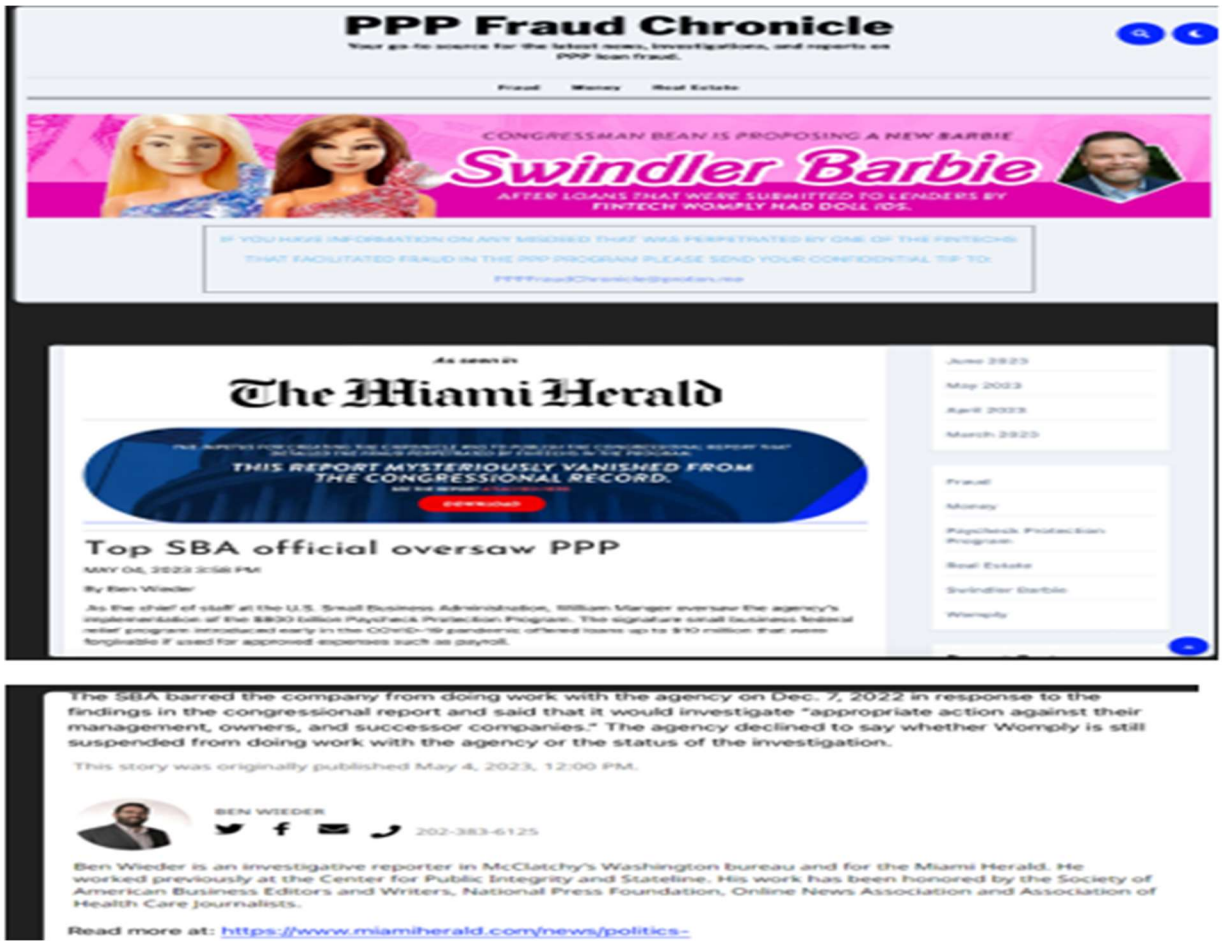
617. On May 2, 2024, after speaking to Defendant Moran, Farrow and Farrow Law filed, Spagnuolo's Verified Motion to Recuse or Disqualify Judge Stacy from the 2020 Seminole SLAPP Case.

FTI Uses its Media Outlets and Fictitious Social Media Journalist for Social Engineering Tactics

618. In May 2024, one of Farrow's contacts had suggested he speak with U.S. Congressman Aaron Bean or his staff regarding connecting with Gunby, or FTI, and subsequently this contact coordinated a conversation with one of Congressman Bean's senior staff members, which was through text message to Farrow's cell phone.

619. In or about May 2024, around the time Farrow was schedule a call with Congressman Bean's Office, another media publication attributed to Ben Wieder, this time as an alleged reporter for the Miami-Herald, which related to the payroll protection program.

620. However, identical to the sanyiabooth.org and lawsinflorida.com websites, the article only briefly mentions the Congressman Bean, yet its cover page graphics negatively attack him.



The SBA barred the company from doing work with the agency on Dec. 7, 2022 in response to the findings in the congressional report and said that it would investigate "appropriate action against their management, owners, and successor companies." The agency declined to say whether Womply is still suspended from doing work with the agency or the status of the investigation.

This story was originally published May 4, 2023, 12:00 PM.

BEN WIEDER
202-383-6125

Ben Wieder is an investigative reporter in McClatchy's Washington bureau and for the Miami Herald. He worked previously at the Center for Public Integrity and Stateline. His work has been honored by the Society of American Business Editors and Writers, National Press Foundation, Online News Association and Association of Health Care Journalists.

Read more at: https://www.miamiherald.com/news/politics-

May 2024 - Steven Gunby and Top Four C-Level FTI Executives Make Historical Sale of Personal FTI Stock

621. In or about the beginning of May through May 22, 2024, five C-Level FTI executives with knowledge of Farrow's reporting of his discovery of new evidence related to FTI's manipulation of judicial proceedings using fake experts who work remotely and do not have the qualifications or credentials which are listed on FTI's website and/or their LinkedIn Social Media provides, and/or with knowledge of the contents of Farrow's Motion to Disqualify, intentionally directed the sale of a percentage of their FTI stock.

622. The sale of FTI stock by five C-Level executives, including CEO Gunby and its CFO Linton Paul Alderman were historically unprecedented in FTI's history.

623. Collectively, these five FTI executives sold approximately $36,000,000.00 in FTI Stock between April 30, 2024 and May 22, 2024 at a time when the price of the stock was at near a record high. This activity was characterized as insider "panicking."

SABHERWAL AJAY Chief Financial Officer	Sale at price 226.13 per share.	Direct	134,773	May 22, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Stock Gift at price 0.00 per share.	Direct	0	May 21, 2024
PAUL HOLLY Officer	Sale at price 224.00 per share.	Direct	197,344	May 21, 2024
SABHERWAL AJAY Chief Financial Officer	Sale at price 226.13 per share.	Direct	634,069	May 20, 2024
LINTON PAUL ALDERMAN Officer	Sale at price 222.57 - 223.22 per share.	Direct	696,496	May 15, 2024
SABHERWAL AJAY Chief Financial Officer	Sale at price 226.13 per share.	Direct	134,773	May 22, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Stock Gift at price 0.00 per share.	Direct	0	May 21, 2024
PAUL HOLLY Officer	Sale at price 224.00 per share.	Direct	197,344	May 21, 2024
SABHERWAL AJAY Chief Financial Officer	Sale at price 226.13 per share.	Direct	634,069	May 20, 2024
LINTON PAUL ALDERMAN Officer	Sale at price 222.57 - 223.22 per share.	Direct	696,496	May 15, 2024

LINTON PAUL ALDERMAN Officer	Conversion of Exercise of derivative security at price 36.87 per share.	Direct	225,902	May 15, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Sale at price 220.52 - 222.06 per share.	Direct	9,225,169	May 10, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Conversion of Exercise of derivative security at price 40.36 per share.	Direct	1,685,999	May 10, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Stock Gift at price 0.00 per share.	Direct	0	May 9, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Sale at price 218.61 - 220.34 per share.	Direct	7,472,986	May 9, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Conversion of Exercise of derivative security at price 40.36 per share.	Direct	1,377,850	May 9, 2024
HOLTHAUS GERARD E Director	Stock Gift at price 0.00 per share.	Direct	0	May 7, 2024
HOLTHAUS GERARD E Director	Sale at price 221.14 per share.	Direct	329,941	May 7, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Sale at price 212.80 - 214.36 per share.	Direct	5,814,413	May 2, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Conversion of Exercise of derivative security at price 34.33 per share.	Direct	936,042	May 2, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Sale at price 212.97 per share.	Direct	9,394,746	May 1, 2024
GUNBY STEVEN HENRY Chief Executive Officer	Conversion of Exercise of derivative security at price 34.33 per share.	Direct	1,514,399	May 1, 2024
LINTON PAUL ALDERMAN Officer	Sale at price 216.43 - 217.22 per share.	Direct	3,588,186	Apr 30, 2024
LINTON PAUL ALDERMAN Officer	Conversion of Exercise of derivative security at price 36.75 per share.	Direct	975,786	Apr 30, 2024

624. Having five (5) of the top C-Level Executives selling FTI at the same time, as well as the amount of stock being sold collectively, had either never before occurred, or had never occurred between 2020 and May 2024.

625. The street value of the shares was approximately $36,000,000.00, which was at a time when FTI's stock was at near all-time highs. This activity was characterized as insider "panicking."[20]

[20] FTI Consulting Executives 2024 (USA Stocks:FCN) (macroaxis.com)

626. Farrow emailed CEO Gunby and Curtis Lu in another attempt to have a discussion prior to filing an amended complaint in the 2024 Federal Case.

627. In response, on May 16, 2024, Farrow received a response from FTI's Chief Legal Officer Curtis Lue who directed him to Attorney William Hill, a Miami Based Lawyer with the Gunster Law Firm.

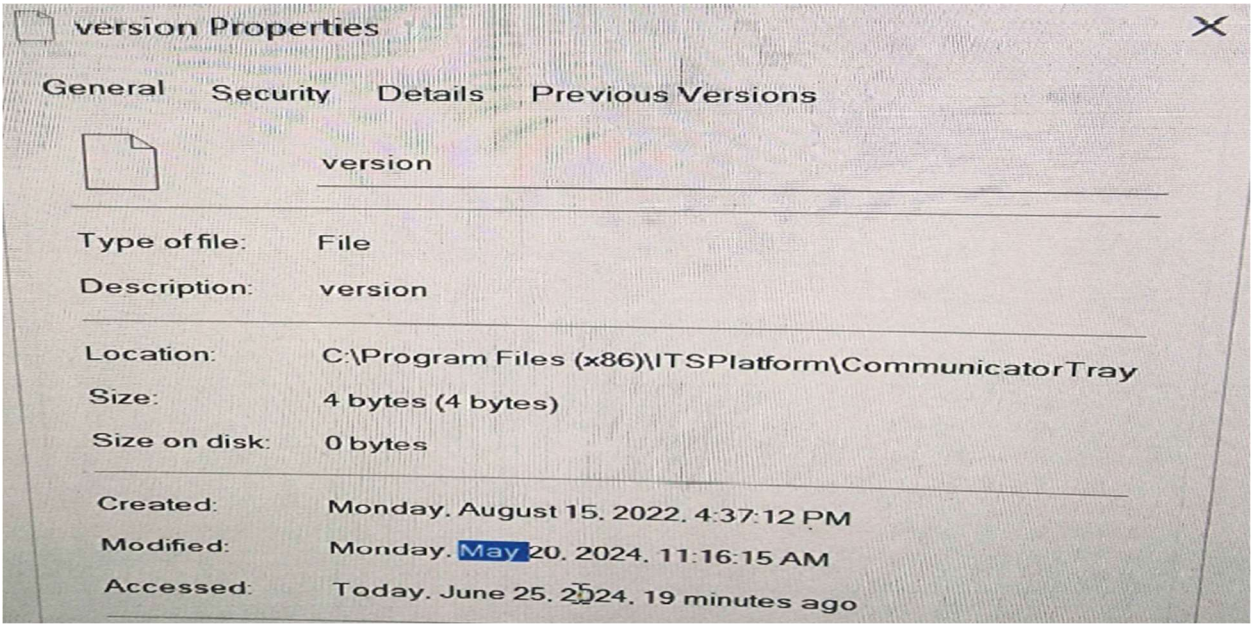
628. On May 17, 2024, Farrow and Attorney Hill spoke on the phone. During that conversation, Farrow mentioned the anomaly of the insider sale of FTI stock as a matter of fact.

629. After that May 17, 2024 conversation**, less than $1MM of the $36MM was sold as referenced in the above chart**.

630. At or about 8:00am Monday, May 20, 2024, Farrow sent FTI's Miami Based Attorney written factual outline of new evidence for his review.

631. Three hours later, at 11:16am, Defendants used fortified footholds within Farrow Law's Network to make modifications to critical Program Files as the Threat Actor Defendants

prepared to exfiltrate data, and files, while sabotaging Farrow Law's network and business operations.



May 2024 through July 10, 2024 - Observable Activities and Conduct Resulting in Effective Closure of Farrow Law on July 10, 2024

632. After May 28, 2024, the Threat Actor Defendants' 'observable' activities and conduct substantially increased literally overnight.

633. On May 28 2024, after returning to CEO Gunby one more time with no response to the proffered evidence, Farrow filed an Amended Complaint in the 2024 Federal Case which named FTI as a Defendant.

634. By June 3, 2024, Farrow had nearly completed an amended injunction motion for filing in the 2024 Federal Case.

635. As of June 3, 2024, Farrow and Farrow Law had not discovered that Gunby, and the other four executives who had just sold FTI stock, were preparing for FTI's annual shareholder's meeting to take place on or about June 5, 2024, where they were all seeking reelection to their current executive positions.

636. **On June 3, 2024,** Farrow received a call from a Verified Number he did not recognize.

637. Farrow did not answer the call, however, immediately noticed the 'verified number' had left a text message with a photograph of Farrow holding Infant Doe on the day he was born, some twenty months before June 3, 2024.

638. This photograph was not taken by Farrow's cell phone, or that of Dr. Doe.

639. This photograph was never posted by anyone's social media account.

640. This photo was taken either by one of Farrow or Dr. Doe's close family members, or by hospital staff as they were the only individuals permitted in the hospital room that day.

641. The photo and the verified call came from an individual who works for one of FTI's larger clients, Charter Communications. This individual has a business relationship with an FTI 'director' that has directly and/or indirect connections with a web developer working for John Ritenour in 2020 and 2021.

642. The Threat Actor Defendants sent Farrow the photograph which demonstrated a level of high technological sophistication.

643. In rapid succession on June 3, 2024, Farrow received spear-phishing emails from the Threat Actor Defendants which appeared to be from his paralegal, a potential client, and Farrow Law's IT vendor, but all were fake and designed to interfere with Farrow's workflow and/or contained malware payloads.

644. On June 5, 2024, FTI held its annual shareholder's meeting with respect to the election of executive officers.

645. At the June 5, 2024 shareholder meeting, and all of the other four C-Level executives which sold FTI stock between April 30, 2024 and May 22, 2024 having insider information, were also reelected to their executive positions.

646. On June 6, 2024, Farrow and Farrow Law filed on behalf of Spagnuolo in the 2024 Federal Case, an Amended Motion for Injunction.

647. In the Amended Motion for Injunction, Farrow and Farrow Law's client Spagnuolo specifically detailed the relationship, roles and activities of Heath, John and IOA and the Carrier Defendants with respect to an alleged bid rigging scheme involving the thousands of insurance policies written each year for the TLE Account, and also alleged FTI's relationship to the Carrier

Defendants which involves the systemic mitigation of financial exposure of insurance carriers by using remote workers as bogus experts to eliminate or reduce policy claims.

648. On June 4 and especially after June 6, 2024, the date Farrow filed the Amended Injunction Motion in the 2024 RICO Case, Farrow began to receive a substantial increase in AI voice generated calls from purported clients, staff members and family members which were made direct or indirectly by the Threat Actor Defendants.

649. These AI Voice calls were designed to, and did in fact, create a situational crisis event, in other words, the content of the call related to a purported event or set of circumstances which had occurred, the result of the same required immediate attention, and the expending of resources.

650. At the same time, on June 3 and especially after June 6, 2024, the number of targeted phishing and spear phishing emails direct to Farrow and Farrow Law's staff and its clients, such as Spagnuolo, increased dramatically.

651. After the filing of the May 28, 2024 Amended Complaint in the 2024 Federal Case, the spear phishing emails which had previously been substantially for the purpose of exploiting a vector vulnerability to implant malware, had shifted to being overwhelmingly designed to cause situational crisis events to disrupt and interfere with Farrow Law's operations and staff workflows.

652. The AI Voice Calls and these spear phishing emails designed to cause situational crisis events were sent by the Threat Actor Defendants to Farrow and Farrow Law's staff at strategic times, which were before client meetings, or court hearings.

653. These AI Voice Calls and spear phishing emails came from purported trusted sources, which included: (1) Farrow and Farrow Law's legal counsel; (2) Clients; (3) a news

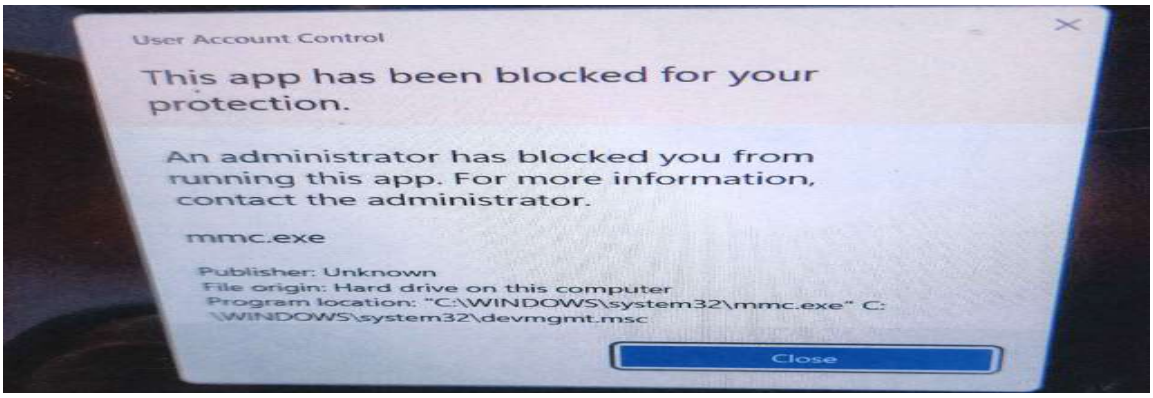
reporter who had published a story in the Daily Business Review; (4) Farrow Law's IT vendor, (5) a long-time contract attorney; (6) Farrow's parents' personal email; and (7) from Farrow's personal yahoo.com address to his Farrow Law email address.

654. The purpose of these AI Voice Calls and spear phishing emails directed at causing situational crisis events were sent by the Threat Actor Defendants to interfere with, confuse and cause Farrow Law's staff to waste resources.

655. The purpose of the AI Voice Calls and spear phishing emails was also to overwhelm Farrow and Farrow Law's staff using a tradecraft tool known as white noise. That is to say, the Threat Actor Defendants purpose was to manufacture as many events as possible, which they accomplished by taxing resources while they also were exfiltrating and stealing information, data and evidence and using their administrator status within Farrow Law's network to cover tracks which are the final sequence framework structures of the APT.

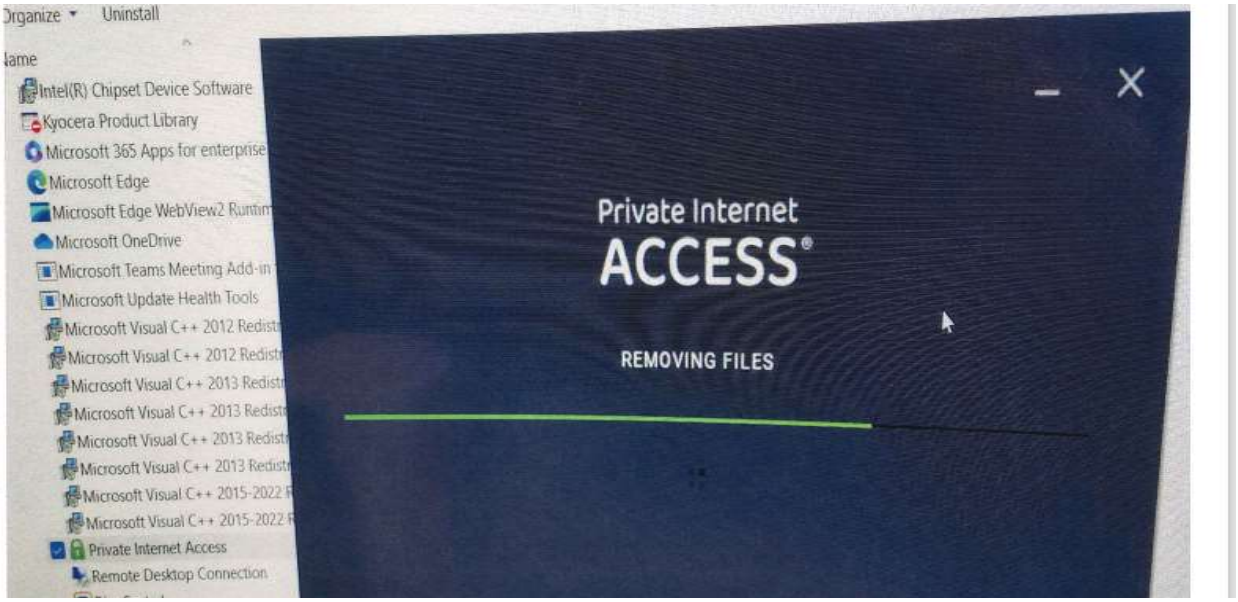
656. By June 6, 2024, while unknown at that time, Farrow lost most if not all administrator permissions over the FLF Network with the Threat Actor Defendants having full administrator or co-administrator status. After June 6, 2024, Farrow began to detect losses to his administrator user status, such as receiving pop-up notifications for the first time in over 16 years that he was denied access to a FLF Network file.

657. On or about June 11, 2024, Farrow began to receive repeated messages while using his business Lenovo laptop which stated that another administrator had blocked him from opening applications and other files.



658. In response, from about June 12, 2024 through present, Farrow and Farrow law regularly took screenshots of Farrow's computer and cell phone, as well as photographs of the screens of computers connected to the FLF Network such to document new obstruction or interferences.

659. In several instances, beginning or about June 12, 2024, Farrow's business computer would suddenly switch to a screen which stated that a remote user was removing files.



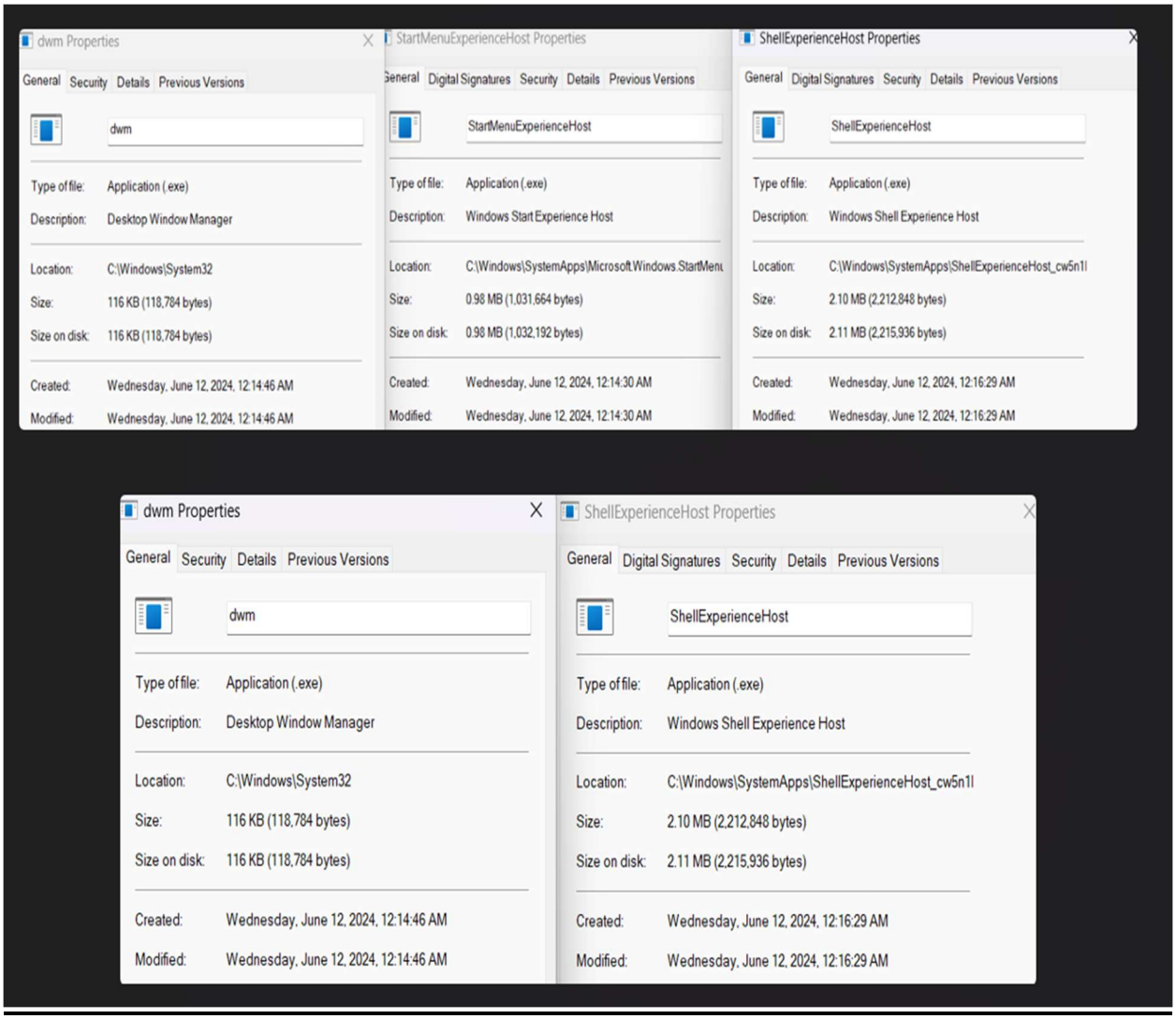
660. On June 11 and 12, 2024, through July 3, 2024, Farrow and Farrow Law's employees experience significant and substantial delays of the otherwise automatic network syncing of document versions, calendar updates and receipt of interoffice emails. This caused substantial interferences with Farrow Law's business operations and employee workflows and was caused by the Threat Actor Defendants issuing remote commands to exfiltrate data and modifying and/or deleting files.

661. **On June 12 2024**, several executable files and shells were created at or around the same time which were installed by the Threat Actor Defendants for purposes of obtaining their Ultimate Goals, especially severing and/or substantial intervening with Farrow and Farrow Law's communications and procuring the effective closure of Farrow Law within weeks.

662. **On June 12, 2024** the Threat Actor Defendants FTI and the Carrier Defendants, requested a sixty-day extension of time to respond to the June 6, 2024 Amended Injunction Motion. Farrow, on behalf of his client agreed, making the Joint Response due on or about August 5, 2024. This request was made in bad faith and for purposes of ensuring that Farrow, Farrow Law and their Client would not be able to present the evidence in support of that motion, reply to Defendants' response or otherwise delay the litigation for malicious purposes.

663. **On June 12, 2024**, before and after, Farrow wrote an email to the lead counsel for some of the Carrier Defendants who had taken a leadership role in speaking and communicating with Farrow, the Farrow Law Network received remote commands installing over fifty executable programs, application modifications and also which exfiltrated confidential information.

664. The screenshots below provide the precise name of some of the malicious files created on June 12, 2024:

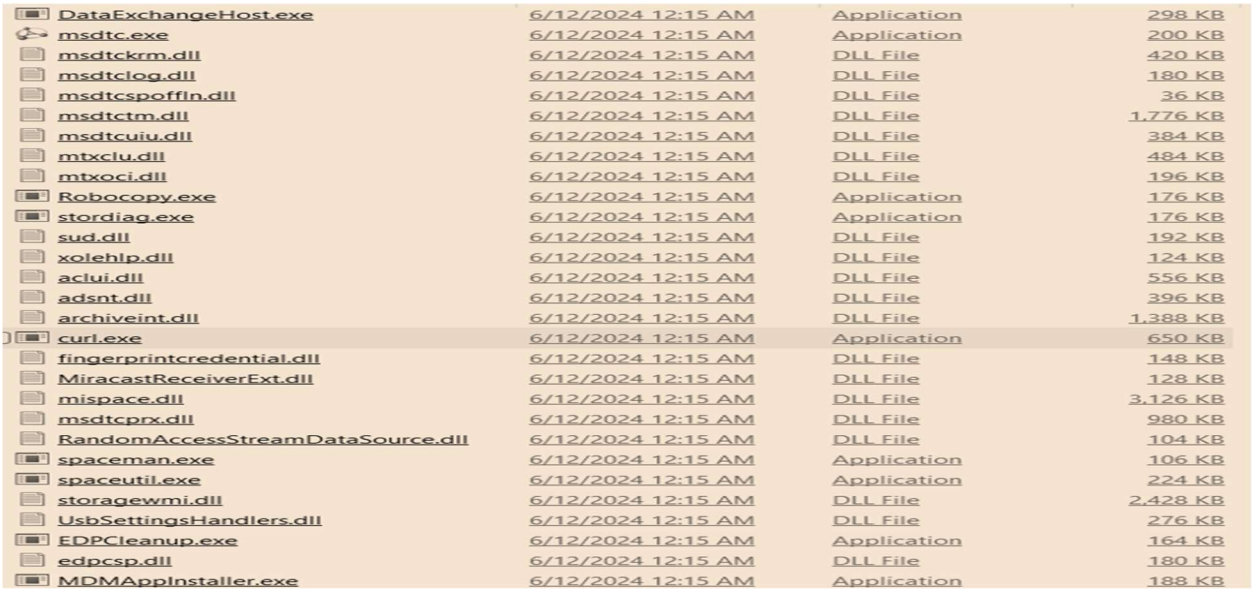


665. Additional screenshots of the scores of files being implanted, or executed by the Threat Actor Defendants using remote access control directed to advance their permissions while down grading those of Farrow, and for purposes of exfiltrating, for example, the 2024 Federal Case File and other files such as those related to JTR, Taylor, and others.

666. This June 12, 2024 activity was discovered in January 2025 and extracted from Farrow's Lenovo Laptop computer, and consists of scores of modifications to DLL files, the creation of others and the installation of application repackages – all of which was designed to

accomplish the Threat Actor Defendants Ultimate Goals by the end of June or the beginning or July 2024. More specifically, the conduct and activities on June 12, 2024 alone just after 12:00 is provided, in part, hereinbelow:

themecpl.dll	6/12/2024 12:16 AM	DLL File	504 KB
credwiz.exe	6/12/2024 12:16 AM	Application	100 KB
FrameServer.dll	6/12/2024 12:16 AM	DLL File	1,304 KB
FrameServerClient.dll	6/12/2024 12:16 AM	DLL File	624 KB
FrameServerMonitor.dll	6/12/2024 12:16 AM	DLL File	340 KB
mfsensorgroup.dll	6/12/2024 12:16 AM	DLL File	518 KB
rdpcorets.dll	6/12/2024 12:16 AM	DLL File	1,732 KB
SyncCenter.dll	6/12/2024 12:16 AM	DLL File	560 KB
Windows.System.Profile.HardwareId.dll	6/12/2024 12:16 AM	DLL File	167 KB
wsp_fs.dll	6/12/2024 12:16 AM	DLL File	1,902 KB
wsp_health.dll	6/12/2024 12:16 AM	DLL File	1,662 KB
DAFIPP.dll	6/12/2024 12:16 AM	DLL File	372 KB
DAFMCP.dll	6/12/2024 12:16 AM	DLL File	304 KB
McpManagementService.dll	6/12/2024 12:16 AM	DLL File	268 KB
powercfg.cpl	6/12/2024 12:16 AM	Control panel item	268 KB
PrintWSDAHost.dll	6/12/2024 12:16 AM	DLL File	164 KB
RdpAvenc.dll	6/12/2024 12:16 AM	DLL File	258 KB
reseteng.dll	6/12/2024 12:16 AM	DLL File	620 KB
ResetEngine.dll	6/12/2024 12:16 AM	DLL File	2,618 KB
ResetEngOnline.dll	6/12/2024 12:16 AM	DLL File	212 KB
ContactHarvesterDS.dll	6/12/2024 12:16 AM	DLL File	256 KB
fodhelper.exe	6/12/2024 12:16 AM	Application	100 KB
LocationWinPalMisc.dll	6/12/2024 12:16 AM	DLL File	156 KB
msi.dll	6/12/2024 12:16 AM	DLL File	3,440 KB
msisip.dll	6/12/2024 12:16 AM	DLL File	92 KB
opengl32.dll	6/12/2024 12:16 AM	DLL File	912 KB
perfmon.exe	6/12/2024 12:16 AM	Application	176 KB
resmon.exe	6/12/2024 12:16 AM	Application	128 KB



DataExchangeHost.exe	6/12/2024 12:15 AM	Application	298 KB
msdtc.exe	6/12/2024 12:15 AM	Application	200 KB
msdtckrm.dll	6/12/2024 12:15 AM	DLL File	420 KB
msdtclog.dll	6/12/2024 12:15 AM	DLL File	180 KB
msdtcspoffln.dll	6/12/2024 12:15 AM	DLL File	36 KB
msdtctm.dll	6/12/2024 12:15 AM	DLL File	1,776 KB
msdtcuiu.dll	6/12/2024 12:15 AM	DLL File	384 KB
mtxclu.dll	6/12/2024 12:15 AM	DLL File	484 KB
mtxoci.dll	6/12/2024 12:15 AM	DLL File	196 KB
Robocopy.exe	6/12/2024 12:15 AM	Application	176 KB
stordiag.exe	6/12/2024 12:15 AM	Application	176 KB
sud.dll	6/12/2024 12:15 AM	DLL File	192 KB
xolehlp.dll	6/12/2024 12:15 AM	DLL File	124 KB
aclui.dll	6/12/2024 12:15 AM	DLL File	556 KB
adsnt.dll	6/12/2024 12:15 AM	DLL File	396 KB
archiveint.dll	6/12/2024 12:15 AM	DLL File	1,388 KB
curl.exe	6/12/2024 12:15 AM	Application	650 KB
fingerprintcredential.dll	6/12/2024 12:15 AM	DLL File	148 KB
MiracastReceiverExt.dll	6/12/2024 12:15 AM	DLL File	128 KB
mispace.dll	6/12/2024 12:15 AM	DLL File	3,126 KB
msdtcprx.dll	6/12/2024 12:15 AM	DLL File	980 KB
RandomAccessStreamDataSource.dll	6/12/2024 12:15 AM	DLL File	104 KB
spaceman.exe	6/12/2024 12:15 AM	Application	106 KB
spaceutil.exe	6/12/2024 12:15 AM	Application	224 KB
storagewmi.dll	6/12/2024 12:15 AM	DLL File	2,428 KB
UsbSettingsHandlers.dll	6/12/2024 12:15 AM	DLL File	276 KB
EDPCleanup.exe	6/12/2024 12:15 AM	Application	164 KB
edpcsp.dll	6/12/2024 12:15 AM	DLL File	180 KB
MDMAppInstaller.exe	6/12/2024 12:15 AM	Application	188 KB

EDPCleanup.exe	6/12/2024 12:15 AM	Application	164 KB
edpcsp.dll	6/12/2024 12:15 AM	DLL File	180 KB
MDMAppInstaller.exe	6/12/2024 12:15 AM	Application	188 KB
NETSTAT.EXE	6/12/2024 12:15 AM	Application	64 KB
CBDHSvc.dll	6/12/2024 12:15 AM	DLL File	1,032 KB
computecore.dll	6/12/2024 12:15 AM	DLL File	946 KB
computestorage.dll	6/12/2024 12:15 AM	DLL File	442 KB
ConsentExperienceCommon.dll	6/12/2024 12:15 AM	DLL File	188 KB
discan.dll	6/12/2024 12:15 AM	DLL File	340 KB
vmdevicehost.dll	6/12/2024 12:15 AM	DLL File	264 KB
Windows.Internal.PlatformExtension.M...	6/12/2024 12:15 AM	DLL File	96 KB
WinHvEmulation.dll	6/12/2024 12:15 AM	DLL File	156 KB
WinHvPlatform.dll	6/12/2024 12:15 AM	DLL File	280 KB
clusapi.dll	6/12/2024 12:15 AM	DLL File	1,212 KB
CodeIntegrityAggregator.dll	6/12/2024 12:15 AM	DLL File	184 KB
diagperf.dll	6/12/2024 12:15 AM	DLL File	1,196 KB
DrtmAuthTxt.wim	6/12/2024 12:15 AM	wim Archive	20 KB
fsutil.exe	6/12/2024 12:15 AM	Application	266 KB
hvax64.exe	6/12/2024 12:15 AM	Application	1,742 KB
hvix64.exe	6/12/2024 12:15 AM	Application	1,922 KB
PerceptionSimulationManager.dll	6/12/2024 12:15 AM	DLL File	776 KB
resutils.dll	6/12/2024 12:15 AM	DLL File	568 KB
sdengin2.dll	6/12/2024 12:15 AM	DLL File	1,248 KB
securekernel.exe	6/12/2024 12:15 AM	Application	1,102 KB
SFAPM.dll	6/12/2024 12:15 AM	DLL File	274 KB
tcblaunch.exe	6/12/2024 12:15 AM	Application	858 KB
tcbloader.dll	6/12/2024 12:15 AM	DLL File	258 KB
ThreatExperienceManager.dll	6/12/2024 12:15 AM	DLL File	186 KB
ThreatIntelligence.dll	6/12/2024 12:15 AM	DLL File	482 KB

spatialinteraction.dll	6/12/2024 12:16 AM	DLL File	460 KB
Spectrum.exe	6/12/2024 12:16 AM	Application	752 KB
vbssysprep.dll	6/12/2024 12:16 AM	DLL File	128 KB
vmbuspipe.dll	6/12/2024 12:16 AM	DLL File	79 KB
Windows.Mirage.dll	6/12/2024 12:16 AM	DLL File	4,525 KB
Windows.Mirage.Internal.dll	6/12/2024 12:16 AM	DLL File	828 KB
AcGenral.dll	6/12/2024 12:16 AM	DLL File	458 KB
AcLayers.dll	6/12/2024 12:16 AM	DLL File	416 KB
DiagSvc.dll	6/12/2024 12:16 AM	DLL File	248 KB
fhcat.dll	6/12/2024 12:16 AM	DLL File	276 KB
fhcpl.dll	6/12/2024 12:16 AM	DLL File	388 KB
mstsc.exe	6/12/2024 12:16 AM	Application	1,368 KB
RDSAppXHelper.dll	6/12/2024 12:16 AM	DLL File	140 KB
rdsdwmdr.dll	6/12/2024 12:16 AM	DLL File	244 KB
SessEnv.dll	6/12/2024 12:16 AM	DLL File	584 KB
SIHClient.exe	6/12/2024 12:16 AM	Application	421 KB
termsrv.dll	6/12/2024 12:16 AM	DLL File	1,284 KB
tlscsp.dll	6/12/2024 12:16 AM	DLL File	68 KB
tsgqec.dll	6/12/2024 12:16 AM	DLL File	88 KB
wkspbroker.exe	6/12/2024 12:16 AM	Application	321 KB
workfolderssvc.dll	6/12/2024 12:16 AM	DLL File	2,038 KB
mstscax.dll	6/12/2024 12:16 AM	DLL File	9,012 KB
pcwutl.dll	6/12/2024 12:16 AM	DLL File	160 KB
SettingsHandlers_Troubleshoot.dll	6/12/2024 12:16 AM	DLL File	305 KB
desk.cpl	6/12/2024 12:16 AM	Control panel item	232 KB
msdt.exe	6/12/2024 12:16 AM	Application	568 KB
rdpclip.exe	6/12/2024 12:16 AM	Application	568 KB
tapisrv.dll	6/12/2024 12:16 AM	DLL File	332 KB

667. At the beginning of April through June, 2024, the Threat Actor Defendants' interference with Farrow and Farrow Law's staff through the substantial increases of vector exploitations activities caused workflow stoppages and communication interferences.

Events and Activities Prior to Hearings involving Heath Ritenour, John Ritenour and IOA

668. The malicious conduct and activities preceded hearings involving Heath Ritenour, John Ritenour, IOA, JTR and Taylor from March through June 2024.

669. These interferences also notably increased surrounding calendared events such as client conferences.

670. With regard to the former, on June 17, 2024, just over two hours before a 10 am hearing in the 2019 Spagnuolo case upon Heath, John and IOA, Inc.'s Motion to Dismiss, Farrow Law received a bogus email (which was "cced" to Farrow and several other lawyers) which appeared to come from the "Seminole Civil GM Dept", and more specifically, the magistrate's judicial assistant asking for a copy of plaintiff's third amended complaint and/or to provide the 'link' for the upcoming hearing.

671. When this June 17 email was opened by Farrow, it prompted an 18th Judicial Network warning notice.

672. At 8:05 am, minutes after Farrow Law received the bogus request from the purported magistrate's judicial assistant, Spagnuolo received a second email from the FDFS indicating an attempted unauthorized breach into his licensed insurance agent portal account. This was the second instance of this attempted breach into that portal within four days of the June 17, 2024 Hearing.

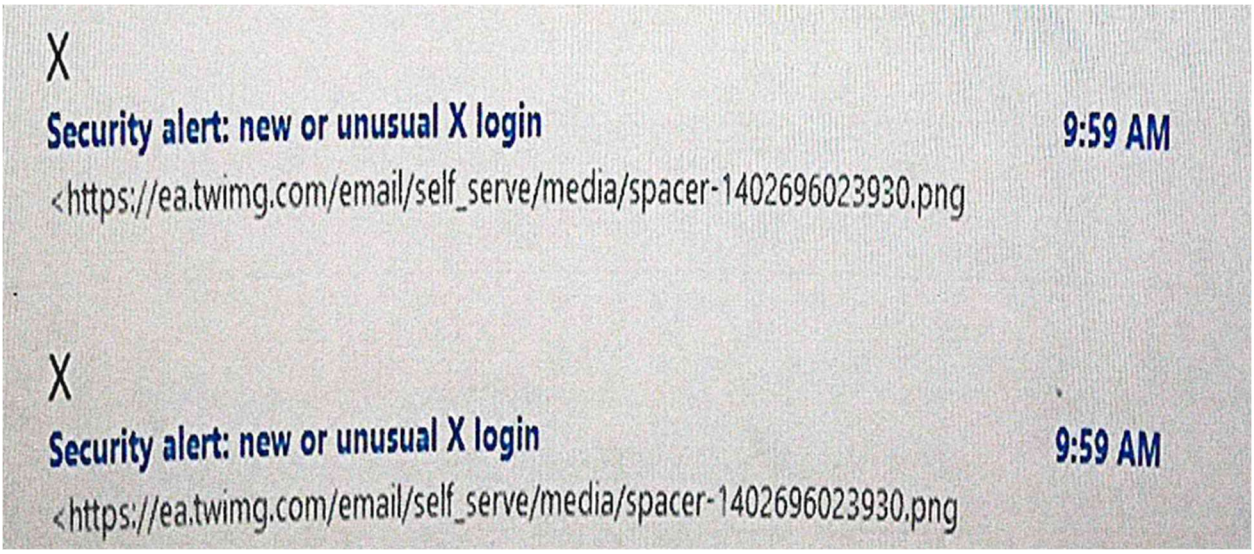
673. At 8:20am the undersigned's paralegal forwarded the third amended complaint as requested.

674. Approximately 20 minutes later, Farrow received another call with one of the two photos of Infant Doe which he received of him lying in a hospital bed.

675. Farrow called Defendant Kolaya on his cell phone and reported he had received another call and photo of Infant Doe lying in a hospital bed, that the magistrate apparently never received the third amended complaint which Defendant Kolaya had represented was within the materials uploaded in his prehearing email to the court, that he had received a warning notice at 8:20 am which, at that time, Farrow believed indicted his Paralegal had clicked on a link which caused a network infiltration of the FLF Network requiring his IT Vendor's emergency attention, and, also, that his client, Spagnuolo had now received two attempts to break into his insurance agent portal, the last of which was at 8:05 am.

676. Farrow asserted that the receipt of the photograph alone warranted rescheduling the hearing, which Defendant Kolaya summarily refused.

677. From 8:30 am through 9:59 am, Farrow received over 10 spear fishing emails, with the last at precisely 9:59am, one minute before the scheduled commencement of the 10am hearing indicating that his firm's twitter (n/k/a "X") account had been hacked.



678. Based upon all of the above, Farrow made an *ore tenus* motion over telephone connection which was granted, in part.

679. On or about June 20, 2024, the Threat Actor Defendants directed a Sitting Duck attack at flcourts18.org, which, upon information and belief, was for malicious purposes of creating foothold fortifications into that network in furtherance of achieving their Ultimate Goals.

680. On June 21, 2024, Farrow filed the first emergency motion he had ever filed in the nearly 20 years of practice before the Southern District of Florida in the 2024 Federal Case, with another on June 24 and a third on July 8, 2024, the last of which had to be filed in person and was drafted without the benefit of a computer connection to his firm's database, or even his business computer.

681. In each successive motion, Farrow outlined what the firm was experiencing and essentially requested the Defendants simply stop the cyber-hacking.[21]

682. Less than twenty-four hours later, on June 22, 2024, Farrow received an email to his personal email from his business email jay@farrowlawfirm.com entitled: A CEO's Golden Rules in Managing a Cybersecurity Crisis.

Jay Farrow

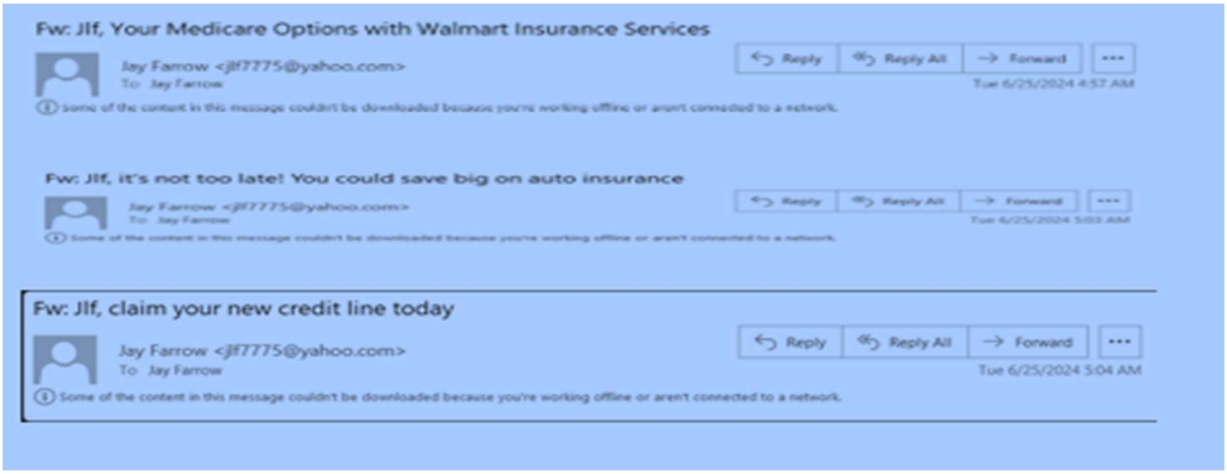
From: Jay Farrow
Sent: Saturday, June 22, 2024 8:06 PM
To: Jay Farrow
Subject: A CEO's 5 Golden Rules in Managing a Cybersecurity Crisis

I thought you might be interested in this article on the importance of CEO's 5 golden rules in managing a cybersecurity crisis. Check it out! https://www.paloaltonetworks.com/cybersecurity-perspectives/a-ceos-5-golden-rules-in-managing-a-cybersecurity-crisis

683. Farrow did not send the email from his business email to his personal email.

684. On June 25, 2024, the day Farrow filed the June 25 Emergency Motion in the Federal Case seeking a restraining order against most of the Threat Actor Defendants, Farrow received multiple emails from his personal @yahoo.com email to his office email jay@farrowlawfirm.com which were sent directly or indirectly by the Threat Actor Defendants.

[21] *See generally* June 21, 2024, June 25, 2024, and Reply to Joint Response which are appended hereto as Composite Exhibit "A" and incorporated herein for all purposes by reference.



685. Upon information and belief, by June 22, 2024 and certainly by June 25, 2024, the Threat Actor Defendants had login credentials for both his business and personal email which were obtained through unauthorized access to the protected computers within Farrow Law's Network.

686. Upon receipt of the June 25, 2024 email, Farrow communicated with his staff that the FLF Network was compromised and to do whatever necessary to reach their IT Vendor whom Farrow had repeatedly attempted to contact with no success.

687. On June 25, 2024, after the filing of the Second Emergency Motion, Farrow's investigation revealed that FLF's paralegal's credit cards she had stored on an FLF computer were compromised and over $1,000 was charged illegally, some of which to pay for computer software which is similar to Microsoft Outlook.

688. In addition to those fraudulent charges, the investigation reported prepared by Farrow as to this incident, provides that immediately subsequent to reporting the credit card fraud, the paralegal received a call purportedly from the Florida Department of Children and Families.

689. However, the call was an AI voice clone spoof and was made to FLF's paralegal directly or indirectly by the Threat Actor Defendants for malicious purposes as part of their continuing digital and non-digital activities in pursuit of their ultimate goals.

690. According to the incident report prepared by Farrow during his phone call of June 23, 2024 with FLF's paralegal, she reported the DCF agent represented that he was investigating her because she had just reported over $1,000 in fraudulent credit card activities which DCF does if a parent with more than 3 children reports fraudulent charges on a credit card or debit card.

691. The incident report provides that based upon the credit card fraud, the DCF call and the previous month of having to remediate the persistent errors caused by network computer errors, she could see a pattern which terrified her.

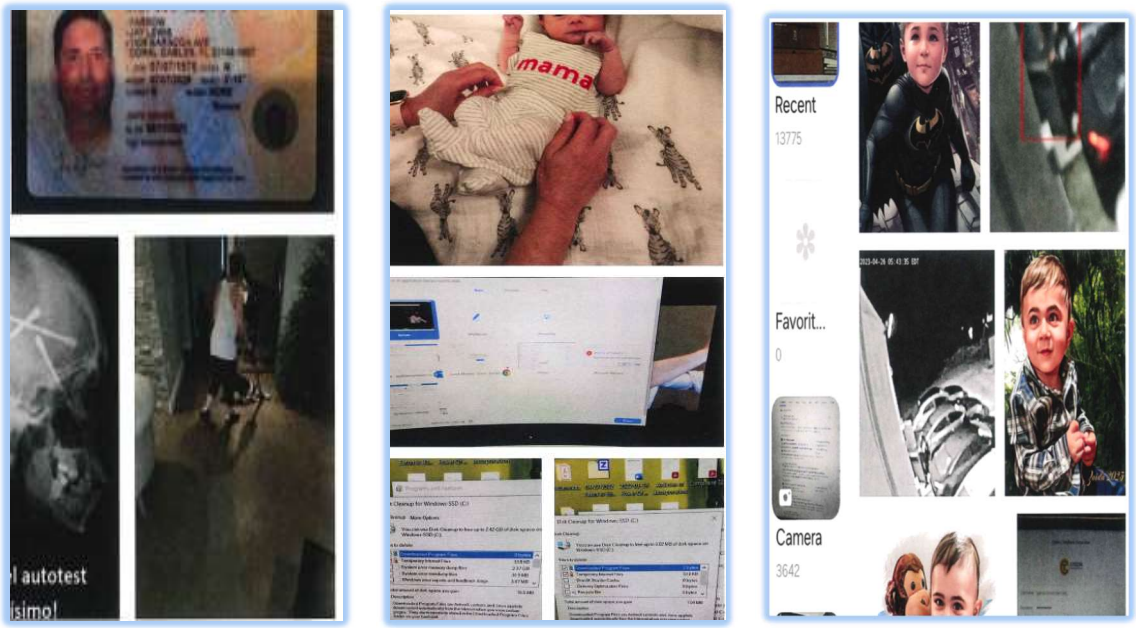
692. On June 25, 2024, FTI, and the Carrier Defendants, filed a Joint Response which did not deny the allegations that FTI had perpetrated a cyber-attack against Farrow and Farrow Law and generally argued that Farrow and Farrow Law lacked standing or otherwise their emergency motions did not meet the evidentiary standard for injunctive relief.

693. **From June 26, 2024 through August 2024** – Defendants APT hacked into Farrow's personal cell phone and caused interference with communications, but also rearranged and/or created numerous photo albums with pictures from Farrow's phone that arranged to send the message that Farrow's real-time documentation of the APT would correspondent to harm to Infant Doe, Dr. Doe and/or Farrow himself.

694. More specifically, the Threat Actor Defendants arranged and rearranged photos and created new 'albums' daily, with all of them including photos of the screenshots or pictures Farrow

was taking to document the cyber-attacks on his Lenovo computer, next to a photo of Infant Doe with a disturbing photo depicting substantial bodily harm.

695. For example, photos of Infant Doe, next to evidence screenshots and an x-ray of a person with nails in their head, and photos of Infant Doe, a photo of Farrow's computer and photos from a security camera highlighting a burglary, were arranged in specific order by the Theat Actor Defendants.



696. On June 26, 2024, as Farrow continued to document the cyber-attack, and having reviewed the Joint Response to the June 21, 2024 Emergency Motion (filed by Threat Actor Defendants FTI and the Carrier Defendants), he and Farrow Law began preparing a Reply which included additional evidence establishing the connections between FTI and the cyber-attacks Farrow and Farrow Law had been experiencing.

697. Beginning on or about mid-June, and especially subsequent to the filing of the first emergency motion on July 21, 2024, the Threat Actor Defendants ramped up their activities further

than experienced between June 3 and June 14, 2024, using a variety of tradecraft tools and interference for purposes of achieving their Ultimate Goals.

698. During this time period, the Threat Actor Defendants utilized the fruits of years of infiltrating the Farrow Law Network its computers and Farrow and Dr. Doe's personal cell phones.

699. More Specifically, from June 15 through July 5, 2024, the Threat Actor Defendants demonstrated through sending emails to Farrow and Farrow Law's staff they had been successful at interfering with substantially all email communications with Farrow Law's clients, vendors, staff, and court staff using the permissions obtained through Sitting Duck and Man-in-the-Midde Attacks.

700. By at least mid-June 2024, the Threat Actor Defendants had successfully interceded in all, or substantially all, of Farrow Law's email communications with clients, opposing counsel and with judicial staff.

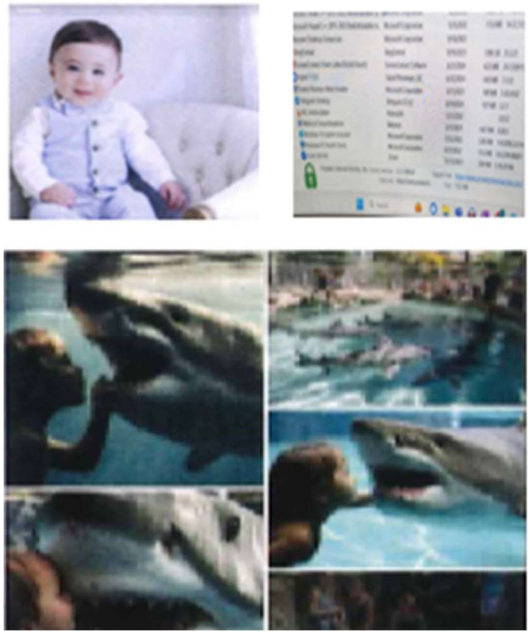
701. This interference allowed them to respond as if they were any party to the respective email communications through Man-In-The Middle Cyber Attacks, and their network infiltrations and/or infiltrations into protected computers allowed them to create documents and, in some cases, file them using the credentials of attorneys without their knowledge or consent.

702. Further, from June 15 through July 5, 2024, the Threat Actor Defendants targeted Plaintiffs with the most sophisticated spear phishing email schemes, that is to say, the emails no longer necessarily were for purposes of delivering a malware payload so much as they were for social engineering a complete breakdown of Farrow Law's business operation and functioning.

703. At the same time, from approximately June 25 or 26, 2024, the Threat Actor Defendants used emails in tandem with the intentional misconfiguration of Farrow's cell phone's

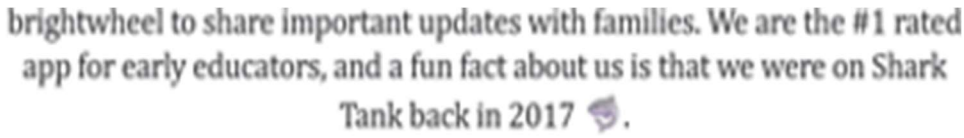
photo gallery to directly and/or indirectly threaten harm to Infant Doe, as well as Farrow and Dr. Doe.

704. On or about June 26, 2024, the Threat Actor Defendants had, once again, hacked Farrow's cell phone and rearranged Farrow's photos to create another 'album' which contained, as before, screenshots taken by Farrow documenting the ongoing cyber-attack, next to photos of Infant Doe and, in this instance, photos of an Infant swimming in a shark tank with great white sharks.



705. On June 26, 2024, on the very same day the Threat Actor Defendants sent Farrow the rearranged photo album which showed, in relevant part, Infant Doe, Evidence Documentation and an Infant swimming in a Shark Take, the Threat Actor Defendnts sent Farrow an email purportedly from the preschool Dr. Doe and Farrow were considering for Infant Doe.

706. More specifically, this June 26, 2024 email stated that Farrow's business email had been set up on the preschool "brightwheel app", and also that a 'fun fact' about their 'brightwheel app' is that it was on 'Shark Tank'.


brightwheel to share important updates with families. We are the #1 rated app for early educators, and a fun fact about us is that we were on Shark Tank back in 2017 .

707. Farrow had never provided the pre-school with his business email address, or his personal email address, but he had visited the preschool and learned about the preschool's app where parents can login to see photos of their child participating in activities and projects. T

708. At the very least, the spear phishing email using Infant Doe's preschool was intended to cause interference and emotional pain, as the receipt of the email to his business email address evidenced that the Threat Actor Defendants had achieved some access to Dr. Doe's email addresses which were provided to this preschool.

709. The Threat Actor Defendants repeatedly rearranged photos and created albums using unauthorized access to Farrow's cell phone and from June 26, 2028 through July 13, 2024, this activity was in tandem with an exponential increase in spear-phishing emails to Farrow and Farrow Law.

710. **On June 27, 2024**, Farrow filed a Reply to the Joint Response which provided evidence obtained connecting the identity of the individual who left the June 3, 2024 text message photo of Farrow holding his sone the day he was born twenty months prior, to one of FTI's purported directors working at its Denver, Colorado office.

711. The filing of this Reply was followed by substantial, relentless and egregious activities and conduct, occurring in tandem, which was intended to cause, and did cause, Farrow Law to effectively close, Farrow's communications with clients, staff and his attorneys to be severed, and the achievement of several of the Ultimate Goals of the Threat Actor Defendants.

712. From June 27, 2024 through present, the Threat Actor Defendants' aggressive and ongoing conduct caused unauthorized access into Farrow and Farrow Law's replacement protected computers, and electronic communication devices.

713. On or about June 27, 2024, Farrow and Dr. Doe discovered that the Threat Actor Defendants used Farrow and Dr. Doe's PII, and unauthorized login credentials to Farrow's jxxxxx5@yahoo.com and Dr. Doe's jxxxxxx@gmail.com personal email accounts, as well as at least the persistent unauthorized access into Farrow's Galaxy 22 cell phone, to create an Xfinity and At&t Hotspot Accounts in the two vehicles which Farrow and Dr. Doe used for personal and business transportation.

714. In so doing, the Threat Actors Defendants established a means to connect and/or reconnect with Farrow, Farrow Law and Dr. Doe's protected computers, and cell phones for malicious purposes.

715. More specifically, these malicious purposes included, *inter alia,* advancing their privileges and permissions within the Farrow Law Network, its computers, Dr. Doe's protected laptop computer and those networks and protected computers Defendants deemed strategically advantageous for purposes of achieving their Ultimate Goals.

716. By Example, the Threat Actor Defendants used the unauthorized and unlawful access vector exploits, to established Wi-Fi hotspot accounts and service to install Wi-Fi service

to Farrow and Dr. Doe's vehicles for purposes of connecting and/or reconnecting with the protected computers and devices they had previously infiltrated and maintained access through Farrow Law's office Wi-Fi and/or Farrow and Dr. Doe's home internet router when the previously one had been replaced or when the password to the router was changed.

717. Until late June or early July 2024, neither Farrow nor Dr. Doe detected the existence of these hotspot Wi-Fi accounts.

718. On or about July 1, 2024, an Order was entered denying both the June 21 and 25, 2024 emergency motions without scheduling a hearing.

719. This Order cited a case from the 8th Circuit Court of Appeals that overturned an injunction against a cyber-security company holding that the district court should not have placed substantial weight upon the timing of the cyber-attacks against the lawyer and law firm which occurred after court filings or before noticed hearing because anyone could have been behind the cyber-attacks and since court proceedings and filings were available to the public, any threat actor could use them to direct additional cyber-activities at that time.

720. The July 1, 2024 Order determined also that Farrow nor Dr. Doe were parties, and notwithstanding, the facts presented in the June 21 and June 25, 2024 Emergency Motions were not at issue in the Amended Complaint, nor was there 'a claim for relief' in that operative complaint to enjoin cyber-interference and, thus, there could be no finding a substantial likelihood of success on the merits of a claim not presented.

721. Finally, in the Order, the Court stated that while it understood the concerns raised in both emergency motions, it could not exercise its inherent powers or any legal mechanism to

provide Farrow, Dr. Doe or Farrow's client, Spagnuolo, the 'drastic' and exceptional injunctive relief they requested.

722. By Monday, July 1, 2024, Farrow had lost meaningful administrator status over the Farrow Law Network, and notwithstanding his efforts to replace computers and/or create a new cloud-based network for Farrow Law, each new computer was infiltrated within 24 hours of purchase.

723. As well, by July 1, 2024, Farrow had to purchase temporary phones due to the substantial interference by the Threat Actor Defendants with his Galaxy 22 phone.

724. Further by July 1, 2024, Farrow Law's staff were disconnected from meaningful access to Farrow Law's network as practically all email communications with clients, opposing counsel and the courts were compromised by the Threat Actor Defendants MitM interferences.

725. As well, to the extent that the firm's paralegal, and her husband, the firm's legal assistant, had had substantial fraudulent charges on their credit card followed by AI Voice Calls falsely pretending to be Florida Department of Children and Families agents claiming an official investigation against them was initiated for reporting the credit card fraud, with inquiries also into employment status, they believed resigning and finding new employment was in their best interests.

726. On July 2, 2024, Farrow began to prepare an emergency motion seeking ex parte emergency relief which requested at a minimum a live hearing such that he could present and/or proffer evidence to connect the dots beyond mere 'temporal proximity' in a safe sterile environment.

727. On July 3, 2024, Farrow requested a staff member to deliver documents and materials through an alternative means to ensure the electronic filing and uploading the emergency request for a live hearing, however, due to the upcoming holiday weekend, his contact at the Broward County Courthouse had left for the day.

728. After the July 1, 2024 Order denying both the June 21 and 25, 2024 Emergency Motions, the Threat Actor Defendants activities and conduct over the next 48 hours were substantial more brazen and terrifying.

729. By example, the spear phishing emails Farrow and Farrow Law received on July 2 and 3, 2024, directly or indirectly by the Threat Actor Defendants caused chaos, substantial emotional distress and were designed to work in tandem with the persistently taxing stress they had been exerting over the last four previous weeks for purposes of achieving their Ultimate Goals.

730. Specifically, the inhanced spear phishing emails received on July 2 and 3, 2024 alone, included, *inter alia:* (1) a purported Florida Bar letter claiming Farrow had not responded to a Bar Complaint; (2) a client claiming to have spent the day filing a police report against Farrow with the Pinellas County Sheriff's Office; (3) Farrow Law's Landlord's letter that Farrow Law had abandoned property at its office location, yet it had never moved out; (4) security warnings as to Farrow's business email; (5) security warnings as to Farrow's private email; and (6) Defendant Kolaya requesting a hearing for Defendant Heath Ritenour, John Ritenour and IOA, Inc.'s Motion to Dismiss which had been continued on June 17, 2024 due to the inhanced activities prior to the hearing on that date, which Defendant Kolaya knew had only increased since June 17, 2024.

731. On or about July 3, 2024, another example of inhanced activities was the theft of the evidence folder from the 2024 Federal Case. had been stolen and Farrow could not access any

documents therein, however he had, in the weeks leading up to July 3, 2024, taken photographs of his computer with the screenshots and other photo evidence were available.

732. On or about July 2 through 5, 2024, the Threat Actor Defendants continued to manipulate Farrow's cell phone to rearrange photo 'albums' to directly and/or indirectly threaten and/or intimidate Farrow and Dr. Doe.

733. For example, on or about July 3, 2024, Farrow's cellphone's photo gallery was rearranged showing photos of the stolen evidence Farrow had taken of his computer from his cell phone before losing access to it at approximately 5:22am on July 3, 2024, next to a picture of a human head with over 20 stiches in his head.

734. On July 4 or 5, 2024, the screenshots of Farrow documenting the stolen Farrow Law Admin Folder which contained, *inter alia,* the stolen 2024 Federal Case Evidence File, and Farrow's personal files, were also rearranged such that they were next to a photo of Infant Doe taken in August 2023 where he was lying in a post-operation hospital bed, which were immediately followed by four Barbie Doll Faces with progressive rapid facial mutilations and an unconscious child at a playground.

735. On or about July 5, 2024, Farrow could no longer access the Farrow Law Network, and at the very least, the Folders which had contained the evidence from the 2024 Federal Case,

2020 Seminole SLAPP Case, the 2020 Palm Beach SLAPP Case and the [Insurance Office of America] General file.

736. Nevertheless, Farrow prepared an ex parte emergency motion which he filed in person in the Miami Federal District Court Clerk's Office on July 8, 2024.

737. This ex parte motion requested a live hearing such that Farrow could have an opportunity to proffer or submit evidence that the Threat Actor Defendants' conduct and activities went far beyond temporal proximity.

738. However, on or about July 10, 2024, the federal court denied that motion in an order which stated, in part, that the issue of temporal proximity was not the exclusive reason for the denial of the June 21 and 24, 2024 Emergency Motions and admonished Farrow against filing further emergency motions which presented the same facts and legal arguments.

739. By July 10, 2024, Farrow's communications with his staff had been severed and/or rendered unsafe and unsecure due to the Threat Actor Defendants conduct and activities.

740. By July 10, 2024, Farrow Law was effectively closed, its staff had resigned, and Farrow's communications with Farrow Law's clients had ceased to be safe and secure or otherwise been severed through manipulations to Farrow's Galaxy 22 Android Phone.

741. By July 10, 2024, Farrow's communications with other contacts he had in his phone had been substantially interfered with through the manipulation of 'do not disturb' preferences in his and, upon information and belief, devices belonging to family, friends, his legal counsel and other colleagues.

742. From April through July 2024, the Threat Actor Defendants executed remote commands to Farrow and Farrow Law's Network and protected computers to exfiltrate select files,

information and data, while also deleting user accounts they had created to navigate throughout the Farrow Law Network from at least January 2021 through July 2024.

743. From April through July 2024, the Threat Actor Defendants aggressively worked to sabotage, and were successful in completely sabotaging Farrow Law's Network, individual protected computers by, *inter alia,* deleting files from one computer and placing them in renamed encrypted files and/or making modifications to data files, including rearranging them and changing the location which the document, pdf or photograph was properly organized for purposes of achieving their Ultimate Goals.

July 12, 2024 – the Threat Actor Defendants Completed All APT Sequences and Accomplished Substantially All Ultimate Goal

744. **By Friday, July 12, 2024, in summary:** (1) Farrow Law Firm had effectively closed; (2) the Threat Actor Defendants had stolen files and evidence from the Farrow Law Network related to the 2024 Federal Case, the 2020 Seminole SLAPP Case, the 2020 Palm Beach SLAPP Case, and the 2019 Spagnuolo Case rendering further prosecution improbable and practically impossible; (3) the Threat Actor Defendants had engaged and completed substantial efforts to cover their tracks by deleting files, user accounts and other means of detecting their unauthorized access into Farrow Law's Network; (4) Farrow's last attempt for a judicial hearing was denied in the 2024 Federal Case; (5) Farrow's communications with all but a few contacts had been severed; (6) unauthorized access into collateral networks and computers of individuals and entities associated with Farrow and Farrow Law had been manipulated to filter and reject communications from Farrow, such as opposing counsels in the 2024 Federal Case; (7) Farrow and Farrow Law's banking institution of over 25 years had frozen and permanently closed they

accounts; and (8) simultaneously, the Threat Actor Defendants directed AI voice clone calls to Farrow and Dr. Doe to create situational crisis events directed at inflicting the maximum amount of pain, stress and interference with their relationships and, most importantly, causing Infant Doe trauma.

VIII. THE APT'S DIGITAL BREADCRUMBS "ID" THE TADS' FINGERPRINTS

745. Plaintiffs allege that the fingerprints or digital DNA exists, *inter alia,* and was registered on external open sources and within Farrow's and Farrow Law's protected computers.

746. Plaintiffs further allege that the digital evidence which remains, and continues to be registered, identifies the Threat Actor Defendants as the only perpetrators accountable for the damages suffered by Plaintiffs.

747. While not observable from January through July 2024, Farrow and Farrow Law's protected computers, Farrow's cell phone and other indicators registered the seismic shift of illicit and malicious activity commencing in or about March 2024, and substantially increasing through the end of April and exponentially increasing from May through July 10, 2024, the date of the effective closure of Farrow Law.

748. Thereafter, when Plaintiff demonstrated efforts to seek judicial and law enforcement support, the Threat Actor Defendants adapted their APT using collateral networks and protected computers to effectuate the pursuit of their Ultimate Goals.

749. However, having to accelerate their schemes and plans towards the achievement of their Ultimate Goals in or about March and certainly April 2024, and then, after Farrow Law's effective closure, having to rely upon collateral networks, websites, and accounts as opposed to

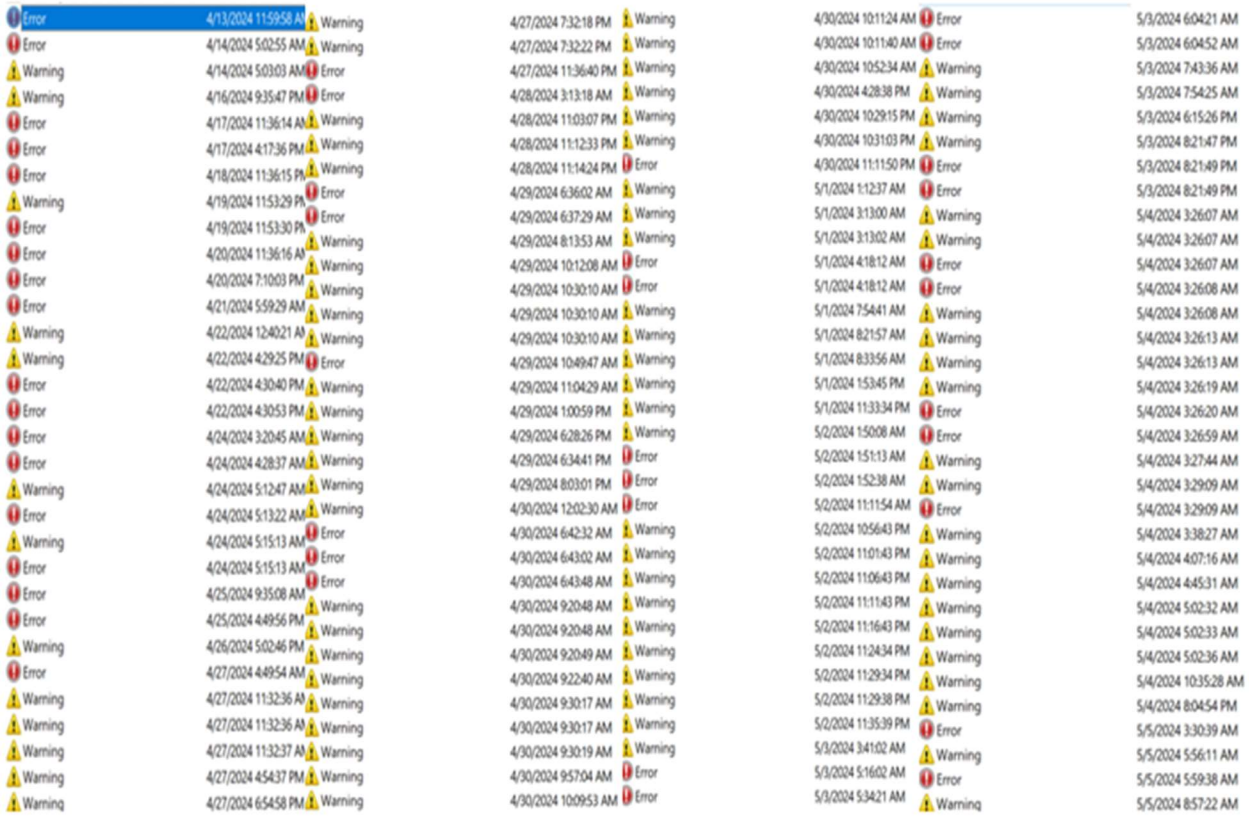
working from within the Farrow Network to achieve their goals, caused a substantial digital imprint as further alleged herein below.

750. In the following examples, the Threat Actor Defendants' malicious conduct directed at achieving their Ultimate Goals increased from 200% to nearly 2,600% in registered activity.

Administrative Logs from Farrow's Lenovo Hard Drive

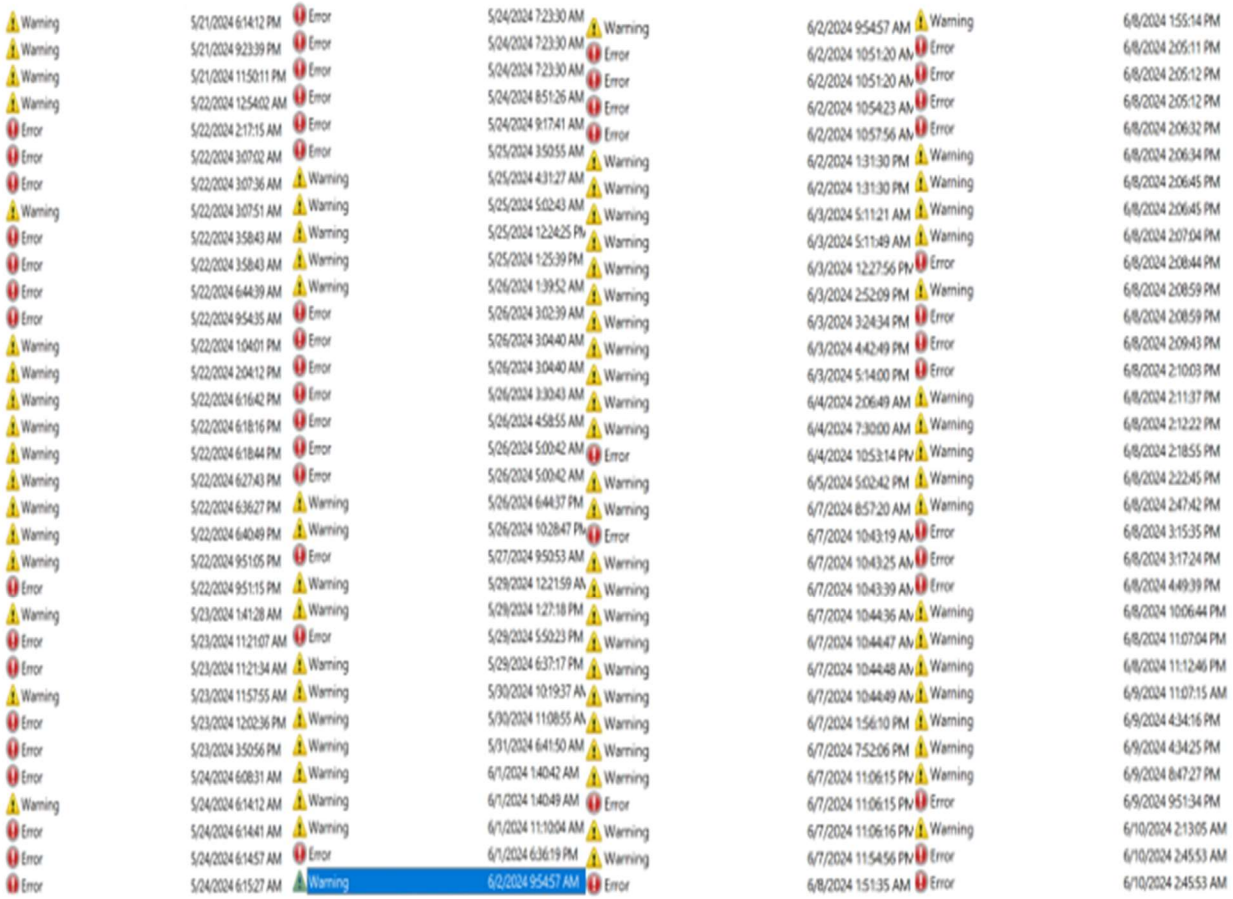
751. The following demonstrative from administrative logs from Farrow's primary business laptop shows the administrative activities resulting in warnings or errors for the approximately three-month period from January 7, 2024 through March 31, 2024.

752. For two-month period from April 13, 2024 through June 10, 2024, the administrative logs reflecting the Threat Actor Defendants activities and otherwise registering warnings and error shows a 200% increase, notwithstanding the same occurred in 1/3 of the time:



Warning	5/5/2024 9:21:51 AM	Error	5/7/2024 5:36:39 AM	Warning	5/7/2024 8:00:28 PM	Warning	5/13/2024 4:51:23 AM
Warning	5/5/2024 9:21:51 AM	Error	5/7/2024 5:36:40 AM	Error	5/7/2024 8:00:50 PM	Warning	5/13/2024 4:51:24 AM
Warning	5/5/2024 9:23:09 AM	Error	5/7/2024 5:36:45 AM	Warning	5/8/2024 7:52:12 AM	Warning	5/13/2024 4:51:24 AM
Warning	5/5/2024 9:30:43 AM	Error	5/7/2024 5:40:43 AM	Error	5/8/2024 7:53:17 AM	Warning	5/13/2024 4:51:24 AM
Error	5/5/2024 10:13:18 AM	Error	5/7/2024 5:41:32 AM	Error	5/8/2024 7:53:47 AM	Warning	5/13/2024 4:51:24 AM
Error	5/5/2024 10:27:32 AM	Warning	5/7/2024 5:43:05 AM	Error	5/8/2024 7:54:18 AM	Warning	5/13/2024 4:51:24 AM
Warning	5/5/2024 10:36:58 AM	Error	5/7/2024 5:43:49 AM	Error	5/8/2024 7:54:48 AM	Warning	5/13/2024 4:51:24 AM
Warning	5/7/2024 5:35:36 AM	Error	5/7/2024 5:43:51 AM	Warning	5/8/2024 7:55:02 AM	Warning	5/13/2024 4:51:24 AM
Error	5/7/2024 5:36:03 AM	Warning	5/7/2024 6:05:52 AM	Error	5/8/2024 7:57:00 AM	Warning	5/13/2024 4:51:24 AM
Error	5/7/2024 5:36:24 AM	Error	5/7/2024 6:05:52 AM	Error	5/8/2024 7:59:33 AM	Warning	5/13/2024 4:51:24 AM
Error	5/7/2024 5:36:25 AM	Warning	5/7/2024 6:05:55 AM	Error	5/8/2024 8:00:03 AM	Warning	5/13/2024 4:51:24 AM
Warning	5/7/2024 5:36:25 AM	Warning	5/7/2024 6:05:58 AM	Error	5/8/2024 8:00:56 AM	Warning	5/13/2024 4:51:31 AM
Error	5/7/2024 5:36:26 AM	Warning	5/7/2024 6:05:58 AM	Warning	5/8/2024 10:22:17 AM	Warning	5/13/2024 4:51:31 AM
Error	5/7/2024 5:36:27 AM	Warning	5/7/2024 6:06:04 AM	Warning	5/9/2024 12:29:25 PM	Warning	5/13/2024 4:51:32 AM
Error	5/7/2024 5:36:28 AM	Error	5/7/2024 6:06:43 AM	Warning	5/9/2024 12:30:00 PM	Warning	5/13/2024 4:51:34 AM
Error	5/7/2024 5:36:29 AM	Warning	5/7/2024 6:07:14 AM	Error	5/12/2024 3:35:19 PM	Warning	5/13/2024 4:51:59 AM
Error	5/7/2024 5:36:29 AM	Warning	5/7/2024 6:07:14 AM	Warning	5/13/2024 4:43:41 AM	Error	5/13/2024 4:51:59 AM
Error	5/7/2024 5:36:29 AM	Warning	5/7/2024 6:07:57 AM	Error	5/13/2024 4:43:51 AM	Error	5/13/2024 4:52:01 AM
Error	5/7/2024 5:36:30 AM	Warning	5/7/2024 6:09:08 AM	Error	5/13/2024 4:44:21 AM	Warning	5/13/2024 4:52:10 AM
Error	5/7/2024 5:36:30 AM	Error	5/7/2024 6:09:08 AM	Error	5/13/2024 4:44:33 AM	Warning	5/13/2024 4:52:18 AM
Error	5/7/2024 5:36:30 AM	Warning	5/7/2024 6:18:14 AM	Error	5/13/2024 4:45:03 AM	Warning	5/13/2024 4:52:18 AM
Error	5/7/2024 5:36:31 AM	Warning	5/7/2024 6:46:47 AM	Error	5/13/2024 4:45:03 AM	Warning	5/13/2024 4:52:20 AM
Error	5/7/2024 5:36:31 AM	Warning	5/7/2024 7:10:22 AM	Error	5/13/2024 4:45:33 AM	Warning	5/13/2024 4:52:49 AM
Error	5/7/2024 5:36:32 AM	Warning	5/7/2024 7:46:41 AM	Error	5/13/2024 4:46:06 AM	Warning	5/13/2024 4:53:31 AM
Error	5/7/2024 5:36:32 AM	Warning	5/7/2024 11:03:09 AM	Error	5/13/2024 4:46:36 AM	Warning	5/13/2024 4:53:31 AM
Error	5/7/2024 5:36:33 AM	Error	5/7/2024 11:03:42 AM	Error	5/13/2024 4:49:58 AM	Warning	5/13/2024 5:00:04 AM
Error	5/7/2024 5:36:33 AM	Error	5/7/2024 11:04:12 AM	Error	5/13/2024 4:50:59 AM	Warning	5/13/2024 5:48:36 AM
Error	5/7/2024 5:36:33 AM	Warning	5/7/2024 7:58:11 PM	Warning	5/13/2024 4:51:00 AM	Warning	5/13/2024 5:48:36 AM
Error	5/7/2024 5:36:34 AM	Warning	5/7/2024 7:58:25 PM	Warning	5/13/2024 4:51:16 AM	Warning	5/13/2024 5:48:37 AM
Error	5/7/2024 5:36:38 AM	Error	5/7/2024 7:58:56 PM	Warning	5/13/2024 4:51:16 AM	Error	5/13/2024 5:59:27 AM
Error	5/7/2024 5:36:38 AM	Warning	5/7/2024 7:59:07 PM	Warning	5/13/2024 4:51:18 AM	Warning	5/13/2024 6:38:15 AM
Error	5/7/2024 5:36:39 AM	Error	5/7/2024 7:59:40 PM	Warning	5/13/2024 4:51:18 AM	Warning	5/13/2024 6:39:10 AM
Error	5/7/2024 5:36:39 AM	Error	5/7/2024 8:00:20 PM	Warning	5/13/2024 4:51:21 AM	Warning	5/13/2024 12:39:39 PM

Error	5/15/2024 11:13:13 PM	Warning	5/16/2024 3:10:29 AM	Warning	5/17/2024 2:55:30 PM	Error	5/19/2024 5:59:18 AM
Warning	5/15/2024 11:25:26 PM	Warning	5/16/2024 3:11:20 AM	Warning	5/17/2024 2:55:30 PM	Error	5/19/2024 5:59:18 AM
Warning	5/15/2024 11:27:10 PM	Warning	5/16/2024 3:11:20 AM	Warning	5/17/2024 2:55:30 PM	Warning	5/19/2024 6:23:02 AM
Error	5/16/2024 1:00:20 AM	Warning	5/16/2024 3:11:32 AM	Warning	5/17/2024 2:55:30 PM	Error	5/19/2024 7:29:20 AM
Warning	5/16/2024 1:12:04 AM	Error	5/16/2024 4:35:59 AM	Warning	5/17/2024 2:55:30 PM	Error	5/19/2024 7:29:32 AM
Error	5/16/2024 1:12:15 AM	Error	5/16/2024 4:36:06 AM	Warning	5/17/2024 2:55:30 PM	Error	5/19/2024 7:31:07 AM
Warning	5/16/2024 1:12:20 AM	Warning	5/16/2024 10:31:58 PM	Warning	5/17/2024 2:55:36 PM	Error	5/19/2024 7:31:28 AM
Warning	5/16/2024 1:12:25 AM	Error	5/17/2024 3:02:44 AM	Warning	5/17/2024 2:55:36 PM	Error	5/19/2024 7:32:58 AM
Warning	5/16/2024 1:12:29 AM	Warning	5/17/2024 3:03:55 AM	Warning	5/17/2024 2:55:37 PM	Warning	5/19/2024 8:00:32 AM
Warning	5/16/2024 1:12:29 AM	Error	5/17/2024 4:34:45 AM	Warning	5/17/2024 2:55:40 PM	Warning	5/19/2024 11:17:52 PM
Warning	5/16/2024 1:12:31 AM	Error	5/17/2024 4:34:45 AM	Error	5/17/2024 2:56:03 PM	Warning	5/19/2024 11:45:42 PM
Warning	5/16/2024 1:12:33 AM	Error	5/17/2024 4:40:22 AM	Warning	5/17/2024 2:56:07 PM	Warning	5/20/2024 7:05:54 AM
Warning	5/16/2024 1:12:51 AM	Error	5/17/2024 4:41:04 AM	Error	5/17/2024 2:56:07 PM	Error	5/20/2024 11:07:09 AM
Warning	5/16/2024 1:12:52 AM	Error	5/17/2024 5:10:57 AM	Warning	5/17/2024 2:56:14 PM	Warning	5/20/2024 11:07:12 AM
Warning	5/16/2024 1:12:52 AM	Error	5/17/2024 5:56:29 AM	Warning	5/17/2024 2:57:02 PM	Warning	5/20/2024 11:07:12 AM
Warning	5/16/2024 1:12:52 AM	Error	5/17/2024 5:56:30 AM	Warning	5/17/2024 2:57:37 PM	Warning	5/20/2024 11:07:12 AM
Warning	5/16/2024 1:13:12 AM	Error	5/17/2024 5:56:36 AM	Warning	5/17/2024 2:57:37 PM	Warning	5/20/2024 11:07:16 AM
Warning	5/16/2024 1:13:17 AM	Error	5/17/2024 5:57:00 AM	Warning	5/17/2024 3:07:44 PM	Error	5/20/2024 11:07:46 AM
Warning	5/16/2024 1:13:17 AM	Error	5/17/2024 5:57:00 AM	Warning	5/17/2024 3:10:52 PM	Warning	5/20/2024 11:08:37 AM
Warning	5/16/2024 1:13:19 AM	Error	5/17/2024 5:57:01 AM	Warning	5/17/2024 3:10:52 PM	Warning	5/20/2024 11:10:30 AM
Warning	5/16/2024 1:13:24 AM	Error	5/17/2024 7:50:49 AM	Warning	5/17/2024 3:13:29 PM	Error	5/20/2024 11:10:30 AM
Warning	5/16/2024 1:13:46 AM	Error	5/17/2024 7:51:35 AM	Warning	5/17/2024 4:23:20 PM	Warning	5/20/2024 11:13:25 AM
Warning	5/16/2024 1:13:48 AM	Warning	5/17/2024 2:55:07 PM	Warning	5/17/2024 9:14:00 PM	Warning	5/20/2024 11:19:18 AM
Warning	5/16/2024 1:13:57 AM	Warning	5/17/2024 2:55:24 PM	Warning	5/18/2024 9:28:51 AM	Warning	5/20/2024 11:30:11 AM
Warning	5/16/2024 1:14:45 AM	Warning	5/17/2024 2:55:24 PM	Warning	5/18/2024 9:37:38 AM	Warning	5/20/2024 11:30:12 AM
Warning	5/16/2024 1:14:57 AM	Warning	5/17/2024 2:55:25 PM	Warning	5/18/2024 9:37:47 AM	Warning	5/20/2024 2:44:29 PM
Error	5/16/2024 1:15:03 AM	Warning	5/17/2024 2:55:26 PM	Warning	5/18/2024 9:38:13 AM	Error	5/20/2024 2:58:41 PM
Warning	5/16/2024 1:15:15 AM	Warning	5/17/2024 2:55:28 PM	Warning	5/18/2024 9:38:23 AM	Warning	5/20/2024 3:23:48 PM
Warning	5/16/2024 1:15:16 AM	Warning	5/17/2024 2:55:30 PM	Warning	5/18/2024 9:38:28 AM	Warning	5/21/2024 1:26:46 AM
Warning	5/16/2024 1:15:23 AM	Warning	5/17/2024 2:55:30 PM	Warning	5/18/2024 9:39:20 AM	Error	5/21/2024 3:18:33 AM
Warning	5/16/2024 1:15:41 AM	Warning	5/17/2024 2:55:30 PM	Warning	5/18/2024 9:40:04 AM	Error	5/21/2024 3:20:33 AM
Warning	5/16/2024 1:15:58 AM	Warning	5/17/2024 2:55:30 PM	Error	5/18/2024 6:27:48 PM	Error	5/21/2024 3:22:33 AM
Warning	5/16/2024 3:10:29 AM	Warning	5/17/2024 2:55:30 PM	Warning	5/18/2024 11:59:21 PM	Warning	5/21/2024 5:55:45 PM



Farrow's Cell Phone's Data Usage Increases 2,600%

753. On or about April 15, 2024, after Farrow had spoken to Mr. Meltz and proffered the results of Farrow's investigation after discovering new evidence on March 21, 2024, Farrow's personal cell phone registered an exponential spike in the use of cellular data in the month of April, and (as the below screen shots from Farrow's phone demonstrate) by the period marked June 4 through July 4, 2024, Farrow's cell phone's use of cellular data had increased 2,600 Percent from April 2024.

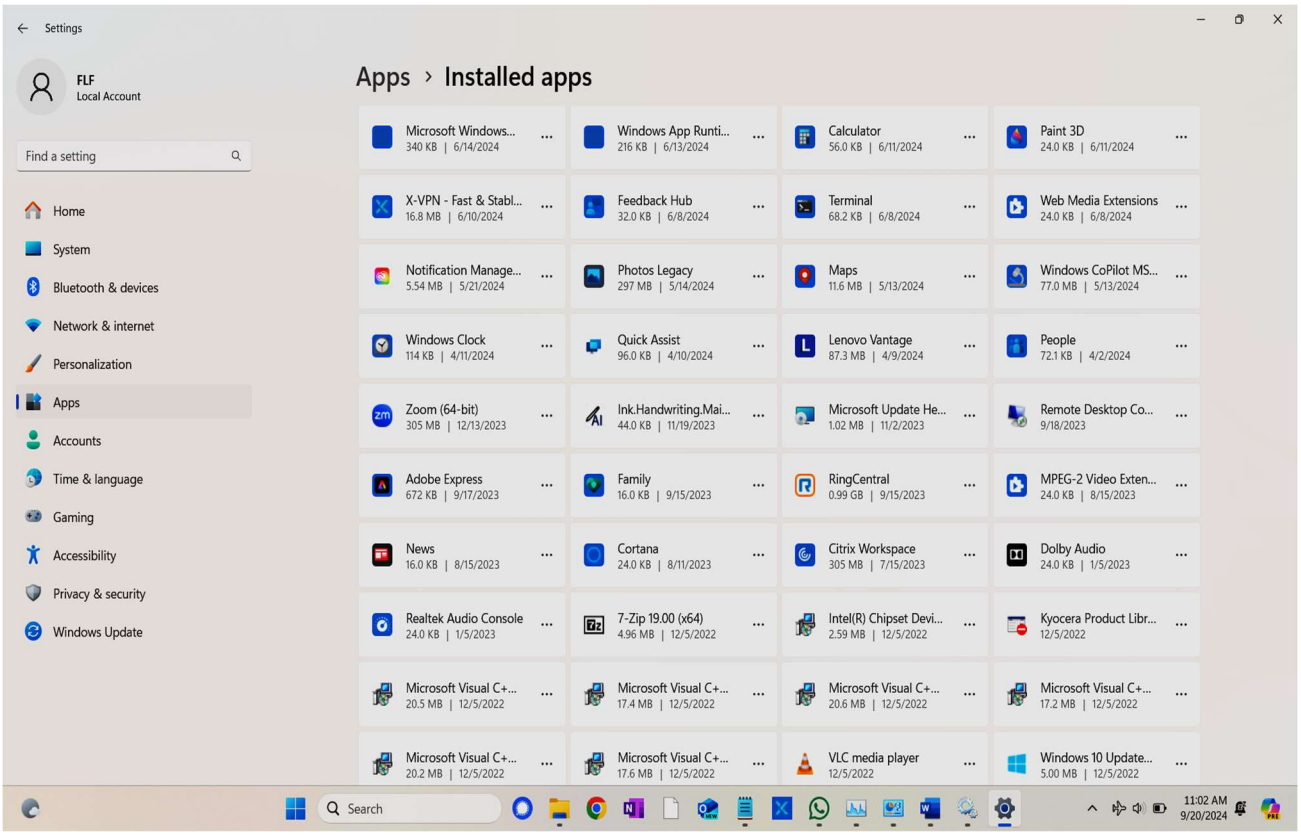
754. Prior to April 2024, Farrow's cellular data usage averaged approximately 1GB per month.

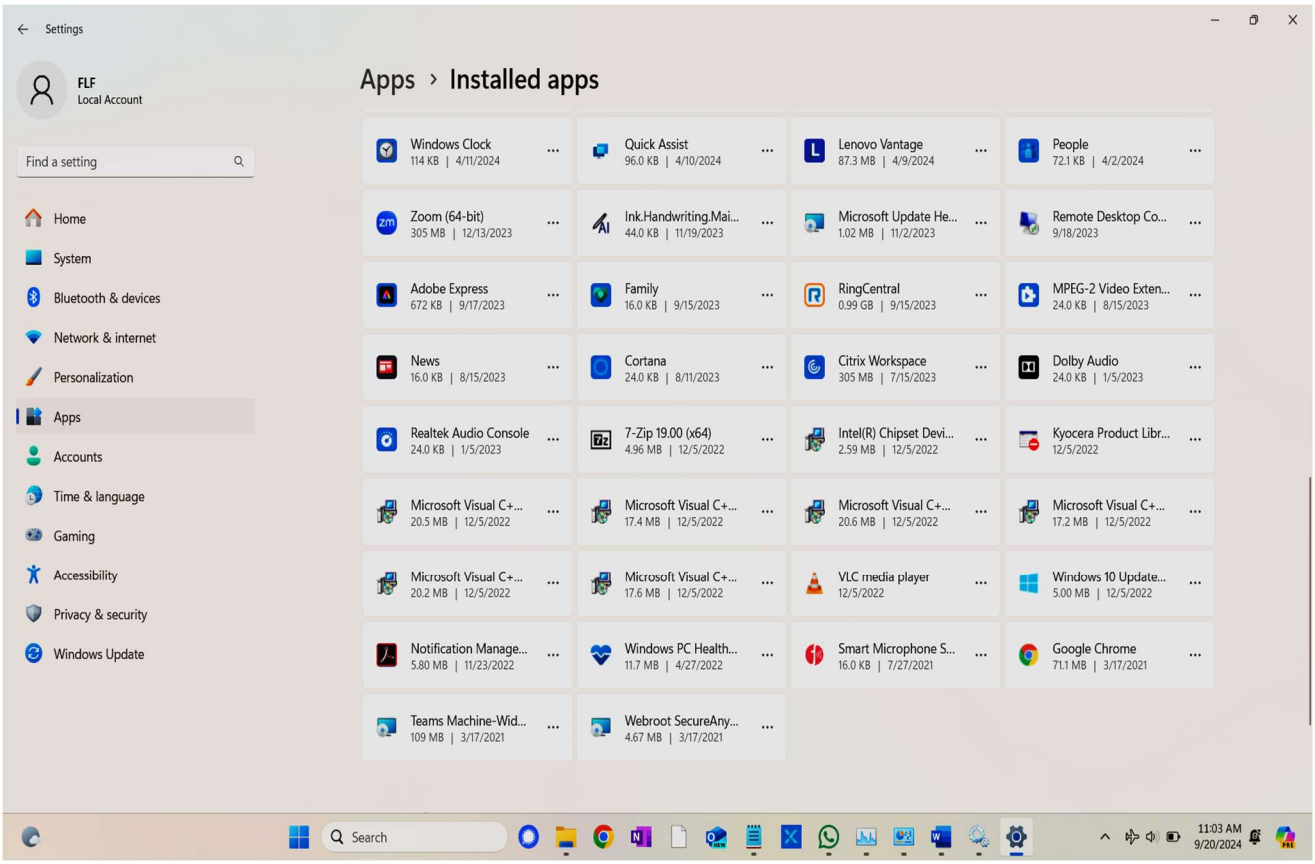
755. From April 2024, through June 30, 2024, the Threat Actor Defendants used Farrow's cell phone and its cellular data to mask spikes of their activities, and, to create hundreds of communication filters which expended cellular data which were used to intercede and interject themselves in communications Farrow was having with Farrow Law's staff, opposing counsels, and his own attorneys,

756. Using the MitM Attack vector with Farrow's cell phone, resulted in Farrow receiving text messages from clients and opposing counsel which were, in reality, communications from the Defendants.

Unauthorized Software Installations, Modifications and Application Repackaging:

757. From April 11, 2024 through July 2024, (as reflected in the demonstrative screenshots from Farrow's Lenovo business computer), Farrow's business lap top registered 200% more application installations and modifications to existing applications in that from 2021 through April 10, 2024.


Settings
FLF
Local Account
Find a setting
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Apps › Installed apps
Microsoft Windows... 340 KB | 6/14/2024
Windows App Runti... 216 KB | 6/13/2024
Calculator 56.0 KB | 6/11/2024
Paint 3D 24.0 KB | 6/11/2024
X-VPN - Fast & Stabl... 16.8 MB | 6/10/2024
Feedback Hub 32.0 KB | 6/8/2024
Terminal 68.2 KB | 6/8/2024
Web Media Extensions 24.0 KB | 6/8/2024
Notification Manage... 5.54 MB | 5/21/2024
Photos Legacy 297 MB | 5/14/2024
Maps 11.6 MB | 5/13/2024
Windows CoPilot MS... 77.0 MB | 5/13/2024
Windows Clock 114 KB | 4/11/2024
Quick Assist 96.0 KB | 4/10/2024
Lenovo Vantage 87.3 MB | 4/9/2024
People 72.1 KB | 4/2/2024
Zoom (64-bit) 305 MB | 12/13/2023
Ink.Handwriting.Mai... 44.0 KB | 11/19/2023
Microsoft Update He... 1.02 MB | 11/2/2023
Remote Desktop Co... 9/18/2023
Adobe Express 672 KB | 9/17/2023
Family 16.0 KB | 9/15/2023
RingCentral 0.99 GB | 9/15/2023
MPEG-2 Video Exten... 24.0 KB | 8/15/2023
News 16.0 KB | 8/15/2023
Cortana 24.0 KB | 8/11/2023
Citrix Workspace 305 MB | 7/15/2023
Dolby Audio 24.0 KB | 1/5/2023
Realtek Audio Console 24.0 KB | 1/5/2023
7-Zip 19.00 (x64) 4.96 MB | 12/5/2022
Intel(R) Chipset Devi... 2.59 MB | 12/5/2022
Kyocera Product Libr... 12/5/2022
Microsoft Visual C+... 20.5 MB | 12/5/2022
Microsoft Visual C+... 17.4 MB | 12/5/2022
Microsoft Visual C+... 20.6 MB | 12/5/2022
Microsoft Visual C+... 17.2 MB | 12/5/2022
Microsoft Visual C+... 20.2 MB | 12/5/2022
Microsoft Visual C+... 17.6 MB | 12/5/2022
VLC media player 12/5/2022
Windows 10 Update... 5.00 MB | 12/5/2022
Search
11:02 AM
9/20/2024



758. These unauthorized installations evidencing the same spike in unauthorized activities as do the administrative logs, Farrow's cell phone records, and reflect the Threat Actor Defendants expanding their privileges and permissions by installing applications into FLF's Network that also had vulnerabilities which the Threat Actor Defendants used specifically in June and July 2024, to completely remove Farrow as one of Farrow Law's Network administrators allowing them complete control over the network.

SITTING DUCK CYBER ATTACKS- breadcrumbs to thumbprints

759. In a fourth metric of exponential activity relates to the Sitting Duck Cyber Attacks, which includes DNS Hijacking, IP Spoofing and MitM Cyber Attacks which explode in February 2024 through present.

760. Here, the Threat Actor Defendants utilization of the Siting Duck Cyber Attacks substantially increase, corresponding with increases in FLF's Administrator log activity, the data usage on Farrow's cell phone, and the installation of unauthorized computer applications - all during a time when more serious allegations had yet to be a matter of public record.

761. For example, between 2019 and March 2023, the Threat Actor Defendants utilized the Sitting Duck Cyber Attack as against 20 web or hosting server domains.

762. Between March 2023 and January 2024, the number had increased to a total of 47 in approximately 5 years from 20 to 47.

763. However, from mid-January 2024 through July 2024, the Threat Actor Defendants had attacked over 100 domains, more than doubling in seven months their utilization of the Sitting Duck attacks in comparison to the nearly five previous years.

20240109 -SEMINOLECLERK.COM-EARL DONALDSON-DOMAINDISCOVER.pdf
20240111 -KETMW.COM-NS37-38-WORLDNIC-MELTZA.pdf
20240113 -KEVIN LEUNG - FTITECHNOLOGY.COM-4NS-AWSDNS-19COM.pdf
20240113 -TROUTMAN.COM-OC CCFED CASE PDNS97-ULTRADNSCOM-20240624-WEBCOM.pdf
20240116 -TRIALLAWFLA.COM-IOA LAWYER CHARLES MELTZ-NS-19-20-WORLDNICCOM-20241003.pdf
20240116 -TRIALLAWFLA.COM-IOA LAWYER MELTZ-NS19-20 WORLDNIC.pdf
20240119 -MYTRAFFICSERVER.COM-DNS1-2-STABLE.pdf
20240122 -RAESHERNLAW.COM-FLA-COCOUNSELPROSPECT-NS67-NS68-DOMAINCONTROL.COM.pdf
20240122 -WELLSFARGO.COM-EDNS1-ULTRADNSBIZCOM-NET-A1-189-AKAMNET-MM.pdf
20240123 -ROSSMANLEGAL.COM-REPLACED FLF RE KEVIN D CASE SQUARESPACEDNS.pdf
20240125 -PBL-LAW.COM-OPPCO-JTRCASES-NS69-70-DOMAINCONTROLCOM-DbyPx.pdf
20240131 - WOMACK - LAW.COM - KHLOE-PRANAB-CLOUDFLARE-WOMACK 2020 CASE.pdf
20240202 -BURKENDT.COM-NS-LAWSINFLORIDA-JUDGE SPRYENSKI.pdf
20240202 -WOMACK - BURKENDT.COM-SERVER UPDATE FOR LAWSINFLORIDA.COM DOMAIN.pdf
20240210 -HOLIDAYRUSSELLCOM-FLF LAWYERS -enomcom5NS-NAME-SERVICESCOM20240513.pdf
20240212 -FLCOURTS.ORG-BLANK-.US-NS.pdf
20240213 -DILPIPER-OC-CCFED CASE-CHRIS OPRISON- PDNS-ULTRADNSBIZCOM-NET-ORG-PERFECTPRIVACY...
20240213 -PRIVATEMAIL.COM -EDNS1-4-REGISTRAR-ULTRA-sternwithheldforprivacy.pdf
20240214 -COMPASSINVESTIGATIONS.NET-processserver-DOUG-LORNA -CLOUDFLARE.pdf
20240218 -SHAREPOINTONLINE.COM - PHISHING EMAIL MAR 24.pdf
20240220 -CISION.COM-VENDORFOR-FLFPRESSRELEASES-AWSDNS.CO.UK-20240919-VENDOR.pdf
20240220 -COUNTRYSIDECYCLE.NET-JLF-UNCLE-WEBSITE-fastdomain-NS1-2-HYPERNET-20240726.pdf
20240220 -WELDERDIGITAL.COM-FLF MEDIA-WEBSITE-VENDOR-FLF-OTHERPROJECTS-DOMAINCONTROLCO...
20240220-NWFCU.ORG-JLF CAR LOAN - ULTRADNSNET-20240624-WEBCOM.pdf
20240224 -MESHDIGITAL.COM-CNS3-CNS4-SECURSERVERNET.pdf
20240224 -ROIGLAWYERS.COM-OC-CCFED CASE FOR NATIONWIDE JLF ATTEMPTS 20 TIMES TO CONNECT - N...
20240227 - DNSIMPLE.COM - SERVER FOR CRIMINALLAW.COM - BERMAN.pdf

20240229 -GUNSTER.COM-NS-MAGNOLIA-RUBEN-CLOUDFLARECOM -PERFECTPRIVACY-WEBCOM-FTILAWYE...
20240302 -ACENTRIA.COM - NAUGHTON.pdf
20240302 -ASENTRIA.COM-CLIENTEMPLOYER-AFTER-IOA-NS17-NS18 DOMAINCONTROL -NAUGHTON.pdf
20240303 -HOLIDAYRUSSELL.COM - SERVER UPDATE FOR SERVER HOSTEDEMAILCOM-NS1-3-MDNSSERVICE...
20240304 -MORANKIDD.COM-NS-EUGENE-JILLIAN-NS-CLOUDFLARECOM-IOARITENOURLAWYERS.pdf
20240306 -WIEDER - MCCLATCY-MIAMIHERALDCOM-REPORTER-BENWIEDER-NS1-4-KR123.pdf
20240307 -HOSTINGMATRIX.COM-SERVERSOFNEWYORKFIRM-IOAFRAUD-SUBPOENA-ON20240306-NS1-2-.pdf
20240307 -WIEDER - HOSTINGMATRIX.COM-SERVER-MCCLATCY-REPORTER-WIEDER-MARRIAGE-NS1-2-HOS...
20240308 -CLARKLAWPA.COM-FORMER-LAWYER-NAUGHTON-LEFTCASE-20200620-NS01-02-DOMAINCONTR...
20240309 -CIVITEKSOLUTIONS.COM - SERVER OF SERVER CHANGED TO DIGICERTDNS.NET-.COM-CHANGED....
20240309 -DIGICERTDNS.NET-COM-SERVER FOR OPP-LAW-FLFCLIENT-STRENGER-TIMEOFMEDIATION-MARC...
20240309 -FD.COM-marcusbfticonsulting-UDNS1-2-CSCCOMUK.pdf
20240309 -MYFLCOURTACCESS.COM- SERVER CHANGE FOR SERVER DIGICERTDNS.COM.pdf
20240309 SUNBIZ.ORG - worxwebllc-wittenbergharry-.pdf
20240310 -HEATHRITENOUR.COM--DbyPxllc-NS21-NS22-DOMAINCONTROLCOM.pdf
20240310 -JOHNRITENOUR.NET -NS21-NS22-DOMAINCONTROLCOM.pdf
20240311 -CHOPPEDNCHEESY.COM -FLF FORMER CLIENT NEW BUSINESS-.pdf
20240313 -SANYIABOOTH.ORG SERVER CHANGE -KNKNWhsllcNS123wordpress.pdf
20240317 -CONTACTPRIVACY.COM -tieredacess.pdf
20240319 -DNSTINATIONS.COM -NS1-7MARKMONITORCOM-gmpgorgheathjohnboothcode.pdf
20240319 -WOMACK - STMICHAELSLEGALCENTER.COM-WOMACK-WORKS-QUOTED.pdf
20240320 -FTIDELTA.COM-UDNS1-UDNS2-CSCDNS.pdf
20240324 -AZURE-DNSCOM-AZURE-DNSINFO-CROWELL SERVERS.pdf
20240324 -VOLCANOCOFFEE.COM - JOHN RITENOUR RESTAURANT SERVER UPDATE FOR SERVER IDIRECT.NE...
20240325 -MYPRIVATENAME.COM-FLF CLIENT GUNTER AND VENDOR NS85-86WORLDNIC-NEWFOLD-FLWLA...
20240327 -REGUS.COM-FLF-LANDLORD-EMAILS-CHANGEIP-20240321-NETNAMESNET-UK.pdf
20240328 -CIVITEKFLORIDA.NET-EARL DONALDSON - FACC -DOMAINDISCOVER.pdf
20240328 -SANYIABOOTH.ORG - PRIVATEWHO-IS-NS1-3-WORDPRESSCOM-ADMIN-CHANGE.pdf
20240330 -COMPLETECAREIT.COM-FLF-IT-VENDOR-PERFECTPRIVACY.pdf

20240402 -CIVITEKFLORIDA.ORG-EARL DONALDSON - FL ASS COURT CLERKS-DOMAINDISCOVER.pdf
20240402 -DYNECTNET-paypal servers.pdf
20240406 -DVIDSHUBCOM-CARLBOOTH-IdentityProSvr-identity-protectorg.pdf
20240408 -AIMBRIDGEHOSPITALITY.COM - MARRIOTT PROP MANAGER AND FTI CLIENT.pdf
20240408 -GOIPOWER.COM SERVER FOR FLF LANDLORD ATTORNEY WSH-LAW-BRENDADAVIDNScloudflarec...
20240410 -GOLDBERGSAGALLA.COM -OPPCOUNSEL-3NS-AWSDNS-18COM.pdf
20240411 -ADAMSDISPUTERESOLUTION.COM -NS39-40-DOMAINCONTROLCOM-naughtonalpine.pdf
20240414 -AKAMNET-SERVERS-FOR-FORMER-NAUGHTON-ATTORNEY-FLFRESOURCE.pdf
20240414 -ANONYMISEDCOM-COMLAUDE-UK-SERVERS-GTLAW.pdf
20240414 -ROSSMANLEGAL.COM - SERVER CHANGE - FORMER FLF CLIENT NEW COUNSEL CASE.pdf
20240414 -SQUARESPACEDNSCOM-DNS1-4P06-NSONECOM-NS01-04-SQUARESPACEDNSCOM-eaton.pdf
20240414 -WIEDER - STABLETRANSIT.COM -serversfortownstylebenwieder-NS1-2-HOST.pdf
20240415 -KOLAWYER.COM - FORMER FLF CLIENT - MICHAEL MAYS LAW FIRM -NS41-42-DOMAINCONROLCO...
20240416 -FAKE SUBPOENA LAW FIRM stabletransitcom-serversnewyorkfirmsentfakesubformoran-cscglobal'.p...
20240416 -FLABAR.ORG-SERVER FOR CENTURYLINK.COM - CENTURYTEL.NET UPDATED.pdf
20240416 -REGUS.COM SERVER CHANGE-NETNAMESNET-UDNS1-2-CSC.pdf
20240423 -FTICONSULTING.COM-CCFED MAIN DEFENDANT - cgctechUDNS1-CSCDNSNET.pdf
20240423 -PROKARTEXP.COM-FLFCLIENT-INTENSE-EMAILS-BEGIN-202404-NS45-46-DOMAINCONTROL-hyjac...
20240424 RANDYBERMAN.COM - TAKEN OVER NO WEBSITE.pdf
20240428 -FLABAR.ORG - SERVER CHANGE FOR SERVER CENTURYLINK.NET -NS1-2CENTURYLINKTEL.pdf
20240429 -WOMACK - JOHNSONSTRATEGIESLLC.COM-UPDATE TO SERVER CALIDESIGN.NET-WOMACK INSUR...
20240430 -ATTDNSCOM-NS1-4-bellsouth-CSCGLOBALCOM.pdf
20240502 -ANZ.COM-AKAN-KevinLeung-PERFECTPRIVACY.pdf
20240505 - 18JUDICIAL.ORG C052623-contactprivacycomCANAD.pdf
20240506 -PRNEWSWIRE.COM-ARA-BAT-NSCLOUD.pdf
20240506 -WIEDER - NEXCESSNET-serverpppfraudpicBENWIEDER-NS-1479-AWSDNS-23.pdf
20240509 -PPPFRAUDCHRONICLECOM - JLF SPEAKING WITH BEAN OFFICE-BENWIEDER-NS1-4-NEXCESS-NET...

20240509 -tylertechcom-AWSDNS-under-egovcom.pdf
20240510 -SAUL.COM-NS91-92-WORLDNICCOM-OC-GARCIA CASE-REP CARRIERS.pdf
20240513 -NAME-SERVICESCOM-DNS1-5-NAME-SERVICESCOM.pdf
20240516 -CNRS.FR-SKINNYBENWIEDER.pdf
20240516 -RANKMATHCOM-LILYANA-RAYDEN-CLOUD-heathjohnboothcode-onecom.pdf
20240518 -SPARKLIGHT.NET - NS1-4 CABLEONE.COM.pdf
20240519 -SHUTTS.COM - SERVER UPDATE FOR SERVER PNAPNET-NS-A-D-PNAPNET.pdf
20240521 -FLORIDA LAWYERS ASSISTANCE - AFFINITYHEALTH-SRI-ULLA-CLOUDFLARE-FLA.pdf
20240521 -WOMACK - LAWYERLEGION.COM-STABLETRANSIT.COM-WOMACK.pdf
20240522 -WIEDER - MIAMIHERALD.COM SERVER FOR SERVER CHANGE -NS1-4-KR123COM-.pdf
20240523 -ACCONLINE.COM-SIMON-WIEDER-advancedcomputer-NS59-60-WORLDNIC.pdf
20240523 -THINKINTEGRATED.COM-JOHN RITENOUR OWNER - CHRISTINE VINES - NS1-4-ASMNETCOM-C01...
20240524 -DOMAINPRIVACYGROUP.COM-NS1-2-NETFIRMCOM-SKYLAKES-WHEELOCK.pdf
20240527 -JHSMIAMI.ORG - SERVER UPDATE FOR SERVER WORLD4YOUBIZ-jhsmiamiorg.pdf
20240528 -ENONCOM-NEWADMIN-FARROWSLAWYER-HOLIDAYRUSSELLCOM.pdf
20240604 -WOMACK - AVVO.COM-BEAU-DANICA-CLOUDFLARE-WOMACK 2525 PONCE.pdf
20240606 -COUNTRYSIDECYCLE.NET - CHANGE SERVER FOR SERVER HYPERNETCOM--NS-NS2HOLA.pdf
20240606 -JFBUSINESSLAWCOM-anativeoc-NS10-NS11-WIXDNS.pdf
20240606 -MYFLCOURTACCESS.ORG - SERVER UPDATE FOR SERVER RDAPANCHOR.COM.pdf
20240608 -BUCKMILES.COM-OPP COUNSEL-LAWFIRM-SERVER FOR SERVER CHANGE.pdf
20240615 -EFILEMADEEASY.COM-PALM-BCH-CTY-NS10-15-DNSMADEEASYCOM.pdf
20240619 -COUNTRYSIDECYCLE.NET-SERVER FOR SERVER CHANGE TO HOLACOM-ALLINTERNETSALES-STOPP...
20240620 -FLDFS.COM-NAMEDSERVER- OPP COUNSEL MYFLORIDACFOCOM-JTRCASE-NS01-04-FLDFSCOM.pdf
20240620 -LAWYEROFJUSTICE.COM-NS10-11-WIXDNSCOM-DOMAIN OF FORMER FLF LAWYER.pdf
20240620 -MYFLORIDACFO.COM -LAWFIRM IN JTR CASE - CHANGE SERVER-NS01-04-FLDFSCOM.pdf
20240621 -SECURESERFVER.NET.pdf
20240621-RISKSCORE.COM - IOA - SERVER FOR SERVER CHANGE TO SECURESERVERNET-riskscorecomserver....

764. Upon information and, belief, as the above and following collaterally strategic web domains associated with Farrow, Farrow Law, and Dr. Doe illustrate, since mid January 2024 and the beginning of January 2025, the Threat Actors have utilized the Sitting Duck Attack in furtherance of their APT over 250 instances, with the following domains associated with Florida's eFiling Authority, the Florida Bar, Farrow's clients, Opposing Counsels, Ben Wieder, Mr. Womack, Flcourts.org, flcourts18.org, Infant Doe's pre-school, jacksonhealthsystems.org, jhsmiami.org, fljud13.org, Florida's eFiling payment portal, close contacts, and C2 Domains and C2 Servers. which bolster fictitious information about Wieder and Mr. Womack for example.

20240804 -JACKSONHEALTHSYSTEM.ORG-NS-sk-s7-ans1-ns-klsycom
20240804 -TORRESLAWFL.COM-probono-DAVID-LAURA-CLOUDFLARE
20240805 -FLABAR.ORG - SERVER CHANGE FOR SERVER CENTURYLINKCOM-AUTHNS1-2CENTURYLINKNET-FLABARORG-cscgl...
20240805 -JHSMIAMI.ORG - DR.JANEDOE- SERVER CHANGE FOR SERVER TO WORLD4YOU.COM
20240806 -pendingrenewaldeletioncom-VA-WEBCOM
20240807 -CSCDNSORG-CSCGLOBALCOM-pdns1-2-CSCDNSNET
20240808 -tucows-NS1-3tucowscom-tieredaccesscom
20240809 - fljud13.org
20240809 -FLWLAW.COM-PERFECTPRIVACY-GUNTERCASE
20240811 -GTLAW.COM-comlaudecom-4NS-AWSNDS-25COM
20240812 -WINSTON.COM-foslidhouston-PERFECTPRIVACY-CLOUDFLARE
20240814 ----GRAY-ROBINSON.COM-NS0-4-DNSMADEEASYCOM----PERFECTPRIVACY-
20240816 -web-hostingcom-tipcyber-EDNS1-4-REGISTRAR-
20240819 -FLCOURTS.ORG - CHANGE SERVER OF ADMIN networksolutionsprivateregistrationcom-HEIDI-REX-CLOUDFLARE-flc...
20240819 -networksolutionsprivateregistration-PERFECTPRIVACY-HEIDI-REX-CLOUDFLARE
20240820 -WOMACK - LISAMILLERASSOCIATES.COM-ALEXIS-COCO-NS-CLOUD-WOMACK 2020
20240824 - DNSIMPLE-EDGE.NET - SERVER CHANGE FOR DNSIMPLE.COM - BERMAN
20240824 -BLUESHARQCOM-FLF CLIENT - NS39-40-DOMAINCONTROL-strenger
20240824 -MGMRECOVERYORG-FLF CLIENT NS21-22-DOMAINCONTROL-
20240824 -STBLAW.COM-OPAL-VALENIN-CLOUDFLARE-PERFECTPRIVACY-WEBCOM
20240824 -WIEDER - NABJONLINE.ORG-WIEDER-MAY2024butreportfrom2023-banjonkline
20240826 -TOWNSTYLE.COM-benwiederruthigielnik-NS1-2-MYTRAFFIC
20240829 -CALEZCAPITAL.COM-ELLE-JAZIEL-NS-CLOUDFLARE
20240829 -CSCDNSUK-DNS1-2CSCDNSNET-menswh-CSCGLOBALCOM
20240830 -NETNAMES.COM-CSCUDNS1-CSCUDNSCOM
20240905 -FBI-TELEPORTER01ORG-sameday-NS275-34-AWSDNS-24com-IdProSrc
20240907 -GOFAMILYLAWYERS.COM -NS53-54-DOMAINCONTROL-BOOTH
20240908 - LAPIAZZAACADEMY.COM - INFANT DOE - SAME REG-TECH MARK

20240908 -FLORIDASUPREMECOURT.ORG-NS2-3 FLCOURTS.ORG
20240909 -WOMACK - LAW.NET-SOFTLAYER.COM-WOMACK INSURANCE LAWYER
20240912 - NAMEFIND.COM SERVER FOR OC SHELL BAY
20240912 -LOGS.COM OC-JTR AND OTHER CASES - PDNS11-12-DOMAINCONRTROLCOM
20240913 - ULTRADNS.ORG
20240917 SOFLOINDUSTRIAL.COM CLIENT OM
20240918 -FLABAR.ORG-SERVER CHANGE
20240919 -BIT.LY-JUDGE JOSEPH PERKINS - SERVERCHANGE - AWSNDS-24NET
20240919 -FLCLERKS.NET-EARL DONALDSON - FACC-DOMAINDISCOVER
20240919 -FTITECHNOLOGIES.COM - SERVER CHANGE FOR SERVER AWSDNS-19COM
20240919 -MYFLCOURTACCESS.NET-EARL DONALDSON - FACC DOMAINDISCOVER
20240919 -MYFLORIDACOURTACCESS.COM-EARL-DOMAINDISCOVER
20240919 -PAYFLCLERKS.COM-BLANK-LOOKSLIKE-EARL-TIERRA.NET
20240919 -SEMINOLECLERK.NET-EARL DONALDSON-FACC-DOMAINDISCOVER
20240919 -WIEDER - AWSDNS-23COM-PPPFRAUDDOMAIN - ASSOCIATED BEN WIEDER-HIGHLYPROTECTED
20240920 -MCCALLA.COM-FLF CLIENT MILLS-A1-BERNS-B1-BERNS
20240920-COMCAST.NET-DNS101-105-COMCASTNET-CSCGLOBALCOM
20240923 -VOLCANOSCOFFEE.COM-JOHN RITENOUR RESTAURANT NS1-2PENDINGRENEWALDELETIONCOM-johnritenour
20240924 -AWSDNS-45ORG-ASSOCIATED WITH FORMER FLF CLIENT CHARLENE EATONPIC-BEHANCENET
20240924 -BIT.LY-JUDGE JOSEPH PERKINS - SERVERCHANGE-AWSDNS-43ORG
20240924 -FLCLERKS.ORG-EARL DONALDSON -DOMAINDISCOVER
20240924 -MYFLCOURTACCESS.ORG-reg-auth-EARL DONALDSON
20240924 -MYFLORIDACOURTACCESS.COM-EARL DONALDSON - FACC-DOMAINDISCOVER
20240924 -MYFLORIDACOURTACCESS.ORG-EARL DONALDSON FACC --tierranet
20240924 -MYFLORIDACOURTACCESS.ORG-EARL DONALDSON -FACC-DOMAINDISCOVER-
20240924 -PAYFLCLERKS.ORG-BLANK-EARL DONALDSON-NS-FLCLERKS.COM-EARL
20240924 -WIEDER - AWSDNS-40-ORG-pppfraudBENWIEDER-HIGHLYPROTECTED-MARKMONITOR
20240924 -WIEDER - AWSDNS-56ORG-pppfraudBENWIEDER-HIGHPROTECTION
20240928 -WIEDER - MIAMI.COM-ASSOCIATED WITH BEN WIEDER-NS1-4-KR123.COM

765. Each instance of an update correlates to a strategic target at a strategic time, and was accomplished by the threat actor defendants to accomplish the Ultimate Goals of the APT.

766. **SPEAR PHISHING/SOCIAL ENGINEERING**: A fifth vector vulnerability infiltration which substantially increased from May 28, 2024 through July 10, 2024, were the spear phishing emails directed at Farrow and Farrow Law which were designed to cause substantial interferences with Farrow and Farrow Law's business activities, workflows, and with communications.

IX. THE TADS' OPERATIONS AFTER FARROW LAW'S EFFECTIVE CLOSURE

The Ongoing Persistent Attacks Achieve All Ultimate Goals

767. **On July 15, 2024,** five days after the federal court denied Farrow's last motion requesting a hearing on July 10, 2024, using only that old computer and external hard drives, Farrow drafted and drove to the Courthouse to file what became Jay Farrow v. FTI Consulting, Miami-Dade Circuit Court, Case Number 24-13000-CA-01 ("2024 Family Circuit Case").

768. Immediately after filing the Verified Complaint, Farrow had the stamped copy scanned and email from a court-services company, Judicial Investigations, to the personal email of a close family member, an Assistant United States Attorney (Miami Office) Farrow worked for when he clerked for the Miami-Dade State Attorney's Office in 2000 and a personal his personal @yahoo.com address having not discovered that the same had been compromised until September 27, 2024.

769. Upon information and belief, on July 16, 2024, the Threat Actor Defendants forwarded the July 15, 2024 email from the court services company to unknown recipients.

770. **On July 19, 2024**, after three days of drafting a Petition for Cyberstalking Injunction against FTI CEO Steven Gunby, Farrow went for a third time to the Miami Court district

where it took over six hours to file the Petition in the Domestic Division and receive a case number ("2024 Domestic Cyberstalking Case").

771. However, the Domestic Violence Circuit Court took no time in entering its first order directing the Washington, D.C. Capitol Police to find FTI's CEO Steven Gunby and serve the judicial order requiring Gunby to appear on August 9, 2024 to defend against the charges.

772. As retaliation, between July 15 and 19, 2024, the Threat Actor Defendants sent Farrow and Farrow numerous emails designed to create situational crisis events, panic and fear.

773. As retaliation, on July 19, 2024, hours after Farrow filed the 2024 Domestic Cyberstalking Case against FTI's CEO Steven Gunby, Dr. Jane Doe received a call from alleged Farrow Law clients when she was in front of Infant Doe. These individuals yelled and screamed at Dr. Jane Doe, called her disparaging racial names and they threatened to 'come after her' physically.

774. **Before, On and After July 19, 2024**, as with the call from a purported client on July 19, 2024, the Threat Actor Defendants had used and continued to use AI generated voiced cloned calls to create situational crisis events, and interfere with family relationships of Farrow and Dr. Doe.

775. By July 20, 2024, the Threat Actor Defendants made over 30 AI generated calls to Farrow and Dr. Doe which were convincing and essentially a perfect imitation of the family

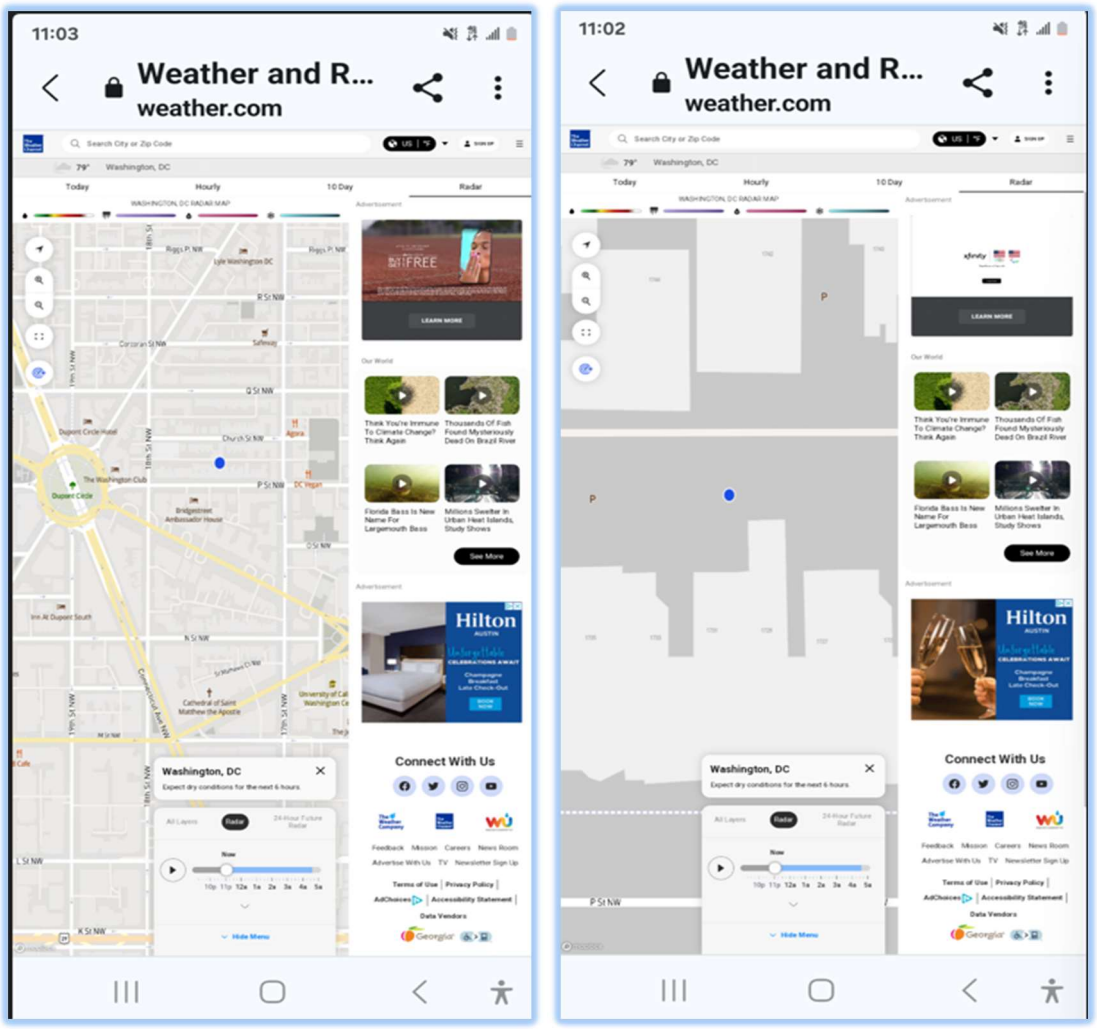
member, or other individual such that the receipt of any telephone call was, in itself, the cause of a situational crisis event.[22]

776. These calls resulted in decisions not to leave the family home unless necessary for work or hand-filing documents in court.

Farrow's Galaxy 22 Phone Reveals Location of Remote Access User

777. By July 31, 2024, Farrow discovered that his main cell phone which he no longer used, a Galaxy 22+ Ultra, which was hacked, mirrored and cloned by Defendants in June 2024 was "located", **very close to FTI headquarters in Washington, D.C. and a location where it has used computer servers of one of the companies/vendors.**

[22] Farrow and Dr. Jane Doe believe that the phone calls were AI generated voice clone spoofing calls as each one was with an individual whose chosen words, responses and answers to questions were so out of proportion and context with anything related to the individual, that on at least two of these calls the 'individual' who had initiated the call hung up abruptly. By July 30, 2024, Farrow had some tools which to 'test' whether they were actually speaking with a family member, friend or other known person such as asking questions which would establish the authenticity of the conversation. It became a hallmark sign that the individual caller would hang up the phone when confronted with questions or that they had provided incorrect answers.



From August through December 2024

778. **On August 6, 2024**, Farrow filed a Supplemental Petition in the 2024 Domestic Cyberstalking Case in person at the Miami-Dade Circuit Court. This Supplemental Petition was the result of weeks of work to extra photos and data, print the same out at a print store, write the supplemental petition and rewriting it after much of it was compromised from an infected hard-drive, all the while having to work through the latest situational crisis events, such as his mother receiving threatening calls from Wells Fargo bank after being release from a 10 hospitalization.

779. In this instance, the Threat Actor Defendants used AI Voice Calls to harass Farrow's mother, and unauthorized access to networked protected computers which successfully resulted in Farrow's mother and father's bank accounts to be frozen, and thereafter permanently closed, within 3 days of her hospitalization and just 15 days after the same bank froze and permanently closed all of Farrow and Farrow Law's accounts.

780. Additionally, by August 6, 2024, the stress and emotional toll upon Plaintiffs was substantial, particularly after an AI Voice Call from one of Farrow's trusted contacts, which was by far, the most deceptive through August 6, 2024, suggested Farrow call Gunby or email him to apologize for filing the May 28, 2024 Amended Complaint "before [Farrow] gets two bullets in the back of [his] head."

781. **On August 8, 2024,** Farrow and Dr. Jane Doe appeared at the scheduled hearing for FTI's CEO Steven Gunby to appear and defend against the Cyber-Stalking Injunctions. CEO Gunby did not appear and the matter was reset to August 29, 2024.

782. **On August 11, 2024**, Farrow, Dr. Doe and Infant Doe were evicted from a hotel room in Miami where they had sought to escape the Threat Actor Defendants' cyber-fence so as to celebrate Infant Doe's birthday. However, as these arrangements were made months previous to August 11, and the receipt for the hotel stay was emailed to Dr. Doe's compromised Gmail account, the Threat Actor Defendants used AI Voice Calls and unauthorized access to protected computers to cause two hotel security guards to vigorously evict the family from their room early Sunday morning, and paraded them through the lobby which cancelled the birthday breakfast planned to acknowledge Infant Doe's second birthday.

783. This event, just one business day after Farrow and Dr. Doe appeared at the August 8, 2024 hearing seeking a permanent injunction against Gumby, caused substantial trauma and emotional distress to Infant Doe as he witnessed hotel security issue order after order to Dr. Doe that she 'hurry' packing and immediately vacate the premise.

784. **On August 19, 2024,** Plaintiffs filed an Ex Parte Verified Emergency Motion in the July 19 Farrow Case, and on August 23, 2024, Dr. Doe submitted an Affidavit in support of that Motion. This Ex Parte Motion did not include, as Plaintiffs did not have at that time, *inter alia,* the Expert Report of Marlin Technologies, the facts and allegations regarding the MitM attacks, or the pattern of conduct revealed by the Sitting Duck Cyber Attacks or the evidence and facts related to the unauthorized infiltrations into the Florida Bar's protected computers or Florida's eFiling Authority's protected computers.

785. **August 29, 2024** Farrow and Dr. Jane Doe appeared again for the second time for the second scheduled hearing for FTI CEO Steven Gunby to appear to face the Cyberstalking allegations, however, he did not appear and that hearing has been rescheduled to October 9, 2024, leaving Plaintiffs no recourse and no relief whatsoever.

786. **September 4, 2024 through present:** As Farrow Law's Network and substantially all files therein were actually or constructively stolen as of approximately July 10, 2024, since that time, and as it relates here to the timeline of events, the Threat Actor Defendants have used a sprawling array of methods and means to achieve unauthorized access into strategically advantageous Networks, and their protected computers, hosting servers, email servers, and communication devices for malicious purposes directed at achieving all their Ultimate Goals which remained after successfully procuring the effective closure of Farrow Law, shutting down

its network, and severing communications between Farrow, his staff, clients and family and friends.

787. **Since September 4, 2024 through present**, the Threat Actor Defendants, the Threat Actor Defendants have continued obtain, maintain and advance their privileges and permissions within these Networks, protected individual computers within those Networks, new computers used by Farrow since August 2024, email servers, hosting servers, personal emails and/or personal communication devices, such as cell phones, iPads and Android Tablets in their continuing concerted effort to achieve their Ultimate Goals.

788. On September 16, 2024, Farrow spoke with John Derek Womack, a purported attorney working for the Florida Bar who claimed there were numerous bar complaints which required a response. Farrow informed Mr. Womack of the factual timeline herein described, and also that on September 4, 2024, two Special Agents from the FBI Miami Field Office came to his and Dr. Doe's home in response to their separate reports of cyber-crime.

789. On September 16, 2024, Farrow also informed Mr. Womack that he had gone to the Miami Field office on or about September 5, 2024 to meet with the two agents, and provided th.me FBI Agents with some of his electronic devices for inspection, and that his responses to any complaint would substantially be identical.

790. On September 16, 2024, Farrow also filed an Amended Motion for Restraining Order and Injunctive Relief in the 2025 Family Circuit Case.

791. On September 17, 2024, Farrow received an email from Mr. Womack that purportedly identified the alleged Bar Complaints, yet blocked out part of the case numbers and emanated from an email which did not belong to Mr. Womack.

792. On September 24, 2024, Farrow called Mr. Womack at his purported extension, and with no answer, proceeded to call his 'legal secretary' who connected the call. During this conversation, Mr. Womack agreed that Farrow could provide one response to the individual Bar Complaints which he could serve on Mr. Womack the week ending October 11, 2024, and would likely come in the form of a filed Second Amended Injunction Motion.

793. During this call, Farrow expressed serious concerns for at least two of the clients whom were able to speak and communicate with Farrow since August 2024, and that both of their emails and cell phones had been attacked, and their emails compromised. As such, Farrow and Mr. Womack agreed to allow Farrow to submit one response and not yet serve the individual bar complainants as Farrow was anticipating receiving updates from the FBI investigation.

794. Moreover, as there was a rescheduled hearing in the 2024 Domestic Case against Gunby on October 9, 2024, Farrow and Mr. Womack agreed that any such 'unlimited paged' response would be due after October 9, 2024.

795. On September 30, 2024, Farrow filed the Second Verified Amended Injunction in the 2024 Family Circuit Case.

796. On September 30, 2024, Farrow received a letter of default from a purported attorney for his landlord, Regus Management. However, Farrow had spoken to Regus about the FBI investigation and the cyber-attack and Regus was intent on learning more information and cooperating with any investigation for the protection of its other clients at its Columbus Center Coral Gables Location.

797. Farrow attempted to reach this attorney, located in Oklahoma, but no response was ever received. On October 4, 2024, Heath Ritenour and John Ritenour were served with copies of

the September 4, 2024 Amended Complaint and the Second Amended Injunction Motion of September 30, 2024.

798. On October 10, 2024, Farrow, using a new domain and email, attempted to serve a copy of the Amended Complaint and Motion upon other parties to the 2024 Family Circuit Case, but they were all rejected, as were other emails Farrow attempted to use.

799. On October 13, 2024, one of Farrow's previous clients reached out to him through a third party.

800. On or about October 14, 2024, this client received a contextually threating social media message followed by the exact type of cell phone interference and spear phishing emails and text messages.

801. n October 14, 2024, Farrow, the first business day after the reopening of the courthouse after weather related closures of the previous week, Farrow served a copy of the 'response' to Mr. Womack and his legal assistant.

802. On October 14, 2024, Farrow received a confirmation of receipt from the legal assistant.

803. While not discovered until December 2024, the next day, October 15, 2024, the Threat Actor Defendants used unauthorized access to prepare a letter stating that Farrow failed to respond to the Bar inquiries.

804. While not discovered until December 2024, from October 15, 2024, through October 18, 2024, over 10 letters were prepared and signed by Mr. Womack with each going to Richard Wiess, the purported Chief of Grievance Committee 17F of the Fort Lauderdale Branck of the Florida Bar.

805. On October 17, 2024, Farrow sent materials and further information to the FBI.

806. On October 18, 2024, a letter was posed on Farrow's Office door from the law firm of Wiess Serota – of which Chief Richard Wiess is the firm's founder.

807. On October 18, 2024, hours later, Farrow received an email from Mr. Womack's legal assistant stating she was 'sorry' that she had not gotten these 'letters moving' regarding Farrow's alleged failure to respond to an office Bar inquiry. This email was served upon, Chief Richard Wiess and Farrow, and in violation of their clear agreement, upon Farrow's email address which had been hacked by the Threat Actor Defendants.

808. Throughout the next week, Farrow receive more emails from Mr. Womack's legal assistant, although he could not reach Mr. Womack. In fact, Farrow has not heard back from Mr. Womack via telephone since September 24, 2024.

809. On October 23, 2024, Farrow attempted to email Mr. Womack and his legal assistant and he received a message that his legal assistant was out of town. Farrow called the Florida Bar and asked to speak with this legal assistant, and was informed she had been on vacation for the last week and a half and not otherwise available. The Florida Bar representative was very clear that she had not been in the office and could not account for her sending out any letters on October 18 through October 23, 2024.

810. In late October 2024, Farrow was contacted by another client who purportedly filed one of the bar complaints, and he sent Farrow all the letters he received which included each and every letter related to each other alleged Bar complaint.

811. Once again, Farrow contacted the Florida Bar with respect to this apparent breach of protocol, and that he had not heard from Mr. Womack and he would not respond to any

communication. In response, Farrow was redirected to Mr. Womack's alleged legal assistant's voicemail.

812. On October 30 and 31, 2024, Farrow discovered that one of Farrow Law's client(s)' and communication systems with those client(s) had been compromised. Upon reestablishing contact, Farrow informed them that he needed to report that he was and is privy to information related to some of his clients working with federal agencies in active domestic law enforcement operations, and that this particular communication compromise created a real and present danger to that individual and others.

813. On November 2, 2024, Farrow requested an emergency meeting at the Miami Field Office and that afternoon he met with two Special Agents and provided them with specific information that should this happen again, and he may have to seek relief in circuit court for a restraining order as it would be the only means of stopping the interference.

814. On November 4, 2024, Farrow drove to the Florida Bar from Miami to deliver an updated response, and to provide them with his communications with the FBI such that there would be no question that his response had been received.

815. On November 4, 2024, Farrow received a phone call from Reporter Wieder, and at that time, he did not know about his alleged previous two articles.

816. Wieder informed Farrow, as alleged further herein, that he was writing an article about him abandoning his clients, and the two spoke for over an hour.

817. On November 11, 2024, pursuit to a repeated breach of the confidential communication system with one of his clients who was working with a federal agency during an active domestic field operation, Farrow filed a motion seeking a 72-hour restraining order.

However, upon information and belief, due to the Threatt Actor Defendants' unauthorized accuses into protected computers related to the Miami-Dade Clerk's Court Map, he could not upload the emergency motion properly.[23]

818. On November 20, 2024, a hearing was unilaterally scheduled upon FTI's second motion for enlargement of time to respond to the Amended Complaint.

819. Farrow attended that hearing, and hours later, one of his clients who had reestablished contact received an email directly from the JTR Partners attorney which provided them 2 hours to select a hearing date upon JTR's motion for summary judgment with the message that if they did not respond, that JTR's attorneys would unilaterally schedule the hearing.

820. On November 25, 2024, the Florida Bar through Womack filed a Petition for an Order to Show Cause as to why Farrow should not be immediately suspended for alleged failure to respond to an office bar inquiry. However, Farrow was not served by Womack or the Florida Bar at that time.

821. This Petition, which was advanced by Chief Richard Wiess, alleged Farrow failed to respond after receiving Womack's September 17, 2024 email, and alleged that Farrow had not provided any cause whatsoever to justify his failure.

822. On December 4, 2024, Farrow did receive an acknowledgement from the Florida Supreme Court of a new case requiring Farrow to respond by December 17, 2024.

---

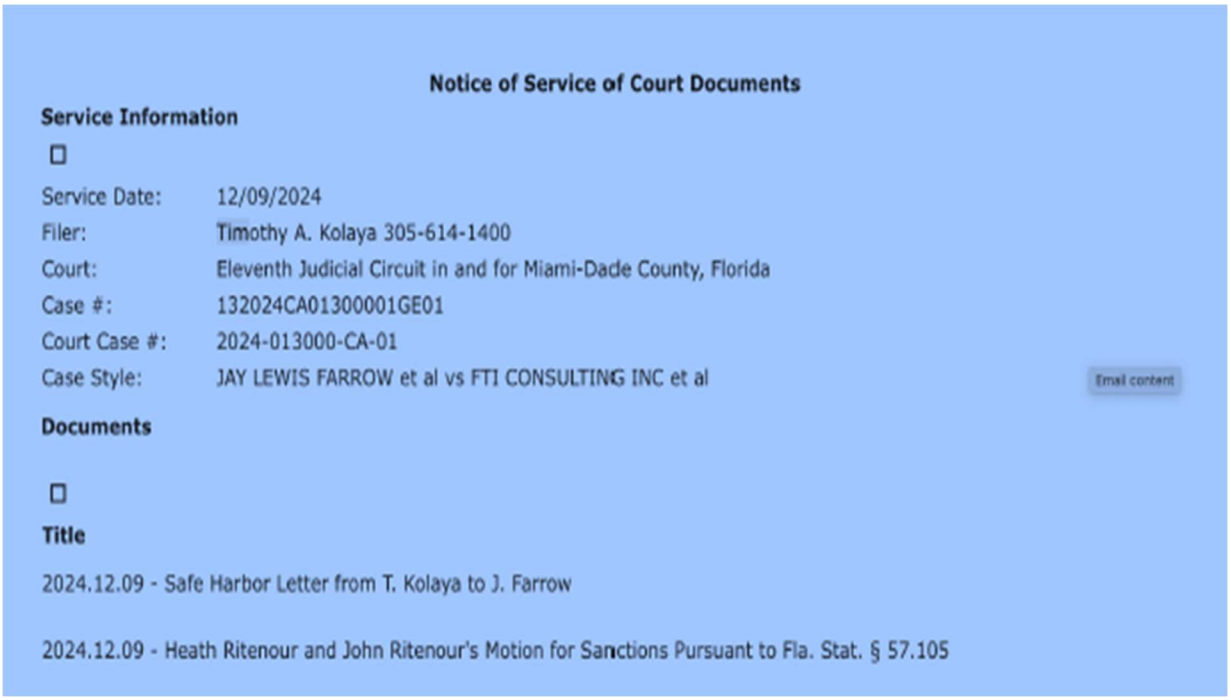
[23] A copy of the November 11, 2024 Emergency Motion is incorporated herein and appended as Exhibit "E". While Farrow believed he uploaded this Emergency Motion and corresponding proposed order, the same had suffered the same issues with the Miami-Dade CourtMap portal Farrow had experienced since October 2024.

823. On or about December 5, 2024, Farrow was traveling for purposes of obtaining an expert opinion as to the cyber-attack and after receiving the same, he drove to Tallahassee for a second time, first visiting the Clerk's Office of the Florida Supreme Court to inquire as to whether the Petition was filed.

824. On December 7, 2024, Chief Richard Wiess' firm filed a lawsuit on behalf of Farrow Law's Landlord for eviction, although a copy of same was not posted on Farrow Law's Office Door at that time.

825. On December 9, 2024, Farrow received an email from Defendant Kolaya entitled "Notice of Service of Court Documents", which referenced two documents, one was a motion for sanctions pursuant to Fla. Stat. 57.105 as against Farrow, Dr. Doe and Farrow Law, and the other was a letter which warned Farrow to disclose the letter and the motion to "his wife".

826. December 9, 2024 was the date the "57.105 Motion" was served, and thus any referenced being filed in court or otherwise that the accompanying letter was filed in court was false.



Notice of Service of Court Documents

Service Information

Service Date:	12/09/2024
Filer:	Timothy A. Kolaya 305-614-1400
Court:	Eleventh Judicial Circuit in and for Miami-Dade County, Florida
Case #:	132024CA01300001GE01
Court Case #:	2024-013000-CA-01
Case Style:	JAY LEWIS FARROW et al vs FTI CONSULTING INC et al

Email content

Documents

Title

2024.12.09 - Safe Harbor Letter from T. Kolaya to J. Farrow

2024.12.09 - Heath Ritenour and John Ritenour's Motion for Sanctions Pursuant to Fla. Stat. § 57.105

827. On December 16, 2024, because the response to Florida Supreme Court's Order was of obvious importance, Farrow drove to Tallahassee again to file the same in person.

828. Hours before he departed, on December 16, 2024, Chief Richard Wiess's firm, Defendant Wiess Serota, posted an alleged filed Lawsuit for Eviction on Farrow Law's Office Door.

829. On December 18, 2024, due to the fact that Farrow was not able to file in person and that the ePortal system indicated that his Response to the Petition was rejected, he turned around to Tallahassee to hand-file the Corrected Response.[24]

[24] True copies of Farrow's December 18, 2024 Corrected Response to the Florida Bar Petition for Order to Show Cause and December 27, 2024 Motion for Protective Order and for Confidentiality Instructions in the matter styled Florida Bar v. Jay Lewis Farrow, Florida Supreme Court, Case Number: 2024-1681 are Appended hereto Marked Composite Exhibit "F."

830. On December 22, 2024, Farrow received an Order from the Florida Bar indicating that his hand filing was incomplete, that pages 21 through 36 were missing and that it was missing a certificate of service.

831. Due to this, Farrow's plan to spend time with Dr. Doe and Infant Doe out of town was substantially interfered with and consumed with repeated attempts to electronically file his document.

832. The Florida Bar was served, however, via email to Mr. Womack's email address on December 18, 2024, and Farrow received a response from Mr. Womack admonishing Farrow not to visit the Florida Bar in person and that he would respond timely with the Florida Bar's Reply on December 27, 2024.

833. However, Womack did not respond on December 27, 2024.

834. Instead, on December 31, 2024, a different attorney filed a Reply.

835. On January 3, 2024, with precise evidence of the compromises of the Florida Bar and Florida's eFiling Authority's networks, Farrow, Dr. Doe and Infant Doe traveled together to Tallahassee to deliver the evidence to the Florida Supreme Court Clerk and the Florida Bar.

836. As further alleged hereinbelow, ne++ither Dr. Doe, Farrow or Farrow Law received anything from the Florida Bar except a Substitution of Counsel by Randell Berman for the Florida Bar who also has not responded to any communications.

X. NETWORKS, INDIVIDUAL PROTECTED COMPUTERS AND EMAIL SERVERS UNLAWFULLY ACCESSED BY THE THREAT ACTOR DEFENDANTS

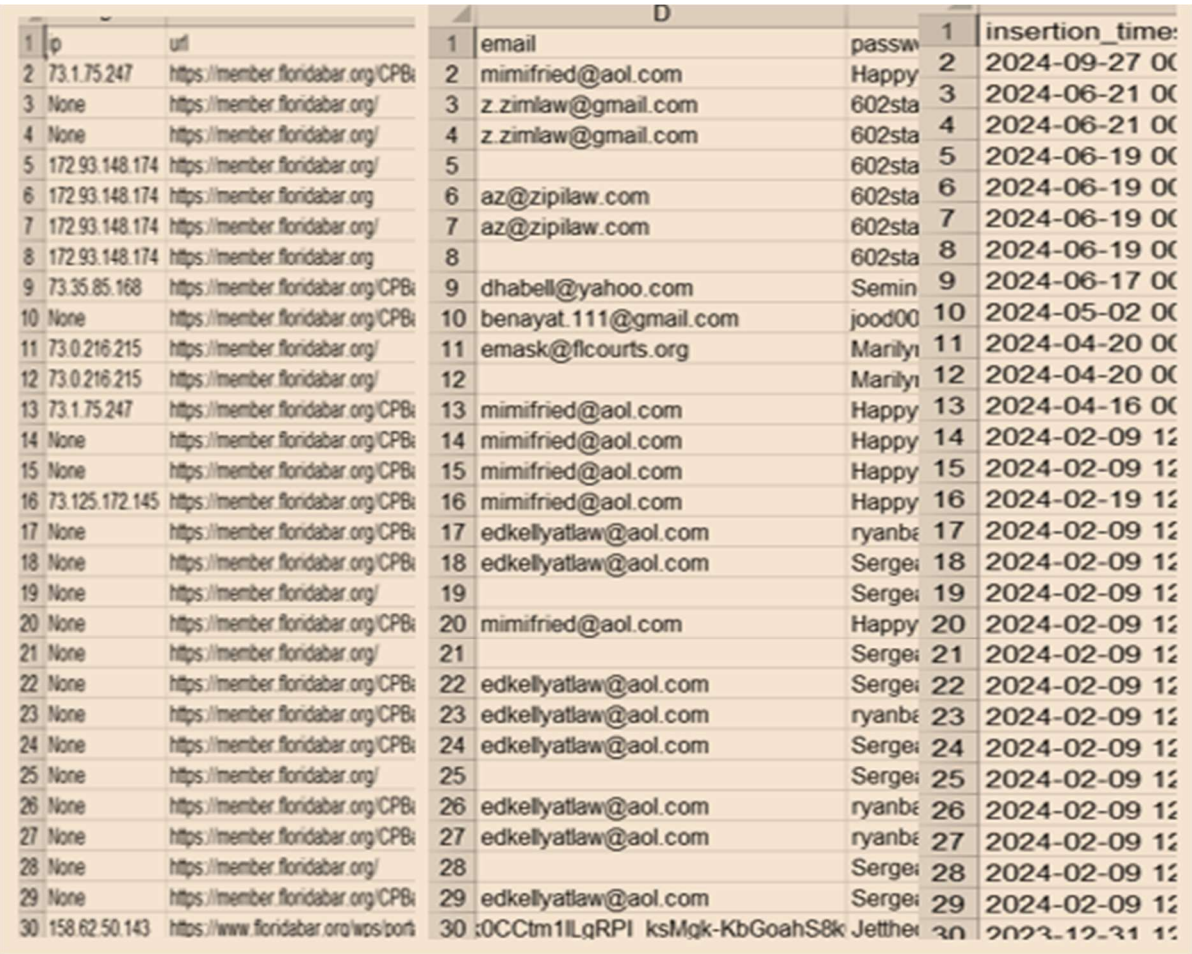
The Florida Bar and Florida's eFiling Authority's Networks and Protected Computers

837. From at least September 2023, the Threat Actor Defendants infiltrated the protected Florida Bar Network, its individual protected computers and had achieved other unlawful access for malicious purposes directed to and have caused Plaintiffs substantial damages and harm.

838. From at least September 2023, the Threat Actor Defendants infiltrated the protected Florida Bar Network, its individual protected computers and had achieved other unlawful access for malicious purposes.

839. More specifically, these unauthorized infiltrations were, *inter alia,* for purposes of the Threat Actor Defendants' illicit use of confidential information, forms and login credentials such as to prepare documents, and, in some cases, file court documents related to Farrow under the guise the same were filed by a purported client and/or authorized Florida Bar staff attorney or Bar Counsel.

840. The following screenshots represent partial views of the URLs, usernames, passwords and time stamp logs of entries into the Florida Bar Network.



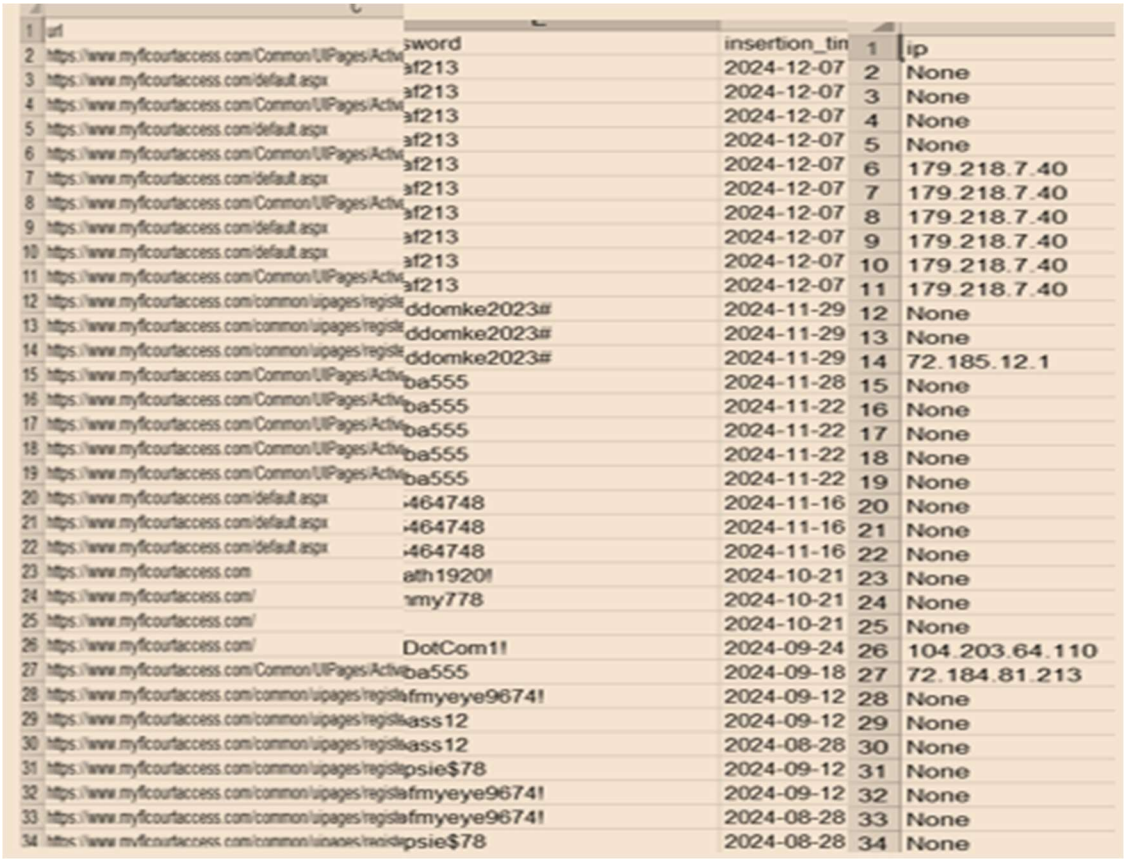
	ip	url
2	73.1.75.247	https://member.floridabar.org/CPB
3	None	https://member.floridabar.org/
4	None	https://member.floridabar.org/
5	172.93.148.174	https://member.floridabar.org/
6	172.93.148.174	https://member.floridabar.org
7	172.93.148.174	https://member.floridabar.org/
8	172.93.148.174	https://member.floridabar.org
9	73.35.85.168	https://member.floridabar.org/CPB
10	None	https://member.floridabar.org/CPB
11	73.0.216.215	https://member.floridabar.org/
12	73.0.216.215	https://member.floridabar.org/
13	73.1.75.247	https://member.floridabar.org/CPB
14	None	https://member.floridabar.org/CPB
15	None	https://member.floridabar.org/CPB
16	73.125.172.145	https://member.floridabar.org/CPB
17	None	https://member.floridabar.org/CPB
18	None	https://member.floridabar.org/CPB
19	None	https://member.floridabar.org/
20	None	https://member.floridabar.org/CPB
21	None	https://member.floridabar.org/
22	None	https://member.floridabar.org/CPB
23	None	https://member.floridabar.org/CPB
24	None	https://member.floridabar.org/CPB
25	None	https://member.floridabar.org/
26	None	https://member.floridabar.org/CPB
27	None	https://member.floridabar.org/CPB
28	None	https://member.floridabar.org/
29	None	https://member.floridabar.org/CPB
30	158.62.50.143	https://www.floridabar.org/wps/portal

	D	
1	email	passw
2	mimifried@aol.com	Happy
3	z.zimlaw@gmail.com	602sta
4	z.zimlaw@gmail.com	602sta
5		602sta
6	az@zipilaw.com	602sta
7	az@zipilaw.com	602sta
8		602sta
9	dhabell@yahoo.com	Semin
10	benayat.111@gmail.com	jood00
11	emask@flcourts.org	Marilyn
12		Marilyn
13	mimifried@aol.com	Happy
14	mimifried@aol.com	Happy
15	mimifried@aol.com	Happy
16	mimifried@aol.com	Happy
17	edkellyatlaw@aol.com	ryanba
18	edkellyatlaw@aol.com	Serge
19		Serge
20	mimifried@aol.com	Happy
21		Serge
22	edkellyatlaw@aol.com	Serge
23	edkellyatlaw@aol.com	ryanba
24	edkellyatlaw@aol.com	Serge
25		Serge
26	edkellyatlaw@aol.com	ryanba
27	edkellyatlaw@aol.com	ryanba
28		Serge
29	edkellyatlaw@aol.com	Serge
30	:0CCtm1lLqRPI ksMqk-KbGoahS8k	Jetthe

	insertion_time
2	2024-09-27 0(
3	2024-06-21 0(
4	2024-06-21 0(
5	2024-06-19 0(
6	2024-06-19 0(
7	2024-06-19 0(
8	2024-06-19 0(
9	2024-06-17 0(
10	2024-05-02 0(
11	2024-04-20 0(
12	2024-04-20 0(
13	2024-04-16 0(
14	2024-02-09 1:
15	2024-02-09 1:
16	2024-02-19 1:
17	2024-02-09 1:
18	2024-02-09 1:
19	2024-02-09 1:
20	2024-02-09 1:
21	2024-02-09 1:
22	2024-02-09 1:
23	2024-02-09 1:
24	2024-02-09 1:
25	2024-02-09 1:
26	2024-02-09 1:
27	2024-02-09 1:
28	2024-02-09 1:
29	2024-02-09 1:
30	2023-12-31 1:

841. At the very least, between August and present, the Threat Actor Defendants have gained unauthorized access to Florida's eFiling Authority, and the protected computers attached and/or connected to such network and have used such unauthorized access for malicious purposes, such as to substantial interfere with Farrow, Dr. Doe, Infant Doe and Farrow Law's ability to file court documents electronically. Below are examples of infiltrations into various URLs associated

with Florida's eFiling Authority, such as myflcourtaccess.com, as well as, IP addresses, usernames, partial passwords and time stamps.



	url	sword	insertion_tin		ip
2	https://www.myflcourtaccess.com/Common/UIPages/Activ	af213	2024-12-07	2	None
3	https://www.myflcourtaccess.com/default.aspx	af213	2024-12-07	3	None
4	https://www.myflcourtaccess.com/Common/UIPages/Activ	af213	2024-12-07	4	None
5	https://www.myflcourtaccess.com/default.aspx	af213	2024-12-07	5	None
6	https://www.myflcourtaccess.com/Common/UIPages/Activ	af213	2024-12-07	6	179.218.7.40
7	https://www.myflcourtaccess.com/default.aspx	af213	2024-12-07	7	179.218.7.40
8	https://www.myflcourtaccess.com/Common/UIPages/Activ	af213	2024-12-07	8	179.218.7.40
9	https://www.myflcourtaccess.com/default.aspx	af213	2024-12-07	9	179.218.7.40
10	https://www.myflcourtaccess.com/default.aspx	af213	2024-12-07	10	179.218.7.40
11	https://www.myflcourtaccess.com/Common/UIPages/Activ	af213	2024-12-07	11	179.218.7.40
12	https://www.myflcourtaccess.com/common/uipages/regist	ddomke2023#	2024-11-29	12	None
13	https://www.myflcourtaccess.com/common/uipages/regist	ddomke2023#	2024-11-29	13	None
14	https://www.myflcourtaccess.com/common/uipages/regist	ddomke2023#	2024-11-29	14	72.185.12.1
15	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-11-28	15	None
16	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-11-22	16	None
17	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-11-22	17	None
18	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-11-22	18	None
19	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-11-22	19	None
20	https://www.myflcourtaccess.com/default.aspx	-464748	2024-11-16	20	None
21	https://www.myflcourtaccess.com/default.aspx	-464748	2024-11-16	21	None
22	https://www.myflcourtaccess.com/default.aspx	-464748	2024-11-16	22	None
23	https://www.myflcourtaccess.com	ath1920!	2024-10-21	23	None
24	https://www.myflcourtaccess.com/	-my778	2024-10-21	24	None
25	https://www.myflcourtaccess.com/		2024-10-21	25	None
26	https://www.myflcourtaccess.com/	DotCom1!	2024-09-24	26	104.203.64.110
27	https://www.myflcourtaccess.com/Common/UIPages/Activ	ba555	2024-09-18	27	72.184.81.213
28	https://www.myflcourtaccess.com/common/uipages/regist	afmyeye9674!	2024-09-12	28	None
29	https://www.myflcourtaccess.com/common/uipages/regist	ass12	2024-09-12	29	None
30	https://www.myflcourtaccess.com/common/uipages/regist	ass12	2024-08-28	30	None
31	https://www.myflcourtaccess.com/common/uipages/regist	psie$78	2024-09-12	31	None
32	https://www.myflcourtaccess.com/common/uipages/regist	afmyeye9674!	2024-09-12	32	None
33	https://www.myflcourtaccess.com/common/uipages/regist	afmyeye9674!	2024-08-28	33	None
34	https://www.myflcourtaccess.com/common/uipages/regist	psie$78	2024-08-28	34	None

l79.218.7.40	https://www.myflcourtaccess.com/default.aspx	shoaf213
l79.218.7.40	https://www.myflcourtaccess.com/default.aspx	shoaf213
l79.218.7.40	https://www.myflcourtaccess.com/default.aspx	shoaf213
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	
72.185.12.1	https://www.myflcourtaccess.com/common/uipages/register.aspx	
Vone	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/default.aspx	kian123
Vone	https://www.myflcourtaccess.com/default.aspx	kian123
Vone	https://www.myflcourtaccess.com/default.aspx	kian123
Vone	https://www.myflcourtaccess.com	
Vone	https://www.myflcourtaccess.com/	
Vone	https://www.myflcourtaccess.com/	Jessm85
l04.203.64.110	https://www.myflcourtaccess.com/	
72.184.81.213	https://www.myflcourtaccess.com/Common/UIPages/ActivationCor	Summer
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	ampareja
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	ampareja
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	
Vone	https://www.myflcourtaccess.com/common/uipages/register.aspx	

842. While Farrow and Dr. Doe have information databased within close to 2000 rows between the Florida Bar and Florida's eFiling Authority.

843. With respect to the Florida Bar, the login theft permits either the Threat Actor Defendants or others, to also login to that Florida Bar attorney's account of, for example, law enforcement agencies, flcourts.org, and other highly protected networks.

https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://clearwaterfl.mycusthelp.com/WEBAPP/_rs/(S(jxgqedtpbf5siyh3osj3	jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezr	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezr	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://leecountysheriff.govqa.us/WEBAPP/_rs/(S(dztht24ymq1vebykx0dm	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://securemail.csbflorida.com/s/e	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org
https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org
https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG

844. As with any network, unauthorized access in the same provided the Threat Actor Defendants to advance the privileges and permissions for that user and to also achieve access after stealing another user's credentials.

845. On November 25, 2024, the Threat Actor Defendants' unlawful access to protected networks and computers belonging to the Florida Bar caused a Petition to be filed against Farrow seeking his immediate suspension.

846. On December 18, 2024, Farrow file his response to that petition, and the same is incorporated herein by reference.

847. On December 30, 2024, Farrow filed a motion for protective order and motion to permit filing of confidential documents specifically documenting unlawful uses of login credentials belonging to several Florida Bar counsels, as well as evidence documenting unlawful access to Florida's eFiling Portal. The same is appended hereto and incorporated herein by reference.

848. On January 3, 2024, Farrow, Dr. Doe and Infant Doe personally visited the Florida Supreme Court Clerk's Office to ensure it had on its docket system, Farrow's December 18, 2024 Response and the December 30, 2024 Motions for Protective Order and Confidentiality.

849. On January 3, 2024, Farrow, Dr. Doe and Infant Doe personally hand-delivered the evidence of direct uses of Florida Bar counsel's login credentials, and the evidence of the infiltrations of Florida's eFiling Portal.

850. However, through the filing of this Verified Complaint, there has been no communication from the Florida Bar, nor has it filed any updated response to the Florida Supreme Court to Farrow's Motion for Protective Order.

851. On December 31, 2024, a Reply to Farrow's December 18, 2024 Corrected Response to the 'Petition' for Order to Show Cause was not filed by 'John Derek Womack'. It was purportedly filed by 'Staff Counsel' for the Fort Lauderdale Branch of the Florida Bar, Patricia Savitz.

852. On or about January 8, 2025, the Florida Bar filed, purportedly through yet another "Bar Counsel" and/or Staff Counsel, Randell Berman, a "Notice of Substitution of Counsel."

853. Since January 3, 2025, Farrow attempted to reach both Ms. Savitz and then Mr. Berman, with no response.

854. From at least late-August through present, the Threat Actor Defendants have used, and continue to use, a variation of a MitM Cyber Attack to deny Farrow contact with the Florida Bar, and they have done so using unauthorized access to protected computers connected to the Florida Bar Network.

855. From at last late-August through present, notwithstanding Farrow's attempts to communicate with the Florida Bar, responding as agreed, and hand-delivering responses, communications with Farrow and the FBI Miami Field Office, and then evidence of at least some of the user accounts, user names and passwords being compromised, along with evidence that Farrow Law's clients who have reconnected with Farrow have been targeted repeatedly, the Florida Bar continues to issue various correspondences evidencing that new bar employees' individual accounts have been compromised.

856. The Petition filed directly or indirectly, by the Threat Actor Defendants remains pending as of the time of the filing of this Lawsuit.

857. The Motion for Protective Order remains pending as of the time of the filing of this lawsuit.

Florida Lawyer's Assistance, Inc. – Unauthorized Access to Protected Computers

858. In May, 2022, a collateral target website domain for Florida Lawyer's Assistance was "updated" according to its official records, meaning that the website domain either changed ownership, a permission to access the website domain from a new administrator was uploaded or the authoritative named servers for the website domain were changed.

859. As of December 2024, FLA was unaware of any authorized updates to the DNS records of its website which would have triggered an update in its ICANN records.

860. As part of the FLA program, from at least February 2020 through the beginning of June 2024, Farrow attended the 'Fort Lauderdale Tuesday 5:30pm' FLA group's confidential meeting with other lawyers, judges and other legal professionals to discuss and share issues related to the FLA program via "RingCentral" video connection application.

861. The link remained the same each week, however, it was calendared into Farrow Law's Network Calendar as a reoccurring meeting. The calendar entries had the email addresses to all the invitees.

862. Prior to February 2020, these Tuesday evening Fort Lauderdale meetings were conducted at St. Anthony's Church in downtown Fort Lauderdale, and Farrow had regularly attended those meetings since 2017.

863. Other than legal professionals, the weekly meeting is not opened to the public, is considered highly confidential given the nature of the topics discuss and to foster and encourage open dialogue.

864. No legal professional is required to be officially associated with the FLA programs to attend, and the same is to foster an environment where anyone willing to seek support may do so confidentially and the same is critical to FLA's mission.

865. Moreover, the highly confidential requirements to be in attendance is one of the protections for participants.

866. The other is that nothing discussed at the meeting can be shared with anyone else not in attendance or not part of the FLA program.

867. The content of or the participants of any FLA meeting is a substantial reason for the success of the program, which has been in existence for over 40 years and has supported thousands of lawyers and members of the judiciary.

868. FLA meetings are not recorded, and are not permitted to be recorded by any participant or any third party as the information discussed is confidential, however, the date, time and zoom invitation may be put into a participant's online calendar, which is what Farrow had done on a reoccurring basis since January 2018.

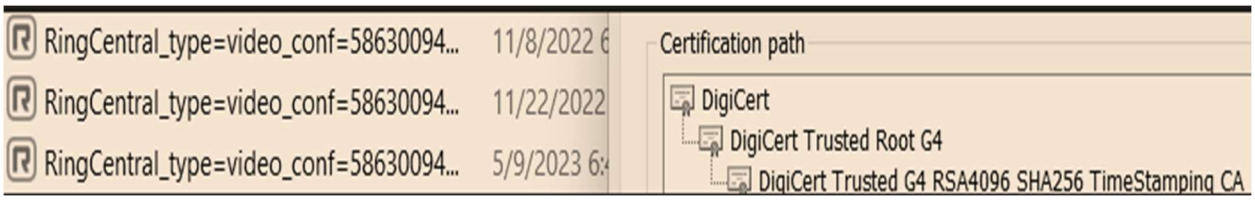
869. From January 2018 through present, Farrow has successfully adhered to his obligations as documented in his HIPPA protected records, and sworn to by FLA administrators in various Affidavits from 2018 to present which were stored in Farrow Law Firm's OneDrive Databased in an encrypted file which no other member of the firm had access to except for Farrow as administrator.

870. Due to his commitment to FLA and any obligations on his part, Farrow was asked by FLA to monitor new FLA members as to their progress in the program, and to record monthly reports into a health application on his cell phone.

871. In or about September 2024, in reviewing the hard drive of the Lenovo computer he had used since 2021, he discovered a folder which captured the weekly calendar entries for the FLA meetings and which had been assembled in order in that folder which had not existed prior to May or June 2024.

872. In December 2024 and January 2025, aside from the computer registering recorded calendar entries for the FLA meetings, it also registered files indicating that certain meetings were recorded, and those recordings were exfiltrated from the hard drive. Nevertheless, the dates and

times of the modifications of these files, and the signature certificates reveal the Theat Actor Defendants monitored these meetings, and in some cases recorded these confidential meetings.



873. Further, from at least 2022, Farrow had submitted monthly reports through this health application which information was and is protected by HIPPA, and the same included, photographs of any prescribed medications, which were stored in the Farrow Law Encrypted Administration Folder.

874. In late June, along with the rearranged photos of Infant Doe, Farrow and/or Dr. Doe, next to an individual suffering physical harm, was a photo album of the photos of prescriptions Farrow had taken as part of being in compliance with FLA.

875. While Farrow's social media over the course of years was dedicated to supporting others suffering from trauma response related life challenges, he did not give the Threat Actor Defendants permission to infiltrate the Farrow Law Network, FLA's Network or Affinity Heath's Network, or his personal cell phone to retrieve his FLA records.

876. However, FLA's Network was the subject of the Theat Actor's DNS Hijacking Scheme in or about May 2022, as was Affinity Health.

877. Farrow is proud of FLA, his participation in it, and the work he has done with other lawyers and legal professionals successfully handling the FLA program.

878. Here, however, the Threat Actor Defendants used the agreements Farrow had with FLA, the photographs, the collection of meetings with participant information, and information

obtained through monitoring the Tuesday 5:30 RingCentral meetings, as a form of medical shaming and extortion.

879. More specifically, in what remained of Farrow Law's folders and files found in the "Downloads" folder, there were specifically designated sub-folders, one of which contained rearranged documents, pfds and other materials related to Farrow's FLA documents.

880. Further, with respect to the rearranged and maliciously created 'photo albums' Farrow received on his cell phone, one related to photos Farrow regularly took for his participation in FLA and otherwise protected by HIPPA.

881. Farrow has been a member of FLA for nearly a decade, he has provided FLA with personal medical information, and has monitored other legal professionals going through their requirements to complete voluntary and non-voluntary contracts with FLA.

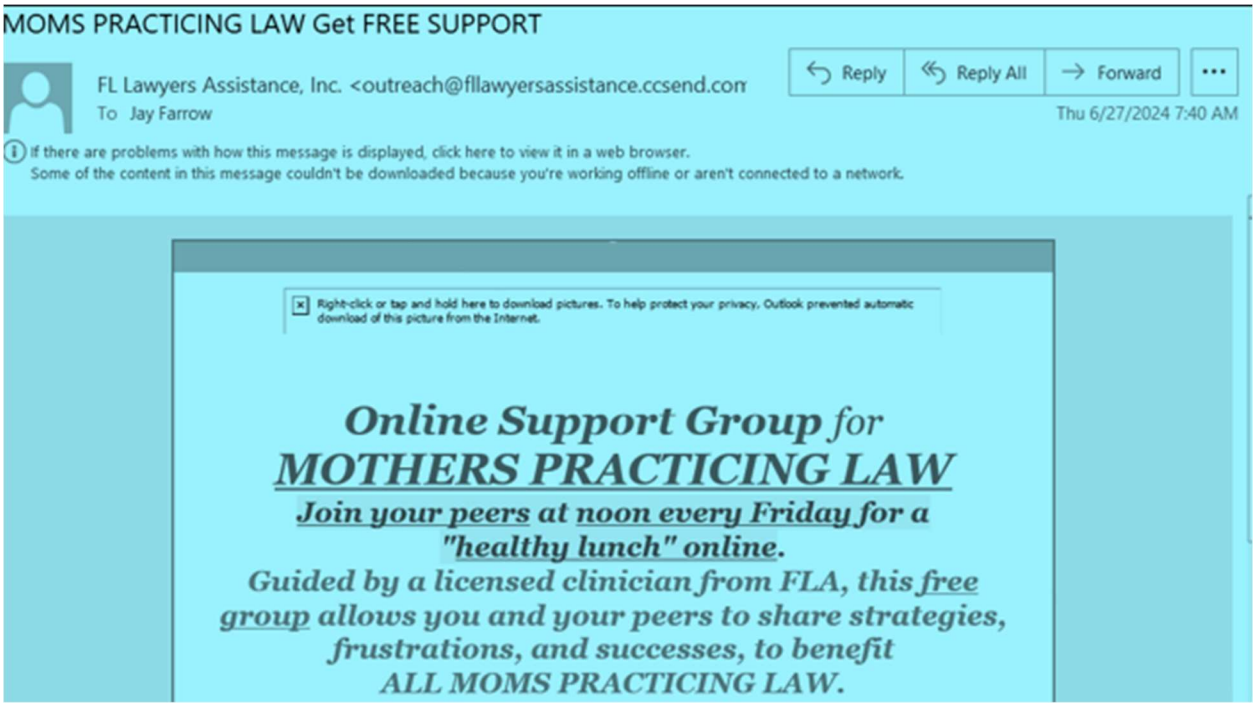
882. The Threat Actors used the exploitation of FLA's website domain to interfere with his communications with FLA, to steal confidential information from FLA's Network and employees with respect to Farrow, and the Threat Actors also stole confidential calendar entries on Farrow Law's Network which provided the names of other participants at the Fort Lauderdale Tuesday Meetings and the Threat Actors unlawfully recorded a least two meetings of FLA – which are highly confidential.

883. More specifically, from August through October 2024, Farrow attempted to send emails to at least three of FLA's key team administrators, and never received a response.

884. As well, the Threat Actor Defendants used spear phishing emails directed at Farrow using a purported domain belonging to FLA, however, that domain is not an official FLA domain

and was created by the Threat Actor Defendants for malicious purposes such as acting as a C2 Domain.

885. On June 27, 2024, the Threat Actor Defendants sent Farrow a spear phishing email purported from FLA, however it was not a legitimate FLF email.



886. Yet, on June 27 or 28, 2024, the Threat Actor Defendants had manipulated the photos in his phone which related to the HIPPA information in his FLA file within the Farrow Network, which he could no longer access due to his network status relating to that protected file was downgraded from administrator to employee.

Alleged Miami Herald Reporter Ben Wieder Informs Farrow has Farrow's FLA and Using it to Write an Article About him "Deserting" His Clients

887. On November 4, 2024, Farrow received a call from a purported journalist, Ben Wieder, from the "Washington, D.C. Bureau" of the Miami-Herald who, *inter alia,* claimed he had Farrow's FLA File.

888. However, FLA did not provide Wieder or anyone else Farrow's FLA file.

889. Wieder, in all events, purports to work for the Miami Herald, but he works, if at all for McClatchy, a large media company who owns numerous newspapers including the Miami Herald.

890. During this November 4, 2024 phone call, Wieder inquired about Farrow's medical history, but only as it pertained to the FLA program because, he 'had a copy of Farrow's FLA file' which he claimed was public record- yet FLA is a private corporation which works in tandem with the Florida Bar, however, does not have per se authority to turn over its files at they are protected by HIPPA.

891. More specifically, during their November 4, 2024 conversation, Wieder stated that he apparently read through Farrow's FLA agreements, that he had read through all the alleged 'new' Bar Complaints, and that he had spoken with 'most' of the clients who purportedly filed those Complaints.

892. During this conversation, Farrow informed Wieder that he and his wife were cooperating with an FBI investigation into the Threat Actor Defendants, and that, certain clients had been able to reach Farrow and each of them experienced substantial interference with their

cell phones and emails after making contact, with certain individual(s) having received threats of physical altercation.

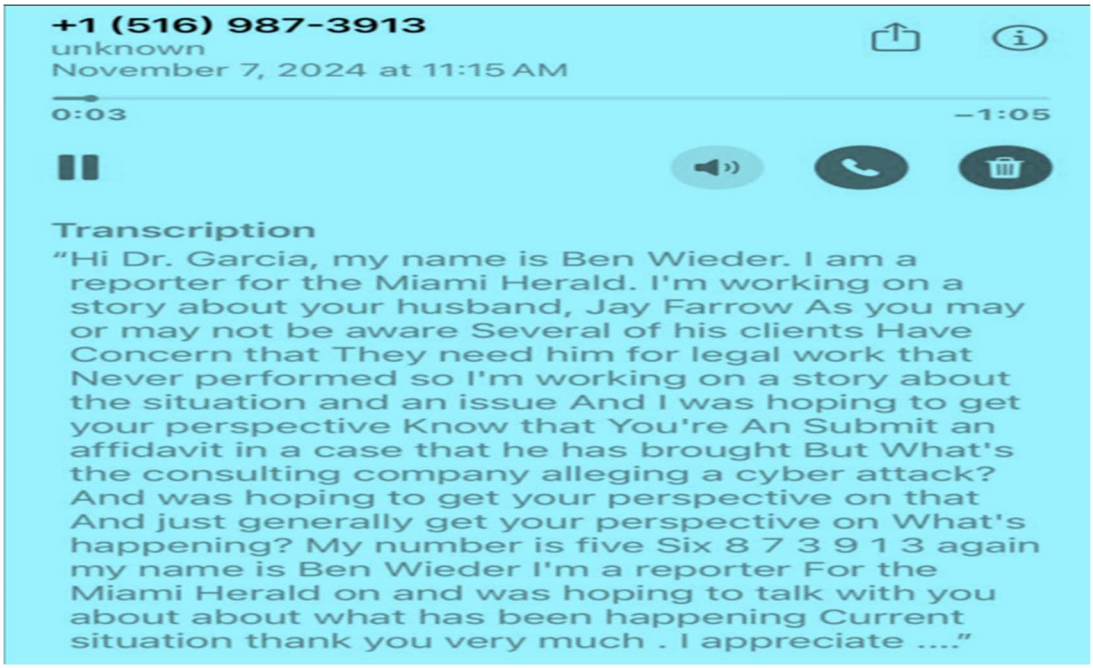
893. At the end of the call, Wieder asked what Farrow was doing at that moment on the afternoon of November 4, 2024, specifically about the purported Bar Complaints, and Farrow informed him that he had driven 10 hours and was at that moment pulling up to the Florida Bar to deliver materials, including written documents between Farrow and Special Agent Andrew Morton and Special Agent Ryan Schafer of the Miami Field Office of the FBI whom he had an emergency meeting with on November 2, 2024.

894. Farrow specifically informed Wieder as to how investigations revealed the unauthorized access into the Florida Bar Network, and, in detail, how the Threat Actor Defendants were using illegally procured login credentials of Florida Bar employees.

895. Farrow also informed Wieder of the breaches into FLA's network, and to his client's network and offer to meet Wieder to show him the evidence and communications with the FBI.

896. Wieder, in a text refused.

897. On November 7, 2024, Wieder called Dr. Doe and left as message on her voice mail while she was at a medical conference, which was sent to Dr. Doe in a translated voice to text message and stated:



898. Dr. Doe's cell phone number is highly protected, it is not provided on the University of Miami Miller School of Medicine where she is an assistant professor of medicine, nor on any website connected with Jackson Memorial Hospital or the Miami Transplant Institute.

899. Dr. Doe is on call one to two weeks each month, and even when not specifically on call, her number is akin to calling 911 as she takes the calls 24 hours a day when an organ is being offered to MIT for transplant.

900. Dr. Doe did not call Wieder back on November 7, 2024.

901. The information Wieder claim to be in possession of from FLA, came from the documents within the stole Farrow Law Firm JEO folder which was stolen by the Threat Actor Defendants on or about July 3, 2024.

902. Based upon Wieder's own statements on November 4, 2024, he had shared Farrow's FLA file with the purported clients which had filed Florida Bar Complaints against

Farrow since allegedly June through September 2024, and he claimed to have received those complaints allowing him to locate those clients from the Florida Bar, and specifically from an alleged Bar Counsel John Derek Womack and from Womack's Legal Secretary Christine Mitchell.

903. Wieder's identity, social media accounts and/or his login credentials were stolen by the Threat Actor Defendants, and used to prepare articles, publications and direct social engineering phone calls to obtain information from Farrow, Dr. Doe and Farrow's clients to be used for malicious purposes by the Threat Actor Defendants for purposes of achieving their ultimate goals.

904. In January 2024, Wieder call Dr. Doe at night stating: "are you ok Dr. [Doe]." Wieder indicated she had just called him, which was not true, and Wieder was calling from a different number that the number left on November 7, 2024.

905. Wieder purportedly texts her back asking for an interview, and he allegedly called her the next day, on or about January 20, 2025.

906. Wieder's call came at a time when Dr. Doe was on call and came from an area code in Long-Island, New York.

907. Upon information and belief, Wieder's call was for purposes of harassment and based upon Farrow's conversation with Wieder on November 4, 2024, he knew or should have known that Dr. Doe had been traumatized by random calls from individuals associated with the Threat Actor Defendants attempting to persist in causing her additional pain and suffering.

908. Wieder's call was not as a journalist, and upon information and belief, Wieder is a direct or indirect employee or agent of FTI Consulting.

INTERFERENCES WITH FARROW'S CLIENT(S) WORKING WITH FEDERAL LAW ENFORCEMENT AGENCIES AND MIAMI-DADE COURTMAP WEBSITE

909. On November 2, 2024, Farrow requested an emergency in person meeting with the two FBI Special Agents who were investigating he and his wife's cyber-complaint.

910. After going through protocol, Farrow disclosed to them he has client(s) working in certain roles with federal law enforcement, some of these individuals were working in active domestic field operations and that he had strong actionable information that their communication devices or the apps on those devices, had been compromised.

911. From November 8 through 10, 2024, Farrow's email was compromised, due to malware being uploaded through a seemingly legitimate application.

912. By November 10, 2024, Farrow had regained control over his email that he had been using for communicating with the FBI, the Florida Bar, and a few of the Clients he had been in contact with, and subsequently he proceeded to with collecting evidence, working with law enforcement and inching towards locating cyber-experts.

913. However, on November 11, 2024, this particular compromise of his email and other communications systems related to client(s) who were working with a federal agency in active domestic law enforcement operations, caused Farrow to file an Ex Parte Motion for Restraining Order on the exclusive basis that Farrow's communications systems with these person(s) presented a clear and present danger to them and those they work with in field operations.

914. However, when Farrow attempted to file this motion and upload it to the Miami-Dade Court Maps, the website appeared with an AI Chat, and unless Farrow entered a question in

the chat box, the CourtMap website would not allow for logging in Farrow's username and password.

915. Upon information and belief, the Threat Actor Defendants used DNS spoofing or IP spoofing to interfere with his ability to upload this ex parte emergency motion and other motions in the July 15 Circuit Court Case. Upon information and belief, this interference prevented the Court from receiving the November 11, 2024 emergency ex parte motion and the same was never ruled upon.

INTERFERENCES WITH FARROW LAW'S CLIENTS

February 2024 through July 2024

916. From February through July 2024, each of Farrow's communications with the clients of Farrow Law were infiltrated by utilizing one or more types of the Man-in-the Middle Cyber Attack.

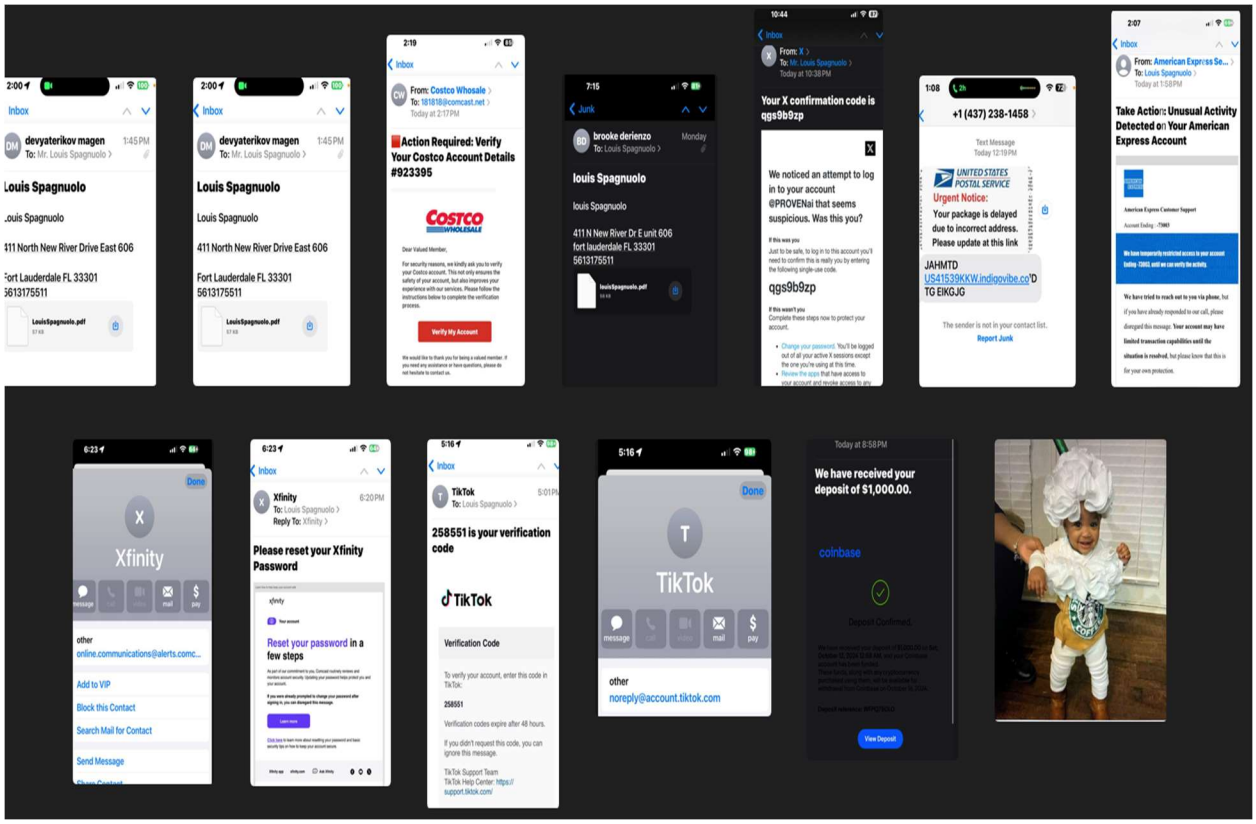
917. From April through July 2024, the Threat Actor Defendants sent and received and respondent to emails masquerading as Farrow, or a Farrow Law Staff member, or a client of Farrow Law, such that secure and authentic communications continue to be unsafe and impossible.

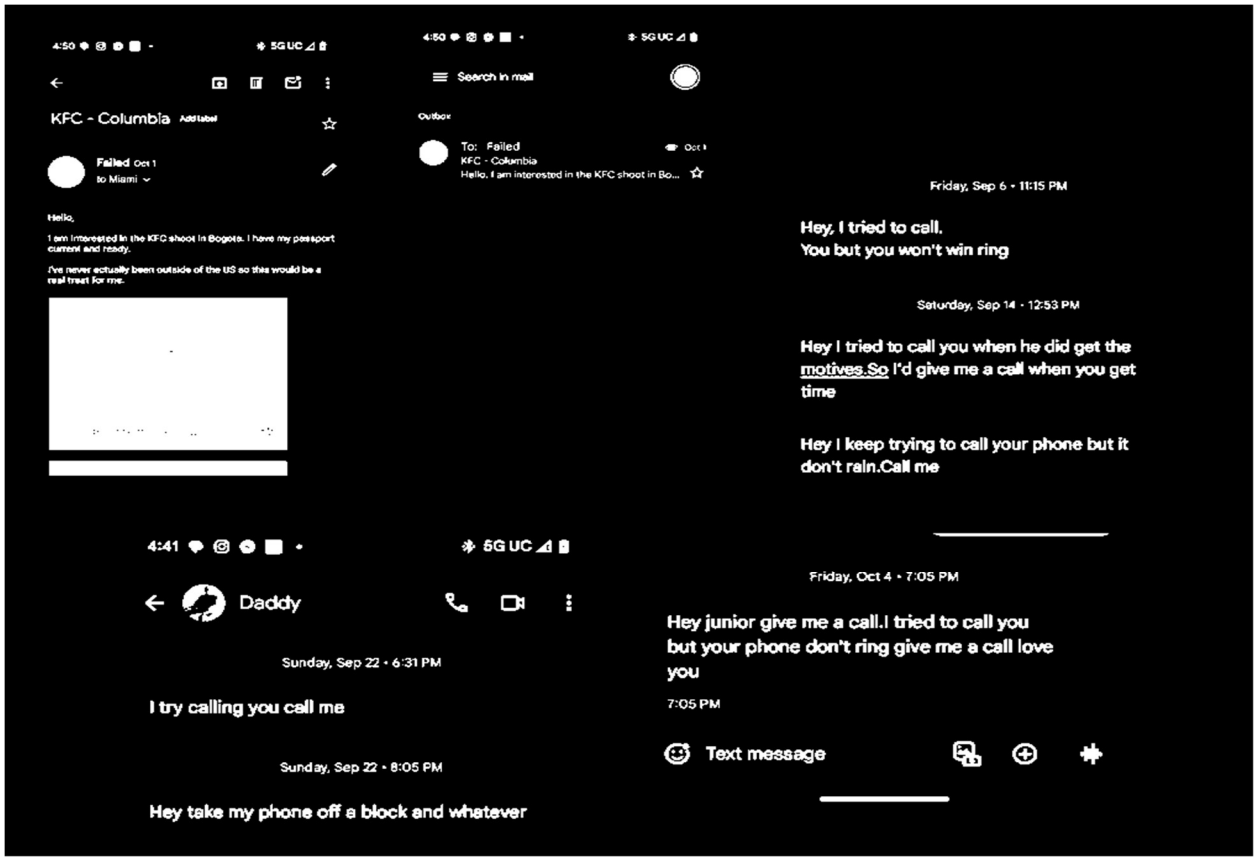
918. Since July 2024, Farrow has been in contact with certain clients.

919. Some of them reestablished contact with Farrow in late August 2024, and early October 2024.

920. Each of the clients who communicated with Farrow since July 15, 2024 has had their emails, personal cell phones and other devices compromised in nearly identical ways.

921. For example, the messages below were received by the individual clients who have been able to reestablish contact with Farrow for the period September 6 through October 10, and represent approximately 25% of all such messages received during that time which was immediately following the filing of the September 4, 2024 Corrected Amended Complaint and the service of that complaint and the September 30, 2024 Second Amended Emergency Motion on October 4, 2024 upon Heath Ritenour and John Ritenour.





922. From late August 2024, collectively, these individuals have been targeted over 100 times, with some of the messages directly threatening them with 'live' altercations.

Ben Wieder Attacks 5th Victim Using Online Platforms – Sitting Duck Attacks Reveal How Threat Actors Accomplish Stealing Identities and Creating Fictitious Back Stories

923. On Monday, November 13, 2024, Dr. Doe called Farrow from work to inform him that she had received a message on social media containing a link to a 'front page' article in the Miami Herald along with a threatening message.

924. Dr. Doe has since been approached by third parties and co-workers about this 'front page' article which has caused her extreme emotional distress.

925. In this Article, written by none other than Ben Wieder, of the Washington D.C. Bureau of the Miami Herald, and McClatchy, is entitled: “Clients say Miami lawyer disappeared, Florida Bar didn’t warn them of his past.”

926. Dr. Doe also reported that most of her coworkers at the hospital had received the article in their social media feeds.

927. Between November 13, 2024 and November 25, 2024, along with the article about Farrow, there were, in the aggregate, over 30 messages sent to Dr. Doe, Farrow’s clients, and Farrow, which collectively were purportedly written by several clients/former clients of Farrow Law, all use Wieder’s article or highly sophisticated spear phishing directed to interfere with Farrow and Doe’s relationships.

928. Representative examples of those spear phishing messages are:

929. More specifically, the individuals who received the social media messages with the Wieder links are colleagues, friends, family co-workers and or Farrow's clients.

930. Farrow and Doe allege that the Wieder article was not, in fact, written by Wieder and that the company Wieder works for, as he proports, is McClatchy, a large media company owning numerous newspapers around the United States, including the Miami Herald.

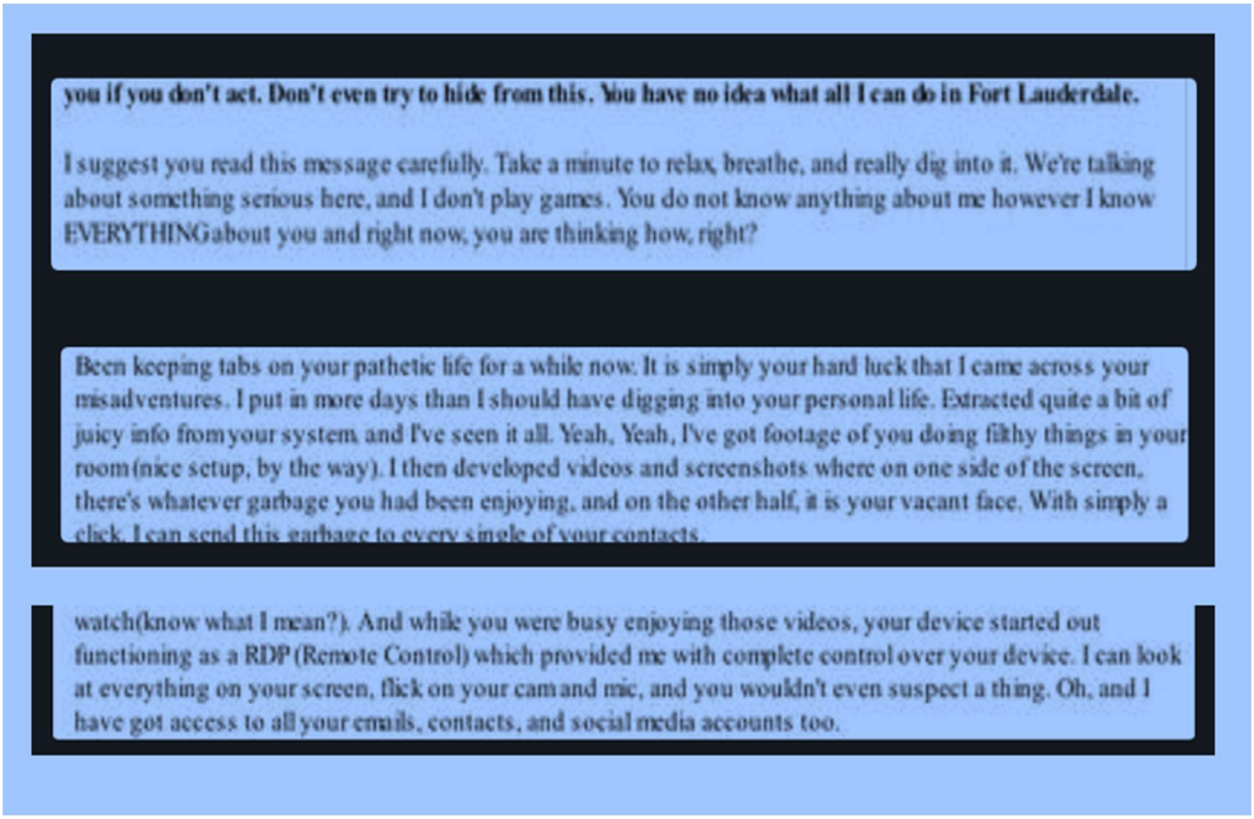
931. McClatchy is a client of FTI and one of its go-to media outlets for strategic communications campaigns.

932. On FTI's website, it states that it worked for McClatchy through its bankruptcy proceedings.

933. McClatchy has its own email address at FTI, mcclatchy@fticonsulting.com.

934. Upon information and belief, FTI's relationship to McClatchy as its go-to media outlet allowed the Threat Actor Defendants to engage in the social engineering campaigns related to Farrow, Judge Spryenski, Judge Stacey, Judge Recksiedler and Congressman Bean.

935. On about November 13, 2024, and again in early January 2025, one of the clients who had been in contact with Farrow since at least August, received an email which threatened visiting them at their home, listing their confidential number and stating that they intended to use information against them for extortion purposes.



XI. COMPROMISED ELECTRONIC DEVICES, EMAILS AND PROTECTED COMPUTERS

936. **March 2021 through Present** – the Threat Actor Defendants gained unauthorized access to Farrow and Dr. Jane Doe's Computers, Replacement Computers, an iPad, Cell Phones, Electronic Devices in their Residence Capable of Sending/Receiving Bluetooth connections and even two Motor Vehicles in which they installed Wi-Fi Hotspot Accounts.

937. Device and Email Hacking Table: The table below represents of some the devices and emails accounts which the Threat Actor Defendants gained unauthorized access to or substantially interfered with from March 2021 through present for purposes of blocking, delaying, severing or interfering with communications between Farrow, Farrow Law, Dr. Doe and their personal and business contacts.

Device Description	Date of Hack/Corruption(apx)	Infiltration Indicators
Lenovo Ideapad 5 Lab Top	March 2021 July 2021 November 2021	Installation of Unauthorized Applications, Repackaging of authorized applications, Unauthorized modification of network and locally saved folders and documents. Unauthorized users removed Farrow's administrator credentials, reducing to employee and denying access to client folders after approximately July 3, 2024.
Dell Inspiron Lab Top	December 2019	July 15, 2024 – administrator change from Farrow, new user changed local password to access screen. Computer completely inoperable.
HP Envy Touchsmart Notebook PC Lab	August 2, 2024	July 20-August 2, 2024,

Top Non-Farrow Law Personal Laptop		new users accounts, installation of unauthorized applications and finally new user changed local password to access screen. Computer Completely inoperable
4 New HP Lab Tops Purchased and Returned from June 2024 through July 31, 2024	June 28, 2024 July 3, 2024 July 7, 2024 August 1, 2024	Identical issue of hack during initial set up. Computers would only allow access as employee, and ultimately locked access to sign in screen
Samsung Galaxy 22+ Ultra Main Phone T-Mobile IMEI: Unknown	From at least June 15, 2024 through August 2024	Once Charged, Bluetooth could not be turned off and applications installed without authorization, location of perpetrator Washington, D.C.
Samsung Galaxy Model Unknown MetroPCS IMEI: Unknown	July 15, 2024	Brand new. 20 minutes after purchase, unauthorized apps installed and phone immediately showed signs of cloning, and ultimately appeared to mirror another phone, phishing text messages and receipt of several AI voice calls, and photos removed that were taken of evidence of hack without authorization.
Nokia Flip Phone IMEI: *****00878 Best Buy	July 21, 2024	Brand New. Worked for 3 days before same issues of not being able to call numbers previously called, especially if they were in contacts on Farrow's main phone. Reports of individuals attempting to call Farrow but went to voicemail. Then phishing text after calls made to phone numbers on Farrow's main phone. Phone locked by unauthorized individual and completely dysfunctional.
SCHOK Flip Phone MetroPCS IMEI: *****478002	July 25, 2024	Brand New. Open phone. Purchased in cash no receipt emailed giving phone data. Phone worked for 3 hours before phishing text after calls made to phone numbers on Farrow's main phone. Phone locked by unauthorized individual and completely dysfunctional.
MOXEE Mobile HotSpot Best Buy	July 2, 2024	Brand New. Hot Spot. Worked for 5 days, but corrupted iPad and MAC computers and

IMEI: *******830890		password changed without authorization. Rendered nonfunctional.
2022 Motor Vehicle Hot Spot Version IMEI: Unknown	July 14, 2024	Unauthorized installation. Could not be disabled as AT&T account was never purchased or set up by Farrow, but it was set up under JLF***5@yahoo.com by unknown individual. Feature taken out of vehicle for $800.00 Pines Lincoln.
2024 Motor Vehicle Hot Spot At&t IMEI: Unknown	August 2, 2024	Unauthorized installation. Appears to have stopped by itself. Provided connection into Farrow and Dr. Jane Does phones unknowingly.
Apple iPhone IMEI: Confidential Service: Confidential	September 20, 2024	Older model. Worked for a few weeks, now experiencing double text alerts, phishing alerts from AMBER, Applications cause phone to crash and restart.
Samsung Moment Smart Phone MEID *******99880	July 9, 2024	Older model phone. Applications installed within an hour of charge and simply rendered dysfunctional, never to make a single call.
BLU Flex B330V Smart Cellphone IMEI: *******unknown CVS Pharmacy	June 30, 2024	Brand New. Phone set up on home Wi-Fi. Locked out of start screen within 10 minutes. Phone could not be restarted or factory reset.
Jay@farrowlawfirm.com	August 2022 or June 2024	June 22, 2024 emails found on personal email @yahoo.com which was from jay@farrowlawfirm.com to @yahoo.com
J*****5@yahoo.com	September 2023 through present	Discovered January 2025. Indicator of compromise are multiple June 25, 2024 emails from this @yahoo.com address send to jay@farrowlawfirm.com
J*****5@gmail.com	May or June 2024	Discovered January 2025. Indicator of compromise are multiple June 25, 2024 emails from this @gmail.com address send to jay@farrowlawfirm.com
Jay.*****.f****w@outlook.com	July 2024	Locked out of newly created Microsoft Account within 24 hours

fre***.f***w@gmail.com	July 2024	Unknown user changed password
J******a@gmail.com	July 2024	Purchase of HP computer and Microsoft Office Software Package on July 7, 2024. Receipt containing Microsoft Software Key and ID number of computer emailed to Dr. Doe's personal Gmail account and 15 minutes later, HP computer boots and is locked by password. Hacked @gmail account used to steal data to gain unauthorized access to new computer
J**7****@outlook.com	July 2024	Locked out of newly created Microsoft Account within 24 hours
F******s@outlook.com	July 2024	Locked out of newly created Microsoft Account within 24 hours
Fa*****r@gmail.com	July 2024	Unknown user changed password
J**********45@gmail.com	July 2024	Unknown user changed password
J*********@proton.me	July 2024	Unknown user installed malware allowing for login credentials to be stolen. Email account lost
S********@farrowlawfirm.com	August 2022 and/or February 2024	Paralegal email account. Signature block changes multiple times, emails sent not written by paralegal. Change in the email name. Emails to unknown third parties April through July 2024
J*******@farrowlawfirm.com	August 2022 through July August 2024	Signature block changes multiple times, emails sent not written by this user. Change in the email name. Emails to unknown third parties April through July 2024
Farrow Law Electronic State Filing	June 2024	Inability to pay court fees, rejections of multiple attempts to file documents, filed documents cut off halfway and need refiling
Farrow Law PACER	June 2024	Paralegal complains of inability to access account due to other users using it.
P******@aol.com	July 2024	Receipt of unauthorized emails from this @aol.com address to

		jay@farrowlawfirm.com
1*****8@comcast.net	July 2024	Email from Threat Actor Defendants specifically stating they hacked email and providing corrected login credentials
M******@gmail.com	July 2024	Locked out by unauthorized user changing password
R*****@farrowlawfirm.com	May or June 2024	Signature block changes multiple times, emails sent not written by this user. Change in the email name. Emails to unknown third parties April through July 2024
jxxxxxxxw@proton.me	August through December 2024	Password changed by unauthorized user. Access restored through alternative method
Jxx.F……@flcounselfirm.com	October 2024	Locked out of account through change of password by unauthorized user

XII. CONDITIONS PRECEDENT

938. Plaintiff has retained undersigned counsel to prosecute this action and has agreed to pay a reasonable attorney's fee and costs.

939. All conditions precedent has been accomplished, waived or satisfied prior to the institution of this action.

940. JURY TRIAL: Plaintiff demands a trial by jury on all claims so trailable.

COUNT I - CIVIL VIOLATION OF FEDERAL RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT ("CIVIL RICO") PURSUANT TO 18 U.S.C. § 1961, *et. seq.* (Plaintiffs v. the Threat Actor Defendants)

941. Plaintiffs reallege Paragraph Numbers 1 through 940 as if fully and completely set forth herein.

942. As to Count I, Plaintiffs allege an action for civil remedies pursuant to the Federal Racketeer Influenced and Corrupt Organizations Act **18 U.S.C. § 1961*, et. seq.* as against Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, Steven Gunby, FTI Consulting, Joe Taylor, Joe Taylor Restoration, Inc., and the Carrier Defendants.**

943. This is an action for civil violations of the Federal Racketeer Influenced and Corrupt Organizations Act ("Federal Civil RICO") pursuant to 18 U.S.C. § 1962(c) and §1964(c). which provides.

944. Pursuant to 18 U.S.C. § 1962(c):

> It shall be unlawful for "any person employed by or associated with an enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs for a pattern of racketeering activity or collection of unlawful debt.

945. Pursuant to 18 U.S.C. § 1962(d), it shall be unlawful to conspire to violate any of the RICO substantive provisions, including section 1962(c).

946. 18 U.S.C. § 1964(c), creates a private right of action for any person injured in his business or property by reason of violation of § 1962 and provides for threefold the damages sustained including reasonable attorney fees.

947. **Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, Steven Gunby, FTI Consulting, Joe Taylor, Joe Taylor Restoration, Inc., and the Carrier Defendants** were and are members and associates of a criminal organization, hereinafter, the RITENOUR APT ORGANIZATION ("RAPTOR"), including its leadership, members, and associates, constituted an "enterprise," as defined by Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact, although not a legal entity ("RAPTOR ENTERPRISE").

948. The RAPTOR ENTERPRISE constituted and constitutes an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the enterprise.

949. The RAPTOR ENTERPRISE was in engaged in, and its activities affected, interstate and/or foreign commerce.

Purposes of the Enterprise

950. The purposes of the RAPTOR ENTERPRISE, included, but not limited to, the following:

A. To achieve all, substantially all or at least one of the Ultimate Goals as defined herein;

B. To install malware on protected computers, to damage such computers, to gain unauthorized access to those and other protected computers;

C. To obtain information and data of value that belonged to the owners and/or users of the targeted protected computers;

D. To enrich the leaders, members, and associates of the enterprise;

E. To provide financial and/or other pecuniary and/or some other benefit to the leaders, members and associates of the enterprise by eliminating the prosecution of civil claims, and/or mitigating the consequences of the prosecution of civil claims against them;

F. To promote and enhance the reputation and standing of the leaders, members and associates of the enterprise;

G. To preserve and protect the profits of the leaders, members and associates of the enterprise;

H. To deny, or substantially interfere with, Plaintiffs access to courts, by and through unauthorized access to protected computers, and/or through unauthorized access to Florida's eFiling Authority's Network and protected computers, and/or the Miami-Dade County CourtMap website;

I. To protect the enterprise and/or its leaders, member, and associates from detection, apprehension, and prosecution by law enforcement, and from further prosecution related to their acts and conduct directed at causing Plaintiffs damages and harm;

J. To protect ill-gotten profits through the manipulation of judicial proceedings which resulted perpetual profiteering through avoiding the civil consequences illegal conduct.

Means and Methods of the RAPTOR ENTERPRISE – the Threat Actor Defendants Activities and Conduct Consisted of a Pattern of Racketeering Activity

951. A 'pattern of racketeering activity' requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity." 18 U.S.C. § 1961(5).

Means and Methods – Predicate Acts

952. The means, methods, conduct and activities by which Defendants Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC. Steven Gunby, FTI Consulting, Inc., Joe Taylor and Joe Taylor Restoration, Inc., and the Carrier Defendants, and other members and associates of the RAPTOR ENTERPRISE conducted and participated in the conduct of the affairs of the enterprise which are re-alleged herein.

953. In summary, the means and methods involved the commission of specific 'predicate acts', which occurred from at least December 2020 through present, which included violations of the CCFA and wire fraud.

Violations of the CCFA Generally

954. Each computer referenced in this lawsuit is a protected computer pursuant to 18 U.S.C. 1030(e)(2)(B), whether owned by Farrow, Farrow Law or Dr. Doe, or any other person or entity.

955. "Unlawful access", pursuant to the CCFA, is defined as wrongful access. As such, each unauthorized and/or unlawful access into a protected computer is sufficient to establish culpability, without any other elements of common law fraud being pled or proved.

956. The RICO Defendants' conduct and activities were not discovered by Farrow and/or Farrow Law until approximately June 2024, and could have been discovered through reasonable inquiry until June 2024.

Violations of CCFA - 18 U.S.C. § 1030(a)(2)(C)

957. From at least December 2020, the RICO Defendants intentionally, knowingly and/or under circumstances in which they should have known, caused and/or directed others to access protected computers without authorization and thereby obtained information from the protected computer in violation of 18 U.S.C. § 1030(a)(2)(C);

958. From at least December 2020, the RICO Defendants intentionally, knowingly and/or under circumstances in which they should have known and/or constructively known, caused and/or directed others to exceed authorized access to protected computers used in interstate

commerce and thereby obtained information from the protected computer in violation of 18 U.S.C. § 1030(a)(2)(C);

959. Use of Tactics, Techniques and Protocols – the Leaders, Members and Associates of the RAPTOR ORGANIZATION, used the sequence framework structures of an APT, target selection, intelligence gathering, initial access, foothold and lateral foothold fortifications, extraction of information, and covering tracks sabotaging protected computers the use of an organized, sophisticated, and persistent cyber-attack activities over the course of five years which followed the flow of, in whole, or in part, and/or mimicked the sequence framework structures of an APT for purposes of accomplishing the purposes of the RAPTOR ENTERPRISE and to achieve the Ultimate Goals of the RICO Defendants, and in particular those activities of an APT which involve a violation of, at the very least, 18 U.S.C. § 1030(a)(2)(C) relating to the unauthorized access into protected computers used in interstate commerce, and thereby obtaining information.

Violations of CCFA -18 U.S.C. §1030(a)(4)

960. On or about January 2021, February 22, March 2, August 10 of 2021, August 16, 2022, August 27, 2023, September 1 and 11, 2023, April 12, 2024, June 5, 2024 and June 12, 2024, the RICO Defendants, in violation of 18 U.S.C. §1030(a)(4) caused, for purposes of achieving their Ultimate Goals, and/or for other benefits, the transmission of a program, information, code, or command to be sent Farrow and Farrow Law's protected computers in furtherance of criminal violation of 18 U.S.C. § 1343, wire fraud, and as a result of such conduct, the RICO Defendants intentionally caused damage, without authorization, to protected computers.

961. More specifically, the RICO Defendants, on the dates referenced above and herein did knowing cause the transmission of a program, information, code or command through pdfs

and links under the pretense of legitimate court related activities, and for their part, Farrow and Farrow Law, reasonably and/or justifiably relied upon the RICO Defendants direct, indirect and/or implied representations, which caused unauthorized access to protected computers in excess of $5,000 in any one year period, in violation of 18 U.S.C. § 1030(a)(4).

Violations of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)

962. From January 2023 through present, the RICO Defendants intentionally, knowingly and/or under circumstances in which they should have known, and/or constructively knew, caused and/or directed others to cause the transmission of a program, information, code, and command, and as result of such conduct, intentionally caused, or attempted to cause, damage without authorization to protected computers, and caused, or attempted to cause, more than $5,000 in loss in one year, and caused, or attempted to cause, damage affecting 1 or more protected computers during a one year period, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B).

963. Whether or not with the intent to defraud, as defined with Section 1030 as being unlawful access as distinct from common law fraud, can be established with respect to the leaders, members and/or associates activities and conduct related to, or directed to, gain unauthorized access to protected computers, that the RICO Defendants, directly or indirectly, accomplished unauthorized access to protected computers which are used in interstate commerce and thereby they obtained information, is, in and of itself, a predicate act which was and is related to each other instance wherein the RICO Defendants achieved unauthorized access into a protected computer used in interstate commerce, and thereby obtaining information throughout the course of at least December 2019 to present, as in each instance, as alleged herein throughout the general allegations,

the unauthorized access into a protected computer was in furtherance of the common purposes and achievement of the Ultimate Goals of the RICO Defendants.

AI Voice Calls – Wire Fraud 18 U.S.C. § 1343

964. The social engineering techniques included 'spoofing' calls where the fraudsters use well-researched outline scripts and initiate a telephone call using an AI technology app masking their voice and using the app to convert the same such that they sound identical to the voice of a family member, friend, colleague, or other individuals.

965. More specifically, between May 28, 2024 and January 2025, Farrow and Dr. Jane Doe collectively received over 30 AI Voice Calls which were caused directly and/or indirectly by the Threat Actor Defendants, over interstate wires, all in violation of 18 U.S.C. § 1343.

966. More specifically, as it relates to Count I, the specific AI Voice Spoofing Calls, using AI Voice Cloning and/or Mirroring Applications were made, directly and/or indirectly, on July 3, 9, 14, 19 and 24, August 21, and September 17, 2024 which imitated, impersonated and used the substantial likeness of, *inter alia:*

967. **FORMER CLIENT 1**: This call was made for purposes of harassment, and to intimidate Farrow for purposes of causing him to believe that this person would cause or attempt to cause him physical harm if he 'didn't quit chasing [Defendant IOA, Inc.] and focus on [other Farrow Law business issues]". During these specific AI Voice Calls, this individual had information regarding Farrow Law, Farrow and Dr. Doe which had been stored within Farrow Law's Administrative folder, as well as, information from emails sent to Farrow Law from its staff at the end of June and beginning of July 2024. This individual also used information related to Farrow stored in Farrow Law Admin File which had been named in part "JEO", which related to

the firm's financial records, and Farrow's health records which had not been shared with any of Farrow Law's staff as they pertained to confidential medical information related to health choices which were being discussed between Farrow and Dr. Doe in March through June 2024.

968. **FLORIDA LAWYER'S ASSISTANCE ADMINISTRATOR**: On or about July 24, 2024, Dr. Doe received a phone call from an individual impersonating, mimicking and/or using AI technology to clone the voice of an FLF Administrator, who introduced themselves as FLA PERSON 1. This call was made for purposes of harassing Dr. Doe and causing her emotional distress and who, under false pretenses, stated that an alleged Bar Counsel, 'John Derek Womack' had called FLA PERSON 1 to locate a new phone number for Farrow who at the time no longer had his previous cell phone.

969. **OTHER AL VOICE CALLS**: Other calls, such as on July 19, 2024 to Dr. Doe's phone allegedly by Farrow Law clients, used racial slurs and invitations for physical altercations to intimidate Dr. Doe as retaliation for the filings of the 2024 Family Circuit Case and the July 19, 2024 Domestic Circuit Case which was filed hours prior to this call on the same date.

970. In each instance, the fraudulent AI Voice Call was designed to fraudulently masquerade using voices imprints of others, and through such false and fraudulent pretenses, extract information from Farrow and/or Dr. Doe, specifically, as to Farrow, Dr. Jane Doe, and/or Infant Doe's whereabouts, future work schedules, school schedule, general questions about pending legal proceedings, healthcare and financial issues.

971. Additionally, with respect to AI Voice Calls from alleged employees of the Florida Bar, such as John Derek Womack, in late August and early September 2024, these calls were designed to create situational events which were intended to and did cause substantial interferences

with Farrow and/or Dr. Doe's resources, and/or to cause Farrow and/or Dr. Doe substantial emotional distress.

Carrier Defendants' Wire Fraud 18 U.S.C. § 1343

963. Each Carrier Defendant, did knowingly, or under circumstances that they should have known, transmit over interstate wires, all in violation of 18 U.S.C. § 1343, in at least two interstate wires within 10 years prior to the filing of this Verified Complaint, which directly or indirectly, falsely represented to the FDFS that it had (1) independently conducted an independent investigation into the character, trustworthiness and compliance with the FIC of Heath Ritenour, John Ritenour, and/or IOA, Inc., and/or (2) that after conducting such an independent investigation, that Heath Ritenour, John Ritenour and/or IOA, Inc. were of such character, trustworthiness and/or that they were conducting themselves in accordance with their transaction of insurance in Florida in compliance with the FIC, under circumstances which they knew, or should have known, that the same was false and/or substantially false.

964. In each transmission of false certification to the FDFS, they intended that the FDFS rely upon such information, and the FDFS did reasonably rely upon the Carrier Defendants respective statements, triggering Heath Ritenour, John Ritenour and IOA, Inc.'s reappointment and consequently, their privilege to transact insurance in Florida as the agents of the Carrier Defendants.

965. The Carrier Defendants intended to make false certifications and/or statements to the FDFS for financial benefits related to the insurance policies these appointed agents directed to each respective Carrier Defendant from 2014 through present, and/or the Carrier Defendants intended to make false statements over interstate wires to the FDFS for purposes of other indirect

financial benefits, such as to avoid the consequences of disclosing the reasons for which the respective Carrier Defendant's investigation did not support reappointment which would have revealed that they had issued, for example, previously false statements to the FDFS with respect to these appointees.

966. Each of these statements and certifications made to the FDFS by a Carrier Defendant was in furtherance of the schemes to procure insurance premiums through illegal and/or deceptive practices from Heath Ritenour, John Ritenour and IOA, Inc.

967. In each of these statements, more particularly, each Carrier Defendant knew or should have known, that Heath Ritenour, John Ritenour and IOA, Inc. and FTI, were engaged in activities which were directed at Plaintiffs, for purposes of achieving the Ultimate Goals and/or the purposes of the RAPTOR ORGANIZATION, which were and are, criminally proscribed pursuant to Title 18 of the United States Code Section 1030 *et seq*., *inter alia,* attempt to, and achieving unauthorized access into protected computers, used in interstate commerce, and thereby obtaining information, in violation of 18 U.S.C. 1030, and that such conduct was disqualative of each Carrier Defendants' certification that Heath Ritenour, John Ritenour and/or IOA, Inc., should be or could be reappointed and thereby licensed to transact insurance in Florida.

Role of the RICO Defendants

968. Leaders, members and associates of the RAPTOR ORGANIZATION, had defined roles in the enterprise.

969. At all times material hereto, the RICO Defendants and other persons, known and unknown, participated in the operation of the management of the enterprise as follows.

970. Leadership - Defendant Heath Ritenour, Defendant John Ritenour, Defendant Steven Gunby created the RAPTOR ORGANIZATION, and they have served as its leaders, with Heath Ritenour serving as the leader of the managers and operators of the criminal organization, who, collectively, controlled the destiny of the enterprise.

971. Heath Ritenour and John Ritenour had ultimate control over the RAPTOR ORGANIZATION, through approximately March 2024, when Defendants Gunby and FTI joined them as leaders with ultimate control over the enterprise, including its membership.

972. Joe Taylor and JTR, Inc. had leadership roles in the RAPTOR ORGANIZATION, and had authority to direct and control some of the managers and/or operators of the criminal organization, however, he did not have, inherent ultimate authority, that is to say, having the last call as to the direction and final destiny of the enterprise.

973. Public Media and Relations – McClatchy, Wieder and others were responsible for certain social engineering campaigns, and the RAPTOR ORGANIZATION'S media publications.

974. Each RICO Defendant conducted the affairs of the Association in Fact Enterprise or acted at the direction of Heath Ritenour, John Ritenour, Steven Gunby and/or Joe Taylor, FTI and/or JTR in the conduct of the affairs of the Enterprise.

975. The RAPTOR Enterprise is an ongoing organization which engages in, and whose activities affect interstate commerce.

976. The Enterprise had longevity, over 5 years, sufficient to permit each of the RICO Defendants to pursue the Enterprise's purpose.

Function Together as Continuing Unit

977. At all times relevant hereto, from at least December 2019 through present, the leaders, members and associates of the RAPTOR ORGANIZATION, functioned together as a continuous unit, with common purposes, alleged herein.

978. Each participant in the RICO Enterprise had systematic linkage to each other through corporate ties, contractual relationships, employment, financial ties and continuing coordination of activities.

979. Each RICO Defendant conducted the affairs of the Enterprise or acted at the direction of its Leaders, and/or other members, and/or associates or the RAPTOR ORGANIZATION, in the conduct of the affairs of the Enterprise.

980. From at least December 2019 through present, each leader, member and/or associate of the RAPTOR ORGANIZATION, agreed to commit at least two predicate acts within 5 years of the Carrier Defendants

Operation and Management/Distinctness

981. As described herein, the RICO Defendants participated in the leadership, management and/or operation of the enterprise by directing its affairs as described herein.

982. While the RICO Defendants participated in –and are members of– the enterprise, they have a separate existence from the enterprise, and are different than the Enterprise which they direct.

983. The Association in Fact Enterprise has existed for more than five years and continues to exist and operate.

Continuity Plus Relationship

984. Plaintiffs allege that the course of conduct engaged in by the RICO Defendants satisfy both "continuity" and "relationship" of the racketeering activity, thereby constituting a pattern of racketeering activity, as that term is defined in 18 U.S.C. § 1961(5).

985. Plaintiffs can show the relatedness prong because the predicate acts have the "similar purposes, results, participants, or methods of commission or are related to the affairs of the Enterprise."

986. All predicate acts had the same purpose of achieving the Ultimate Goals of the Threat Actor Defendants in and through the execution of an operation that was planned, executed and maintain identical to, substantially similar to or patterned, tailored, designed or architected in part based to follow some or all the sequence framework structures of an Advanced Persistent Threat, or APT, as that term is defined by NCIA and FBI.

987. The continuity of the pattern of racketeering activity constitutes closed-ended continuity as it occurred over a substantial period of time, i.e., from approximately June 2019 through present, and involves, as described, multiple schemes and multiple victims as alleged hereinabove.

988. Plaintiffs allege that the pattern of racketeering activity is shown by the threat of open-ended continued activity as the RICO Defendants continue to operate the RAPTOR ORGANIZATION, and the Schemes to interfere with Judicial Proceedings, Farrow Law clients, Farrow's law license and with respect to the fraudulent use of media outlets to damage Farrow and Dr. Doe.

989. Thus, engaging in the pattern of racketeering as set forth herein is the way Defendants regularly conduct the operations of the RAPTOR ORGANIZATION, and their predicate acts threaten future criminal conduct.

The Racketeering Violation

990. From approximately December 2019, and continuing up through the date of the filing of this Complaint, the RICO Defendants –each of whom are persons associated with or employed by the RAPTOR ORGANIZATION, an enterprise,– did knowingly and unlawfully conduct or participate, directly or indirectly, in the Association in Fact Enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(5) (defining "pattern") and 18 U.S.C. § 1961(1) (defining "racketeering activity"), all in violation of 18 U.S.C. § 1962 ("Prohibited Activities").

992. Each of the RICO Defendants have engaged in a pattern of racketeering activity by committing at least two acts of racketeering activity after the effective date of the statute, and also within ten (10) years after a prior incident of racketeering conduct.

WHEREFORE, Plaintiff demands judgment as to Count I against the **RICO Defendants** for compensatory and treble damages, pre- and post-judgment interest, attorneys' fees and costs incurred in bringing this action and for such other relief as this Honorable Court deems just and proper.

COUNT II – CIVIL RICO CONSPIRACY – CIVIL VIOLATION OF RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT ("CIVIL RICO") PURSUANT TO 18 U.S.C. § 1962 (CONSPIRACY TO COMMIT PROHIBITED ACTIVITIES
(Plaintiffs v. Against the RICO Defendants)

993. Plaintiffs reallege -each of the allegations contained in Paragraphs 1 through 992 as if set forth herein at length.

The Conspiracy

994. Plaintiff alleges that commencing in February 2014, and continuing until the present time, the RICO Defendants described above, conspired to violate 18 U.S.C. § 1962(c), all in violation of Fla. Stat. § 18 U.S.C. § 1962(d).

995. Each Defendant agreed that a conspirator would conduct or participate in the affairs of the Enterprise through a pattern of racketeering, consisting of the predicate activity as more fully described in Count I.

996. Plaintiff alleges that the conspiratorial objective of that mutual agreement was intended to obtain Plaintiff's interests in business and/or property, and that such conspiratorial conduct violates 18 U.S.C. § 1962(d), i.e., to conspire or endeavor to violate any of the provisions of 18 U.S.C. § 1962(c).

997. Each RICO Conspiracy defendant intended to further the schemes to defraud, which as described in Count I were completed and satisfied by at least one substantive individual Defendant.

998. As demonstrated in detail above, the RICO Defendants have engaged in numerous predicate racketeering acts in furtherance of the conspiracy as alleged in Count I.

999. The nature of the above-described acts, material misrepresentations, and omissions in furtherance of the conspiracy give rise to an inference that each RICO conspiracy Defendant not only agreed to the objective of conspiring to violate 18 U.S.C. § 1962(c), but they were aware that their ongoing conduct and activities were and are part of an overall pattern of racketeering activity.

1000. As a direct and proximate result of the RICO conspiracy Defendants' agreement that conspirators would violate 18 U.S.C. § 1962(c), Plaintiffs, and others similarly situated, has been and is continuing, directly and proximately, to be injured in their business or property as set forth more fully above.

WHERFORE, Plaintiffs demands entry of judgment against RICO Conspiracy Defendants as to Count II and seeks an award of compensatory and treble damages, for attorneys' fees costs, and for such other further relief this Court deems just and proper.

COUNT III – PRIVATE RIGHT OF ACTION
VIOLATION OF 18 U.S.C. § 1030(g)
(Farrow Law, Farrow and Dr. Jane Doe Against Threat Actor Defendants)

1001. Plaintiffs reallege repeats and realleges Paragraphs 1 through 940 as if set forth herein.

1002. This is an action for civil damages, temporary and permanent injunctive relief pursuant to the Computer Fraud and Abuse Act, and specifically, 18 U.S.C. § 1030(c)(4)(i)(I) and (g).

1003. The Theat Actor Defendants caused authorized access to protected computers belonging to Farrow Law as those terms are defined in 18 U.S.C. §(e)(1) and (2).

1004. These protected computers are used in interstate commerce.

1005. The threat actors did thereby obtain information from the protected computers belonging to Farrow, Farrow Law, Dr. Jane Doe and/or other protected computers as alleged herein.

1006. The Threat Actor Defendants knew, or should have known, and/or constructively knew, that their actions and conduct would result in the authorized access into protected computers.

1007. The Threat Act Defendants conduct and activities caused more than $5,000 in damages to Farrow in any one year, and such damages are related to the damages to the protected computers and/or the data stored therein.

1008. The Threat Act Defendants conduct and activities caused more than $5,000 in damages to Farrow Law in any one year, and such damages are related to the damages to the protected computers and/or the data stored therein.

1009. The Threat Act Defendants conduct and activities caused more than $5,000 in damages to Dr. Doe in any one year, and such damages are related to the damages to the protected computers and/or the data stored therein.

1010. Plaintiffs Farrow, Farrow Law and Dr. Jane Doe either are filing this action within two years of the conduct and activities giving rise to their claims, or they did not discover the activities, conduct and/or the damages therefrom until a time which is within two years of the filing of this lawsuit.

1011. Pursuant to the Threat Actor Defendants' conduct, Farrow has suffered damages in excess of $5,000 in any one year, and unauthorized access to at least one of its protected computers has occurred in each year.

1012. Pursuant to the Threat Actor Defendants' conduct, Farrow Law has suffered damages in excess of $5,000 in any one year, and unauthorized access to at least one of its protected computers has occurred in each year.

1013. Pursuant to the Threat Actor Defendants' conduct, Dr. Doe has suffered damages in excess of $5,000 in any one year, and unauthorized access to at least one of its protected computers has occurred in each year.

1014. The Threat Actor Defendants unauthorized access into Farrow Law's computer, which it now uses, was compromised in or about August 2024, after being purchased on or about July 15, 2024.

1015. Based upon their conduct and activities, which have occurred before and after the effective closure of Farrow Law on or about July 10, 2024, which were and are directed to gain further unauthorized access to any of Farrow, Farrow Law and or Dr. Doe's protected computers which are used in interstate commerce, for purposes of obtaining confidential information, and the evidence of activities directed at not only gaining unauthorized access to the protected computers, but to cause them damage, Farrow Law has no adequate law, and it continues to suffer irreparable harm to the extent that its only remaining functional protected computer is and remains a target of the Threat Actor Defendants pursuit of all or substantially of their Ultimate Goals as defined herein.

WHEREFORE, Plaintiff Farrow Law demands as to Count I, pursuant to 18 U.S.C. 1030(g): (1) an emergency ex parte injunction against Defendants Heath Ritenour, John Ritenour, IOA, Inc., IOA, LLC, their officers, directors and/or employees, and as to Steven Gunby and FTI Consulting, Inc., its officers, directors, employees, or contractors, from attempting to, or gaining unauthorized access to Farrow Law's protected computers; (2) a temporary injunction; (3) a permanent injunction prohibiting these Defendants, or any entity or person under their dominion or acting at their direction, from attempting to or gaining unauthorized access to any of Farrow Law's protected computers, used in interstate commerce; and (4) an award of damages, costs and attorney's fees for having to file and prosecute this action against these Defendants.

COUNT IV
NEGLIGENCE
(Plaintiffs v. the Law Firm Defendants)

1116. Farrow and Farrow Law repeats and realleges Paragraphs 1 through 940 as if set forth herein.

1117. At all times material hereto, the Law Firm Defendants owed a non-delegable duty of reasonable care in the investigation, inspection, oversight of their computer networks, computers and other devices connected to their networks such that they not be used to transmit malicious code and/or malware within documents, links, emails and pdfs to Farrow and/or Farrow Law.

1118. The Law Firm Defendants, individually, breach their non-delegable of reasonable care for which Plaintiffs were foreseeable beneficiaries.

1119. By breaching their individual duties, Plaintiffs have sustained damages.

1120. Alternatively, or conjunctively with the Paragraph immediately above, each Law Firm Defendant, separately, had a non-delegable duty to review its website domains, hosting domain and/or email server domain records, especially with respect to official registered 'updates' recorded and published by open sources, such as ICANN.ORG.

1121. A DNS record 'update' is not a reregistration by a domain owner. DNS record 'updates' are triggered by, for example, changes made by the domain's administrator to, for example, its Top Level Server ("TLS") designations, admin permissions, or altering domain restrictions.

1122. These DNS changes provided the Threat Actor Defendants and their associates the means, and they used these means, to utilize domains belonging to each Law Firm Defendant for malicious purposes, such as to, without limitation, cause communication interferences and/or to procure the theft of PII which was strategically beneficial to their pursuant of the Ultimate Goals to damage Plaintiffs.

1123. With respect to the 'Sitting Duck' and/or 'lame designation' attack, the same was not a zero-day cyber-attack but a well-documented and fairly simple means of using domains for an array of malicious purposes.

1124. Hence, it was foreseeable and, at the same time, would take less than a few minutes to discover and mitigate if necessary.

1125. Yet, the Law Firm Defendants, separately, failed to implement reasonable safe-guards and monitoring policies and procedures notwithstanding the substantial damages which could be accomplished should a threat actor obtaining some or full administrative or ownership control over their domain(s) for any period of time.

1126. As a result of such failures, acts, and/or omissions, the Law Firm Defendants breached their non-delegable duty of care to the Plaintiffs which was foreseeable.

1127. Plaintiffs were foreseeable beneficiaries of the Law Firm Defendants' non-delegable duties of care.

1128. Each of the Law Firm Defendants owed a duty of reasonable care to Farrow and Farrow Law.

1129. The harm caused by the Law Firm Defendants acts and omissions in breach of their duty of care caused Farrow and Farrow Law damages.

1130. The harm caused by the Law Firm Defendants acts and omission to Plaintiff Dr. Doe and Infant Doe was foreseeable.

1131. The harms to Plaintiffs Dr. Doe and Infant Doe with respect to the Law Firm's Defendants knowledge and/or constructive knowledge or negligent ignorance, were foreseeable.

1132. As a result of the action or inactions by the Law Firm Defendants, Plaintiffs have sustained damages to be determined at trial.

WHEREFORE, Plaintiffs demand judgment as to Count IV, for compensatory damages, special damages and punitive damages, along with reasonable costs.

COUNT V
AIDING AND ABETTING
(Plaintiffs v. the Aiding and Abetting Defendants)

1133. Plaintiffs repeat and reallege Paragraphs 1 through 940 as if set forth herein.

1134. The Aiding and Abetting Defendants knew or should have known that Defendants FTI, Gunby, Heath Ritenour, John Ritenour, IOA, Inc. and IOA, LLC were engaged in conduct

constituting unlawful access into protected computers causing damages related to the stolen data or damage to the computer hardware in excess of $5,000 in any given year.

1135. The Aiding and Abetting Defendants were in a position to provide, and did provide material support to these defendants, whether that support was through affirmative acts and/or through omissions, in causing the unlawful access to protected computers which caused damages as alleged herein.

1136. As a result of the Aiding and Abetting Defendants actions or omissions, Plaintiffs have suffered substantial and ongoing injuries.

WHEREFORE, Plaintiffs demand judgment against the Aiding and Abetting Defendants for compensatory damages, special damages, and costs.

COUNT VI
TEMPORARY AND PERMANENT INJUNCTIVE RELIEF UNDER THE FLORIDA RICO ACT, F.S.A. § 895.05 "CIVIL REMEDIES"
(Plaintiffs v. the Threat Actor Defendants)

1137. Plaintiffs hereby assert and reallege allegations 1 through 992.

1138. Fla. Stat. 895.05 provides a private right of action to temporary or injunctive relief pursuant to Florida's Criminal RICO Act.

1139. Plaintiffs allege that the conduct and activities of the Threat Actor Defendants, constitute a pattern of criminal activity as that term is defined in Fla. Stat. 895.03; that the predicate acts alleged to be in violation of 18 U.S.C. 1030(a)(2)(C) from approximately December 2020 and/or at the very least March 2023, are defined as predicate acts pursuant to Fla. Stat. 895.02, which incorporates all the federally proscribed criminal predicate acts within Florida's RICO Act;

and that the Threat Actor Defendants conduct may be enjoined upon a showing of imminent harm or threat pursuant to Fla. Stat. 895.05(6), by and through, enjoining each defendant by either one or more of the following: Fla. Stat. 895.05(1).

1140. By and through their conduct, and the escalation of activities after Plaintiffs seeking law enforcement support and/or judicial relief, with ever more harmful conduct, presents the clear and present danger of immediate harm through the filing of this action;

1141. Separately, and/or collectively, the Carrier Defendants are liable for the acts by their Appointees for engaging FTI to illegal influence judicial proceedings, as it relates here, by and through the cyber-hacking of Farrow Law and Cyberstalking Farrow, Farrow Law and Dr. Jane Doe for purposes of eliminating the prosecution of the 2024 RICO Case, and interfering with that court's proceedings such that Plaintiff could not prosecute that action due to the theft of evidence from Farrow Law's court evidence folder.

1142. Defendants IOA, Heath Ritenour and John Ritenour's conduct, which, as it relates to Plaintiffs, was directed to and did cause an over three year computer and device cyber-attack gained unlawful access Farrow and Farrow Law's Network and Protected Computers, and thereby, they obtained data and information, and/or monitored ongoing litigation file activities, and, after March 2023, also gained unlawful access to protected computers belonging to Dr. Doe and thereby obtained data and information, and/or monitored daily activities.

1143. The Threat Actor Defendants' conduct was directed to interfere with Dr. Jane Doe's work as the medical director of pediatric transplant/adult liver and intestinal transplant at Jackson Memorial Hospital, and had, by hacking into Dr. Jane Doe's phone and devices, had access to messages containing confidential information. Dr. Jane Doe has submitted testimony that

Defendants conduct may result in death or serious bodily harm as the same causes distractions and drains, at the very least, the resource of time her and her staff otherwise dedicate to patient care.

972. The Threat Actor Defendants, by and through their violations of 18 U.S.C. § 1030(a)(4), at the very least, gained unlawful access to Farrow and Farrow Law's Protected Computers and obtaining information related to Farrow and over 40 individuals who participated in the Tuesday 5:30 p.m. online RingCentral video conferences of the 'Fort Lauderdale' meetings.

1144. Upon information and belief, the Threat Actor Defendants used unlawful access into Farrow and Farrow Law's Protected Computers and thereby obtain information by illegally monitoring and recording at least three RingCentral meetings of the Fort Lauderdale 5:30 p.m. Florida Lawyer's Assistance Group, one of which being on or about May 9, 2022.

1145. All of which was intended to benefit the Threat Actor Defendants and the RAPTOR ORGANIZATION, where were acts in violation of 18 U.S.C. themselves, Heath Ritenour, John Ritenour the Insurance Carrier Defendants and which were acts of organized fraud and communications fraud as defined by Florida Statute and violative of Fla. Stat. 895.01 et. Seq. steal identities and to have a fake witness testify and present false evidence of March 2, 2021.

1146. Plaintiffs are demanding, immediate and permanent injunctive relief pursuant to the Florida Criminal RICO Act, Section §895.05(1) and (6) which provides a private right of action for statutory injunctive relief which includes an immediate order entered on an ex parte basis to have the Threat Actor Defendants, and those under their control and direction, agents and contractors, to cease and desist causing, ordering, directing, encouraging and or otherwise setting into motion any act directed to obtain unlawful access into a protected computer for purposes of obtaining information.

1147. Plaintiffs further request a temporary injunction which would include the suspension, restrictions and/or conditions upon Defendant Heath Ritenour, John Ritenour and Insurance Office of America Insurance Licenses pursuant to Fla. Stat. 895.05(6) and (1).

1148. Florida's Criminal RICO Act is distinct from the Federal RICO Act in that it specifically and plainly provides for immediate and meaningful statutory injunctive relief on a codified standard which supplants common law standards for obtaining injunctive relief to a showing of an immediate danger of substantial harm or damage to stop racketeers from profiteering off the backs of the victims of their illegally organized, systemized and normalized patterns of racketeering activities.

1149. Under Section §895.05(6), Plaintiffs constitute aggrieved persons and they hereby demand temporary and/or permanent injunctive relief pursuant to Section §895.05(1)(a)-(e), which provides that: "(1) Any circuit court may, after making due provision for the rights of innocent persons, enjoin violations of the provisions of s. 895.03 by issuing appropriate orders and judgments, including, but not limited to: (a) Ordering any defendant to divest himself or herself of any interest in any enterprise, including real property."

1150. To the extent that this Honorable Court finds and determines that the Threat Actor Defendants Collectively, or individually, have caused the theft of Farrow and Farrow Law's client files, or the evidence file from the 2024 Federal Case, Farrow and Farrow Law respectfully request that this Honorable Court enter an Order requiring them to account for what information and files they have in their possession and to divest such materials as being the fruits of a pattern of criminal activity, as authorized by Fla. Stat. 895.05(1).

WHEREFORE, Plaintiffs demand immediate and permanent injunctive relief as set forth herein, pursuant to Fla. Stat. §895.05(1)(a)-(e), including, but not limited to, the immediate ceasing of all activities directed to cause unlawful access into protected computers owned by Farrow, Farrow Law and/or Dr. Doe, or any other protected computer which has the purpose to obtain information in furtherance of causing imminent harm. Further, Plaintiffs request a temporary injunction as to any further attempts to cause unlawful access to protected computers through the normal course of this case, and permanent injunction prohibiting any of the Threat Actor Defendants from attempt to cause or causing, any unlawful access into a protected computer owned by Farrow, Farrow Law and/or Dr. Doe.

COUNT VII
NEGLIGENCE
(Plaintiffs v. the Carrier Defendants)

1151. Plaintiffs reallege paragraphs 1 through 940 as if fully set forth herein.

1152. At all times material hereto, Carrier Defendants owed a non-delegable duty of reasonable care in the investigation, inspection, oversight of their Appointees IOA, Heath Ritenour and John Ritenour.

1153. The Carrier Defendants breached their non-delegable duties by: (1) failing to reasonably comply with their obligations to investigate Heath Ritenour, John Ritenour and/or IOA, Inc. upon appointment or reappointments; and/or (2) certifying through appointment or reappointment that Heath Ritenour, John Ritenour, and/or IOA, Inc. had the required character and other requirements to be appointed and/or reappointed as the agents of the respective Carrier Defendant.

1154. Carrier Defendants breached their non-delegable duties.

1155. The harm caused by the Insurance Carrier Defendants Agents/Appointees IOA, Heath Ritenour and John Ritenour as to Plaintiffs was foreseeable.

1156. As a result of the action or inactions by the Insurance Carrier Defendants, Plaintiffs have sustained damages to be determined at trial.

WHEREFORE, Plaintiffs demand judgment as to Count VII of the Complaint and for an award of compensatory damages, interest, and costs and for such further relief as this Court deems just and proper.

COUNT VIII
WRONGFUL INJUNCTION
(Farrow and Farrow Law v. Heath Ritenour, John Ritenour and IOA, Inc.)

1157. Plaintiffs Farrow and Farrow Law reallege paragraphs 1 through 940 as if fully set forth herein.

1158. On December 8, 2020, Defendants Heath Ritenour, John Ritenour, and IOA, Inc., filed a Motion for Temporary Injunction in the 2020 Seminole SLAPP Case.

1159. On two previous instances, these Defendants represented to the Court that they, as Plaintiffs, sought no injunctive relief. Pursuant to their representations, and two motions to strike, Farrow and Farrow Law's affirmative defense of unclean hands was stricken prior to these Defendants filing their injunction motion which sought the equitable relief which they denied they were seeking. In so doing, Farrow and Farrow Law were prevented from submitting evidence otherwise relevant and which denied them due process of law.

1160. On November 2, 2020, the Circuit Court had granted a motion for a more definite statement to be filed within twenty days, but these Defendants did not file an operative pleading

until the close of the three day hearing upon their injunction motion. As such, Farrow and Farrow Law were denied due process of law.

1161. On April 14, 2021, the injunction was procured through the presentation of facts and law which were erroneous, and known to be false, such as through the testimony of Kevin Leung. As such, the orders procured with respect to seeking an injunction were frauds upon the court by Heath Ritenour, John Ritenour and IOA, Inc.

1162. An Amended Injunction Motion was entered in April 2023, which exceeded the mandate of the 5th District Court of Appeals.

1163. The injunction was procured in violation of the First Amendment and Farrow and Farrow's rights to due process of law.

1164. IOA had no standing to seek an injunction pursuant to Fla. Stat. 540.01.

1165. IOA had no verified pleading, no verified motion and the documents sent in advance of the injunction motion were for purposes other than for which they were served as further alleged herein.

1166. Heath Ritenour, John Ritenour and IOA, Inc., submitted case law to the court, which was directed to mislead the court, and did mislead the court, as to the law.

1167. As a result of these Defendants actions, Farrow and Farrow Law suffered damages. direct, proximate and foreseeable result of the Carrier Defendants' breaches as alleged herein, Plaintiffs have suffered damages.

WHEREFORE, Plaintiffs demand judgment as to Count VIII of the Complaint and for an award of compensatory damages, punitive danages, interest, attorney's fees and costs and for such further relief as this Court deems just and proper.

VERIFICATION

I, Jay L. Farrow, individually, and as the Corporate Representative of Farrow Law, P.A., do swear under penalty of perjury, and do affirm that the statements made within the following Sections are true and correct to the best of my knowledge, recollection and belief,

Section I.

- Plaintiff Jay L. Farrow
- Plaintiff Farrow Law, P.A.
- Plaintiff Dr. Jane Doe
- Infant Doe

Section VII

- January through March 10, 2024
- March 10, 2024 through April 2024
- March 15, 2024 – the 2024 Federal Case
- March 21, 2024 – Farrow and Farrow Law Discover Substantial New Evidence Related to Manipulating Judicial Proceedings
- Remote Access, Monitoring, Surveillance and obtaining C2 Administrator Status
- APRIL 13, 2024 - Farrow Confidentially Discloses Results from Investigating New Evidence of March 21, 2024 and the Threat Actors' Digital Activities are Exponentially Registered on Five Separate Systems
- May 2024 through July 10, 2024 - Observable Activities and Conduct Resulting in Effective Closure of Farrow Law on July 10, 2024
- Events and Activities Prior to Hearings involving Heath Ritenour, John Ritenour and IOA

Section VIII

- Administrative Logs from Farrow's Lenovo Hard Drive
- Farrow's Cell Phone's Data Usage Increases 2,600%
- Unauthorized Software Installations, Modifications and Application Repackaging:

Section IX

- The Ongoing Persistent Attacks Achieve All Ultimate Goals
- Farrow's Galaxy 22 Phone Reveals Location of Remote Access User
- From August through December 2024
- INTERFERENCES WITH FARROW LAW'S CLIENTS - February 2024 through July 2024

/s/ Jay L. Farrow
Jay L. Farrow, individually, and as:
Corporate Representative of Farrow Law, P.A.

JURY DEMAND

Plaintiffs demand trial by jury on all issues so triable.

Dated: February 5, 2025

Respectfully submitted,

FARROW LAW, P.A.
Attorneys for Plaintiffs
1 Alhambra Plaza, Penthouse
Coral Gables, Florida 33134
Telephone: (954) 805-1915
jaylewisfarrow@proton.me

BY: **/s/Jay L. Farrow, Esq.,**
JAY L. FARROW, ESQ.
Florida Bar Number: 625213