

O.R.A.C.L.E. Detection Response Team

INSTITUTIONAL, PRIVATE ENTITY AND INDIVIDUAL CREDENTIAL LAUNDERING AND RESULTING AUTHORITY-RAIL COMPROMISES



**Authority and the Trusted-Control-Plane Exploitation
Obfuscation through Legal Sector Implicit Trust-Plane Paradigms
Recycling cAPTure-to-Kill APT Components**

IDENTITY • CREDENTIAL • COMMUNICATION • ROLE • STATE • RELIANCE

*A FORENSIC RESEARCH REPORT ON HOW THREAT ACTORS
MANIPULATE APPARENT, ACTUAL, DELEGATED, AND
INSTITUTIONAL AUTHORITY TO PRODUCE GENUINE
CONSEQUENCES INSIDE JUDICIAL AND QUASI-JUDICIAL
ECOSYSTEMS*

REPORT LINEAGE, AUTHORSHIP, AND PEER-REVIEW NOTICE

REPORT LINAGE AND PEER-REVIEW INVITATION

This publication comprehensively expands that certain January 2026 Second Supplemental Avatar Report based upon new evidence and recently published materials which materially supported prior analysis and finding.

Notably, the instant Report's expansion conceptually acknowledges overarching connected relationships between, by example, identified professional-persona operations in which synthetic, stolen, blended, or credential-backed identities entered trusted legal workflows.

More specifically, whereas previously identified imposter personas designed by threat actors through co-opted information from legitimate online presences of 'real' humans, the present report retains that research but enlarges the unit of analysis from the apparent identity of one person to the complete authority-bearing system through which a person, account, role, document, filing, source proposition, or institutional state acquires legal and professional effect. [\[FN 1\]](#)

The Florida record is used because it permits the Authority-Rail Model to be tested across a complete sequence: law-firm communications failure; federal evidence intake; complaint and committee identity; role assignment; response receipt; disputed authorship; sworn emergency authority; notice, consolidation, default, and sanctions; source-to-derivative expansion; Supreme Court review; and terminal public professional status. [\[FN 3\]](#)

The report invites technically specific and source-specific peer review. A later authenticated artifact may correct, narrow, or expand an event-level finding without erasing the historical record that existed when the finding was made. That versioned approach is necessary in an environment where identities, infrastructure, accounts, tokens, publication objects, and institutional records change over time. [\[FN 4\]](#)

ABOUT AUTHORSHIP, RESEARCH, INVESTIGATION
AND EDITORIAL SUPPORT.

Jay Lewis Farrow served as Lead Author and Senior Editor. He is also the legal professional whose law practice and disciplinary record supply part of the multi-year field validation examined in this report. That relationship is disclosed in ordinary language because it explains both the unusual density of contemporaneous evidence and the controls applied to it: first-person recollection is not treated as independent corroboration, and material findings are anchored to source-native communications, filed documents, official dockets, affidavits, public records, independent expert reports, structured datasets, direct FBI communications, or independently verifiable open sources. [\[FN 2\]](#)

Editorial Contributions by the National Attorneys Cybersecurity Association, Inc.

TABLE OF CONTENTS

REPORT LINEAGE, AUTHORSHIP, AND PEER-REVIEW NOTICE.....	ii
I. Executive Orientation: Why Official Authority Is a Cyber Attack Surface	1
A. The Central Problem: Genuine Systems Can Carry Counterfeit Authority	2
B. Principal Determinations.....	5
C. How the Reader Should Use This Report.....	10
II. From Avatar Personas to Authority Manipulation.....	11
A. From Synthetic Persona to Event-Specific Authority	12
B. Communications, Roles, Records, and Institutions as Avatars	15
III. Investigative Method: Reconstructing Authority From Source to Consequence.....	19
A. Source-First Reconstruction and Evidence Hierarchy	20
B. Chronology, State Transitions, and Attribution Discipline	24
C. Citation, Peer Review, and Correction	25
IV. How Authority Normally Moves Through Legal and Quasi-Judicial Systems.....	26
A. From Identity to Filing, Service, and Decision.....	26
B. From Institutional Decision to Public and Professional State	27
V. The ORACLE Authority-Rail Model	29
A. Identity and Credential: Who Appears to Act, and What the System Accepts	29
B. Communications and Role: What Was Represented, and Why the Recipient Was Expected to Act.....	32
C. Procedural State and Adjudicative Intake: What Changed, and How It Reached the Decisionmaker	34
D. Publication and Time: What Becomes Canonical, and Whether the Transition Was Possible.....	37
VI. How cAPTure-to-Kill Uses Authority in a Templated Sequence	39
A. From Reconnaissance to Trusted-Channel Insertion	39
B. From State Transition to Institutional Persistence.....	42
VII. Independent Evidence That the Tradecraft Exists.....	45
A. Synthetic Identity, False Workers, and AI-Assisted Impersonation.....	45
B. Valid Accounts, Tokens, Mailboxes, and Cloud Authority.....	48
C. Legal-Sector Targeting and Judicial-System Risk	54
VIII. Why the Florida Disciplinary Record Is a Field Validation Case	58
A. Why This Record Can Test the Authority-Rail Model	58
B. The Lead Author's Relationship to the Field Record	59
IX. Florida Lawyer Discipline Before the Anomalies: The Process the Reader Must Understand	61

A. Intake, Investigation, and the Grievance-Committee Stage	61
B. Formal Proceedings, Referees, Evidence, and Default	63
C. Emergency Suspension Under Rule 3-5.2	65
D. Supreme Court Review, Terminal Discipline, and Public Record.....	67
X. Field Validation One: How Complaint Identity, Committee Authority, and Role Assignment Entered the Rail.....	68
A. The 11L Baseline and the September 17 Communication.....	68
B. The 17F Assignment Documents and Weiss Chair Representation	71
XI. Field Validation Two: How an Acknowledged Response Became a 'Nonresponse' State	75
A. The October 14 Submission and October 15 Institutional Receipt	75
B. Later Deadlines, Committee Timing, and Physical Delivery	76
C. The November 25 Aggregated Nonresponse Petition	78
XII. Field Validation Three: When the Institutional Communication Channel Itself Became Evidence	79
A. The Proposed Dismissal, Repudiation, and Immediate Disclosure	79
B. Berrena's Changed-Email Statement and the Missing Attribution Bridge	81
XIII. Field Validation Four: How Sworn Authority Amplified a Disputed Source Record	84
A. Separating Personal Knowledge, File Review, and Attributed Statements.....	84
B. The FBI Summary Compared With Direct FBI Communications.....	85
C. From Sworn Summary to Emergency Petition and Later Guilt State	87
XIV. Field Validation Five: How Notice, Consolidation, Default, and New Evidence Changed the Adjudicative State	89
A. Notice, Case Management, Consolidation, and Default	89
B. The September 30 Order, October 1 Hearing, and November 4 Report.....	92
XV. Field Validation Six: How Authority Changes Meaning as It Is Repeated	94
A. From Draft Complaint to Filed-Litigation Conduct	94
B. From Case-Specific Criticism to a Generalized Scheme.....	96
C. Recursive Institutional Authority Amplification	96
XVI. Publication, Media, and Search as Authority Multipliers	100
A. The Terminal Professional Profile	100
B. Byline, CMS, Republished Content, and Search Authority	101
XVII. Why a Compromised Authority Rail Requires a Clean Adjudicative Environment	106
A. The Clean Adjudicative Environment.....	106
B. Cross-Jurisdiction Field Tests.....	107
XVIII. The ORACLE Authority-Provenance Detection Method	111
A. Establish the Ordinary State and the Event-Level Authority	111
B. Preserve and Compare the Communication and Source Object.....	112
C. Reconstruct the State Transition and Downstream Reliance.....	113

D. Verify Through a Known-Clean Channel and Correct the Authority State.....	113
XIX. Meaningfully Timed Response: Preserving Business and Legal Capacity While the Incident Is Active.....	114
A. The First Six Hours: Preserve Source State and Establish Clean Contact	114
B. Six to Twenty-Four Hours: Build the Authority Map and Preserve Institutional Evidence.....	116
C. Twenty-Four to Seventy-Two Hours: Reconstruct State and Contain Consequence....	118
D. Three to Seven Days and Ongoing: Reconcile, Publish, and Monitor	120
XX. Institutional and Industry Recommendations	121
A. Courts, Clerks, Bars, and Regulators	121
B. Law Firms, Legal Departments, and Cybersecurity Providers	123
C. Media, Public-Record Publishers, and Professional Identity Systems	124
XXI. Integrated Determinations.....	126
A. Authority Is an Operational Control Layer.....	127
B. The Accepted State Is the Operational Objective.....	128
C. Authority-Rail Manipulation Is a Distinctive cAPTure-to-Kill Capability	129
XXII. Conclusion	131
A. What the Reader Has Learned About Counterfeit Authority	131
B. How the Report Reached Its Findings.....	133
C. What the Florida Field Record Demonstrated	135
D. Why the Findings Extend Beyond One Proceeding.....	140
E. Containment Before Autopsy	141
F. Clean Adjudication and Institutional Responsibility	143
G. Final Determination	144
FULL ENDNOTES	147

I. Executive Orientation: Why Official Authority Is a Cyber Attack Surface

This Authority Rail Report addresses a form of cyber operation that conventional incident-response language does not fully capture. The operator is not satisfied with stealing a password, reading an inbox, or disrupting a device. The operator seeks control over the pathways by which a court, regulator, lawyer, law firm, client, journalist, provider, licensing body, or public database decides who may act and what later actors will accept as authoritative. ORACLE calls those pathways authority rails. They are the connected identity, credential, communication, role, procedural, routing, publication, and timing systems through which an apparent act becomes a real institutional consequence. [\[FN 5\]](#)

The broader cAPTure-to-Kill model describes an advanced persistent threat directed at legal professionals and the ecosystems surrounding judicial proceedings. Its strategic purpose is not limited to data theft. It seeks to degrade or eliminate the target's ability to communicate, preserve evidence, maintain clients, obtain meaningful review, and continue functioning inside the institutions that ordinarily provide relief. The Authority-Rail Report isolates the tradecraft that makes that strategy unusually effective: the manipulation of apparent, actual, delegated, agency, professional, judicial, regulatory, corporate, and media authority. [\[FN 6\]](#)

A. The Central Problem: Genuine Systems Can Carry Counterfeit Authority

The word avatar is useful because it describes an operating identity: a representation through which another actor can speak, communicate, obtain access, or perform a task. In early ORACLE work, the term principally described professional personas that appeared to possess credentials, biographies, domains, email addresses, and institutional roles but whose histories did not reconcile with the acts performed under their names. That focus captured an important threat class, particularly where a fabricated or blended person is created to obtain trust. It did not yet describe the full mechanism revealed by the later record. [\[FN 7\]](#)

The later record shows that the most effective avatar may be built from components that are individually genuine. A natural person may exist. The

license may be real. The institutional address may belong to the organization. The email can travel through an authorized tenant. The court portal can accept the credential. The document can carry a valid electronic signature image. The attack occurs when those authentic components are arranged to express authority that the source record does not support. [\[FN 8\]](#)

That is why ORACLE now uses authority avatar as the larger category. An authority avatar is the identity, role, relationship, communication, document, or system state through which an operator causes another person or institution to believe that an authorized principal has acted. The represented principal may be a lawyer, investigator, judge, clerk, journalist, law firm, regulator, corporation, committee, court, media organization, or government agency. The operator does not need to control every person inside the institution. It needs enough control over a trusted path to make the next actor accept the false state. [\[FN 9\]](#)

The distinction is practical. If an incident responder treats every problem as a question of whether a named individual is “real” or “fake,” the responder will miss the operation that uses a real person with a false role, a real mailbox with an unauthorized operator, a real order carrying an expanded proposition, or a real public profile pointing to the wrong terminal instrument. The binary question collapses identity, authorship, credential validity, authority, procedural state, and institutional adoption into one label. ORACLE separates those proof layers. [\[FN 10\]](#)

Legal systems are built to convert representations into consequences. A lawyer files a document; a clerk accepts it; a docket records it; a service system sends notice; a judge acts; a regulator publishes a status; a client, employer, bank, insurer, or later court relies on the result. Each step is legitimate because the system assumes that the preceding actor, credential, and record state are authentic enough to support the next transition. [\[FN 11\]](#)

That architecture creates unusual leverage for an adversary. A ransomware operator announces control because payment is the objective. A cAPtUre-to-Kill operator can obtain greater value by leaving the system apparently functional while changing who receives a message, which document becomes the filed object, whether a response is carried forward, which committee appears to possess authority, what a source order is said

to have found, or which public record becomes canonical. The outward system continues to work. The output changes. [\[FN 12\]](#)

Law firms and legal professionals also hold information that is valuable before it becomes evidence: draft pleadings, witness identities, settlement positions, expert reports, provider contacts, sealed materials, client communications, and the timing of emergency applications. Government and industry sources recognize that attorneys and law firms are targeted because their systems contain sensitive case and client data and because disruption can affect the proceeding itself. [\[FN 13\]](#)

The modern court environment increases both efficiency and exposure. A single filing credential can upload an object, create a docket entry, trigger service, generate an email notice, and later support public access. A single professional profile can feed employer, media, search, and licensing decisions. A single authenticated mailbox can communicate with clients, regulators, courts, and providers. When one identity-bearing event creates several downstream states, compromise of that event is not confined to one application. [\[FN 14\]](#)

The distinction matters because legal systems are designed to convert trusted representations into enforceable states. A filing accepted through an authorized account can create a docket event and service obligation. A committee designation can determine who investigates and votes. A sworn affidavit can transform a disputed summary into evidentiary support for extraordinary relief. A court order can be quoted by another tribunal, repeated in a professional profile, and indexed by search engines. If the upstream authority is corrupted, every downstream actor can act honestly and still advance the attacker's objective. [\[FN 15\]](#)

B. Principal Determinations

ORACLE finds that identity in a modern legal environment is not merely a name. Identity is a control layer. It determines who receives a message, which account may file a document, which official may direct a committee, which lawyer may speak for a client or institution, which journalist or publisher appears to authenticate a narrative, and which version of a legal event becomes visible to the public. When an adversary controls that layer, ordinary-looking acts can be produced through genuine systems. The email may pass authentication. The filing may appear on a real docket. The profile may exist on an official website. The consequence may be entered by an

honest decisionmaker. The counterfeit lies upstream, in the identity, relationship, authority, source proposition, or procedural state that the system accepted. [\[FN 16\]](#)

The January ORACLE draft concentrated on avatar personas: apparent professionals whose identities, credentials, profiles, domains, and communications did not reconcile with the operations performed in their names. That work remains important, but the later record demonstrates that a wholly fictitious person is only one form of the threat. A more durable operation uses real people, real Bar numbers, real email domains, real law-firm letterhead, real clerk stamps, real professional biographies, real court portals, and real publication brands. The adversary does not have to invent every component. It has to substitute the relationship among components so the receiving institution accepts a false statement of who is acting, in what capacity, and with what authority. [\[FN 17\]](#)

We therefore define an authority rail as a trusted pathway through which identity is converted into action. The rail begins with a represented actor, continues through credentials and communications, carries a role or institutional relationship, changes a procedural or record state, and ends in an outcome that other actors treat as authoritative. The principal rails examined here are identity, credentials, communications, role and authority, procedural state, adjudicative intake and routing, publication and reputation, and time. Each can be corrupted separately, but cAPTure-to-Kill becomes most effective when several rails converge around the same objective. [\[FN 18\]](#)

The first determination is that authentication does not end the inquiry. SPF, DKIM, DMARC, a valid OAuth token, a successful portal login, a real clerk domain, or a correct professional number may establish that a system accepted a credential or path. It does not establish that the intended natural person authorized the act, that the represented role was valid, that the attachment was the intended version, that the recipient population was correct, or that the event corresponded to a valid legal state. Modern OAuth abuse, token-signing compromise, false-worker operations, and valid-account techniques document the same principle: a legitimate service can process an adversarial instruction as ordinary authorized activity when the credential or signing material has been captured. [\[FN 19\]](#)

The second determination is that the operational objective is the accepted state. Malware, phishing, deepfakes, token theft, DNS manipulation, and false profiles are means. The decisive result occurs when a court, regulator, law firm, media organization, client, insurer, employer, or search engine accepts a false state as true: a response becomes nonresponse; a person becomes counsel; a lawyer becomes an investigating member; one committee identity becomes another; a disputed communication becomes a fabricated filing; a later order becomes proof of an earlier charge; or a public profile reports a terminal sanction while directing the reader to a different instrument. [\[FN 20\]](#)

The third determination is that time is part of authority. A proposition cannot support an earlier act if the source did not yet exist. A party cannot answer a charge that had not been made, respond meaningfully to an order entered one day before a sanctions hearing without notice, or know that a newly entered collateral event will become outcome-determinative after guilt has already been established by default. In the field case, the Sept. 30, 2025 Middle District dismissal/default order did not exist when the June 18 emergency petition was filed or when the Sept. 3 disciplinary default was entered. It was entered one day before the Oct. 1 sanctions hearing and later became part of the Nov. 4 referee report through judicial notice. That sequence is a temporal authority-rail event, not a footnote to the merits. [\[FN 21\]](#)

The fourth determination is that source propositions can acquire broader meaning as they move through institutions. A court order may describe a draft complaint; a later report may say lawsuits were filed. An order may criticize nonparticipation in one case; a later authority may attribute a generalized settlement-pressure scheme to the court. A news article may enter a hearing through opposing counsel, later appear in a judicial order, and then be repeated as though the court independently established the article's narrative. This process is defined here as Recursive Institutional Authority Amplification. Each later source appears independent even when the chain traces to one upstream proposition that changed as it moved. [\[FN 22\]](#)

The fifth determination is that honest institutional reliance is the attack surface. The report does not depend on accusing every named person, clerk, court employee, Bar official, journalist, lawyer, or provider of intentional wrongdoing. A cAPtUre operator gains leverage when ordinary

professionals rely on familiar indicia: an official address, signature block, Bar logo, court caption, e-service notice, docket entry, authenticated mailbox, profile page, or recognized byline. The operation succeeds when a real institution processes the corrupted input and gives it force. [\[FN 23\]](#)

The sixth determination is that the Florida field record supplies a complete authority-rail sequence. A 2023 matter carried an uL identity and a conventional response through independent counsel. In September 2024, an email attributed to John Derek Womack listed matters by base file number and stated that no further response was then required in one matter. A consolidated response was transmitted on Oct. 14 and acknowledged in writing on Oct. 15. Within the same narrow period, documents routed matters into 17F, identified Richard Weiss as chair, varied the language assigning Womack as investigating member, and later supported a petition alleging nonresponse. The record then migrated from 17F to 17A, into emergency suspension, consolidation, default, sanctions, review, and a public permanent-disbarment state without a stable source-traceable bridge at each outcome-determinative transition. [\[FN 24\]](#)

The seventh determination is that the March 2025 communications stream contains an acknowledged authorship failure. One communication attributed to Bar counsel was repudiated. A Bar investigator then wrote that another communication “was not the email I sent you” and “has been changed.” The later referee finding that the affected attorney fabricated emails was not accompanied in the disclosed sanctions record by a native-header attribution, provider-side mailbox audit, server log, endpoint artifact, or email-authorship expert tying creation or alteration to the attorney. The missing attribution bridge is part of the evidence because the communications environment had already been described by an institutional investigator as carrying changed content. [\[FN 25\]](#)

The eighth determination is that the Berrena affidavit converted disputed summaries into emergency authority while omitting qualifying evidence known inside the same stream. The affidavit attributed to FBI agents the categorical statements that the affected attorney had “no case” and that “no investigation was conducted.” Direct FBI communications document meetings, evidence intake, Teleporter uploads, planned computer-analysis response-team review of phones, and continuing review of submitted material. Those communications do not prove that a numbered criminal case remained open in May 2025, but they directly contradict the historical

proposition that no investigative activity occurred. The affidavit also used the disputed Berman-email episode without disclosing the investigator's own contemporaneous statement that a Bar email had changed. [\[FN 26\]](#)

The ninth determination is that public professional identity is a terminal authority rail. The Florida Bar's public record reports permanent disbarment dated May 21, 2026. The linked discipline-document page omits the May 21 terminal instrument and instead presents the corrected Aug. 4, 2025 emergency-suspension order under the label "Amended Supreme Court Order." The completed comparator work found that each directly inspected permanent-disbarment reference page supplied the terminal Supreme Court order. The divergence affects what courts, employers, licensing bodies, insurers, banks, clients, media, and search engines receive as the canonical professional state. [\[FN 27\]](#)

The tenth determination is operational. Legal-sector incident response must begin before the cyber autopsy is complete. The first hours require preservation of native messages and headers, independent contact paths, a map of authority-bearing accounts and roles, identification of deadlines and publication channels, and source-state capture before ordinary systems overwrite the evidence. By twenty-four hours, counsel and responders should know which courts, regulators, counterparties, clients, providers, and public records have accepted the disputed state. By seventy-two hours, the team should have a documented authority graph, a clean communications channel, a continuity plan, and a controlled correction strategy. [\[FN 28\]](#)

C. How the Reader Should Use This Report

The report is organized as a guided investigation rather than a catalog of anomalies. It first explains how authority normally moves through legal and quasi-judicial systems. It then defines the Authority-Rail Model and shows how known impersonation, valid-account, token, cloud, social-engineering, and publication techniques can be combined in a templated cAPTure-to-Kill sequence. Only after that foundation is established does the report present the Florida disciplinary record as a field-validation case. The reader is therefore never asked to recognize a deviation before the ordinary process has been explained. [\[FN 29\]](#)

Each field sequence follows the same method. We identify the last authenticated state; the document, communication, filing, hearing, role

assignment, or publication that purported to change it; the authority carried by that event; the actor or system that relied on the changed state; the consequence; and the evidence required to verify or correct the transition. That method allows judges, lawyers, regulators, cyber professionals, and lay readers to evaluate the same evidence without sharing the same professional vocabulary. [\[FN 30\]](#)

The next Part explains how ORACLE moved from the narrower study of avatar personas to the larger problem of authority manipulation. That evolution is essential because the most effective imposter operation may use a person, credential, institution, and system that are all real. The counterfeit can exist entirely in the relationship among those genuine components. [\[FN 31\]](#)

II. From Avatar Personas to Authority Manipulation

ORACLE began by investigating apparent professionals whose public histories, credentials, communication paths, or institutional appearances did not reconcile with the acts performed in their names. That work remains part of the report. The evidence developed since the January 2026 first draft, however, established that the binary question—real person or fake person—is too crude for modern legal-sector incidents. A real person can be impersonated; a real account can be operated by someone else; a real title can be asserted on the wrong date; a real order can be assigned a proposition it never stated; and a real profile can display a status while linking the wrong supporting instrument. [\[FN 32\]](#)

A. From Synthetic Persona to Event-Specific Authority

The January 2026 ORACLE draft is the starting publication, not an obsolete predecessor. Its central contribution was to treat professional identity as an operational component of an APT rather than as ordinary biographical background. It assembled profile histories, Bar and court records, domains, communications, signature forms, and professional-directory evidence around the question of whether an apparently credentialed person was operating as represented. [\[FN 33\]](#)

The Authority-Rail expansion preserves that question but removes an artificial limit. A later investigation does not have to prove that every named professional is wholly synthetic before it can identify an identity-control failure. A real lawyer can be impersonated. A real Bar employee's

mailbox can be used without authority. A real committee title can be assigned to the wrong person. A real journalist's byline can be copied into an unauthorized wrapper. A real court order can be summarized in language the source did not contain. [\[FN 34\]](#)

This report therefore retains the original ORACLE case-study method—identity history, credentials, contact paths, domains, communications, role, timing, infrastructure, and effect—but applies it to the larger question of who or what carried authority at each event. The result is not a retreat from avatar research. It is the mature form of that research. [\[FN 35\]](#)

A fully synthetic persona is created substantially from fabricated biographical, professional, and social material. The operator may use generated photographs, false employment, invented education, lookalike domains, social accounts, and purchased directory listings. The purpose is not always immediate fraud. Accounts can be aged and cultivated until the identity appears ordinary enough to support later contact or access. [\[FN 36\]](#)

Deepfake and generative-AI tools lower the cost of maintaining this persona. Generated profile images, scripted correspondence, voice synthesis, and automated social activity create continuity across platforms. The technology does not need to produce a perfect imitation. It needs to survive the limited verification applied in the target workflow. [\[FN 37\]](#)

The synthetic persona becomes an authority avatar when another system grants it something real: an account, device, credential, professional relationship, directory status, or institutional role. The false-worker cases demonstrate the transition from invented identity to legitimate enterprise access. [\[FN 38\]](#)

A stolen-identity avatar uses a real person's name, professional history, photograph, license, or account. The downstream recipient sees genuine attributes, making ordinary screening less effective. The operator may use the identity to pass onboarding, establish a mailbox, communicate with trusted contacts, or access an existing account. [\[FN 39\]](#)

Credential-backed avatars are more dangerous than simple lookalikes because the system itself validates them. A valid session or token allows the operator to act from inside the authorized environment. The provider logs a legitimate account event; the recipient sees a familiar domain; the resulting message or state change inherits the institution's credibility. [\[FN 40\]](#)

The distinction between natural person and account operator must remain explicit. Finding that a professional exists does not authenticate the acts performed under that identity. Conversely, finding one unauthorized communication does not establish that every act attributed to the person was counterfeit. ORACLE classifies events, not people in the abstract. [\[FN 41\]](#)

A blended persona combines genuine and false elements. A real address may be paired with false employment. A genuine license may be paired with a fabricated federal admission. A real biography may be copied into a lookalike domain. A real professional's contact information may be supplemented with an account controlled by another operator. [\[FN 42\]](#)

Blending defeats binary verification. Each field checked separately can appear plausible, while the relationship among fields is false. The correct method is relational: does the employer confirm the person; does the domain belong to the employer; did the profile exist before the disputed event; does the account history match the claimed career; and did the natural person authorize this communication? [\[FN 43\]](#)

The Wieder materials illustrate why this category matters. The corpus contains evidence of an apparently real journalistic identity and professional history, while also preserving disputed calls, alternate email paths, derivative publication wrappers, and inconsistent image associations. The ORACLE question is not whether the natural person exists. It is which authority-bearing component—human author, account, telephone path, byline, CMS, derivative site, or search result—performed each act. [\[FN 44\]](#)

These categories are not competing explanations. An operation can begin with a stolen identity, add a synthetic profile, use a genuine professional number, place a false address on a real domain, and later obtain access to an authentic account. ORACLE therefore classifies events and authority states rather than declaring a natural person globally genuine or fictitious. The question is what component carried authority at the moment of the consequential act. [\[FN 45\]](#)

B. Communications, Roles, Records, and Institutions as Avatars

A communications avatar is an event presenting itself as a message from a trusted person or institution. The sender name and address may be genuine. The account may be compromised. Content may be altered after

sending. The attachment may be replaced. The message may be inserted into a real thread. The recipient list may be expanded or changed. [\[FN 46\]](#)

The March 2025 Bar sequence is a direct field example. One message attributed to Bar counsel was repudiated. A staff investigator then stated that a different email was not the email he sent and had been changed. Those statements establish that communications authorship and content integrity were disputed inside the official stream before the later finding that the affected attorney fabricated messages. [\[FN 47\]](#)

A communications avatar is not proven or disproven by appearance. The investigation requires native headers, mailbox and provider logs, message IDs, attachment hashes, tenant audit records, endpoint artifacts, and comparison with known authentic exemplars. Where those attribution objects are absent, a categorical authorship finding lacks the bridge connecting the altered message to a particular creator. [\[FN 48\]](#)

A role-and-authority avatar uses a title or relationship the governance record does not support. The actor can be real. The title can be familiar. The letter can be authentic in form. The false element is the authority claimed at that event. [\[FN 49\]](#)

Examples include a purported committee chair whose term ended, a counsel relationship not established by appearance or engagement, a Bar counsel represented as self-appointing to an investigating role without a separate chair assignment, or a clerk order disposing of a substantive request without visible judicial authorization. Each asks the same question: what source instrument conferred this authority? [\[FN 50\]](#)

The Oct. 15-18 Womack/Weiss documents are important because the language varies within days. One letter says, "I have appointed myself as Investigating Member." Another says, "I will serve as the Investigating Member and will report to the committee when my investigation is complete." The notices identify Womack as the assigned member and Weiss as chair. The variants present different authority stories. [\[FN 51\]](#)

A record-state avatar is a valid-looking state that does not authenticate to the events required to create it. The system may genuinely display the state. The question is whether the source chain supports it. [\[FN 52\]](#)

The Florida field record supplies several forms. A response-received state became nonresponse. An uL matter appeared in 17F and later 17A. A proceeding with an existing responsive record was consolidated into an

emergency case and later defaulted. A timely dispute became uncontested after the transcript path failed. A permanent-disbarment profile points to the earlier corrected suspension order rather than the terminal instrument. [\[FN 53\]](#)

Record-state analysis is the core of ORACLE because the accepted state drives behavior. A later court, employer, client, or media organization is unlikely to reconstruct every antecedent event. It sees the profile, order, docket, or institutional report and acts. Containment therefore requires correction of the state, not only removal of malware. [\[FN 54\]](#)

Media authority can be co-opted without compromising the natural journalist. An authentic article can be copied into a derivative site that retains the original byline and biography while adding a new graphic, headline, or narrative frame. Search users may attribute the entire page to the journalist because the authentic byline acts as a trust token. [\[FN 55\]](#)

A compromised or unauthorized CMS account creates a different mechanism. The article can appear on the genuine outlet domain, under a genuine byline, with the outlet's ordinary social and syndication paths. The inquiry then concerns account history, content revisions, author assignment, publication and modification timestamps, image provenance, and editorial records. [\[FN 56\]](#)

The media rail becomes recursive when the article enters litigation. In Strenger, opposing counsel advised the court about a news report during the December 2024 conference, and the March 19 order later cited the Miami Herald URL. The article's authority was carried into a federal judicial document, where downstream readers could encounter the proposition as part of a court order rather than merely as journalism. [\[FN 57\]](#)

An institutional avatar occurs when a real system carries an unauthorized or corrupted act. The institution itself may be a victim. A real domain can send the message, a real portal can accept the filing, a real profile can publish the status, and a real clerk can process the record. [\[FN 58\]](#)

This is the most consequential category because institutional appearance is often treated as self-authenticating. The familiar seal, masthead, e-service path, or public URL ends the inquiry. ORACLE rejects that stopping point. Official appearance is evidence of presentation, not proof of authorship, authorization, or valid source state. [\[FN 59\]](#)

The security objective is not to undermine confidence in institutions. It is to protect institutional confidence from being weaponized. The institution remains trustworthy only when it can reconstruct who acted, under what authority, through which credential, on what source object, and with what transition record. [\[FN 60\]](#)

The mature Authority-Rail formulation preserves the insight behind the word avatar while removing its artificial limit. An avatar is any representation through which an operator is treated as the authorized principal. Sometimes that representation is a person. Sometimes it is an email account, a committee assignment, a clerk stamp, a professional profile, a filing state, a media byline, or a source proposition attributed to a court. The common feature is substituted authority. [\[FN 61\]](#)

The report will use names where an identity, communication, role, or public record cannot be analyzed without them. It will not infer misconduct by the natural person merely because that person's name appears on a disputed event. That separation is not a disclaimer. It is the core forensic distinction between the represented principal and the operator, process, or system that exercised authority in the principal's name. [\[FN 62\]](#)

The next Part explains the source-first method used to determine which component acted and how an apparent authority state became accepted. Without that method, the report would risk substituting narrative coherence for proof—the very error that authority-rail analysis is designed to prevent. [\[FN 63\]](#)

III. Investigative Method: Reconstructing Authority From Source to Consequence

Authority-rail analysis cannot begin with a conclusion that a person, email, filing, or order is counterfeit. It begins with the source object and the state that existed at the relevant time. The method is deliberately conservative about attribution and exacting about chronology because a genuine system may preserve only the fact that a credential acted, not the identity of the human operator or validity of the authority asserted. [\[FN 64\]](#)

A. Source-First Reconstruction and Evidence Hierarchy

The October 22 CNF report established the integrated cAPTURE model. It treated endpoint compromise, credentials, DNS, MX, portals, communications, and litigation interference as connected evidence rails

within one professional digital ecosystem. It also insisted that containment be planned while the environment remained active rather than after every attribution question had been resolved. [\[FN 65\]](#)

CCDG then isolated a narrower trust problem: technical authentication is not human or workflow authenticity. An email may pass SPF, DKIM, or DMARC because it traveled through an authorized infrastructure path, yet still be operationally counterfeit if the account, tenant, relay, session, signing route, content, attachment, or recipient population was controlled by another actor. [\[FN 66\]](#)

RAPS separated the portal transaction into constituent states. The object prepared by a filer, the object received by intake, the docket entry, the service event, the recipient copy, the chambers or restricted copy, and the public copy are related but not identical proof objects. A cyber-sensitive reconstruction must compare those states rather than assume that one successful portal transaction proves agreement among them. [\[FN 67\]](#)

The September 2026 cAPTURE report then described the trusted control plane: the accounts, permissions, routing, portals, directories, and publication channels that determine who may act and what downstream systems will treat as legitimate. The Civil Cyber-Infrastructure report added the Clean Adjudicative Environment: when credible evidence places the ordinary filing, service, identity, or record channel in dispute, the integrity challenge cannot be tested solely by sending it back through the same disputed channel. [\[FN 68\]](#)

ORACLE occupies the identity-and-authority layer within that research lineage. It asks how an operator acquires the ability to speak with another person's or institution's authority, how that authority is converted into procedural state, and how later systems repeat the result until the original provenance question disappears. [\[FN 69\]](#)

The hierarchy begins with the source-native object: the actual email and headers, filed document, order, docket record, affidavit, roster, portal event, profile page, or preserved publication. A later pleading or expert report can explain the significance of that object, but it does not replace it. Where a later authority says an earlier court “found” a proposition, the earlier order must be compared with the attributed proposition. [\[FN 70\]](#)

Direct institutional records follow the source object. A docket can establish what the public system displays. A staff affidavit can establish what

the affiant swore. A regulator's profile page can establish what the public is told. Those records still require source-layer separation. An affidavit paragraph based on personal observation carries a different foundation from a paragraph reporting what another employee or federal agent allegedly said. [\[FN 71\]](#)

Independent expert reports and structured datasets supply mechanism and cross-source correlation. Marlin, Team B, CCDG, RAPS, CNF, cAPTure, Civil Cyber-Infrastructure, and the Florida historical-proof report were developed at different times and from different objects. Their value is greatest where separate workstreams converge on the same control failure without depending on one another for the underlying fact. [\[FN 72\]](#)

External government, standards, court, provider, peer-reviewed, and technical sources supply mechanism corroboration. MITRE labels techniques; NIST describes identity and incident-response controls; the FBI and DOJ document impersonation and false-worker operations; providers describe token and cloud-control mechanisms; the Judiciary describes attacks against case-management systems. Those sources demonstrate capability and precedent. They are not substitutes for the subject artifacts. [\[FN 73\]](#)

Every material sentence is cited at the point of use. The citation tells the reader where the fact or technical proposition originates, not merely which sources appear somewhere in the same paragraph. That architecture allows a judicial official, investigator, reviewer, or opposing expert to test the report proposition by proposition. [\[FN 74\]](#)

Authority-rail evidence is perishable. Mailbox rules change, social profiles update, public pages are replaced, docket labels are corrected, domains expire, search results shift, and provider logs age out. The preservation objective is not simply to save the words of a message. It is to preserve the message in context: native headers, attachment, sender and recipient fields, visible rendering, account state, date, time zone, and available provider or endpoint evidence. [\[FN 75\]](#)

Visual artifacts are used only where they expose a state difference that prose alone would make harder to see. The Oct. 15-18 Womack instruments, for example, use the same institutional masthead while changing language, formatting, name presentation, and the represented method by which the investigating-member role arose. A reader can understand the significance

more quickly when the variants are placed together and then explained. [\[FN 76\]](#)

Reproducibility also requires negative discipline. The absence of a public biography does not prove a person is synthetic. The use of AWS, Cloudflare, Microsoft 365, Proton, or another common provider does not identify an actor. The evidentiary object is the customer-specific account, timestamp, credential, role, zone change, message, or state transition. [\[FN 77\]](#)

The first evidentiary layer is the source-native object: the email and full headers, the sender and recipient copies, the filed PDF, the portal receipt, the docket object, the service notice, the signed affidavit, the committee roster, the provider record, the public profile capture, or the archived publication. A later pleading or report may explain the object, but it cannot replace it. When two versions differ, both are evidence and the difference becomes a state transition requiring explanation. [\[FN 78\]](#)

The second layer is the institutional record. A docket proves what the docket displayed; it does not prove every upstream proposition embedded in the filing. An affidavit proves what the affiant swore; it does not flatten personal observation, file review, and attributed statements into the same foundation. A professional profile proves what the public is told; it does not by itself prove that the linked source instrument supports the displayed status. [\[FN 79\]](#)

The third layer is independent mechanism evidence. Government advisories, standards, peer-reviewed research, provider investigations, court filings, and reputable technical reporting establish what an attacker can do and what evidence those actions leave. They are used to test feasibility and operational fit. They are not used as a substitute for event-level proof in the subject record. [\[FN 80\]](#)

B. Chronology, State Transitions, and Attribution Discipline

Chronology is not a decorative timeline. It determines whether authority could have operated. A later order cannot support an earlier petition if it did not exist. A committee cannot consider a response before the represented response period has ended. A participant cannot answer a hearing or evidentiary use that was not disclosed through a meaningful notice path. The report therefore fixes each event to a source date and asks what the institution and affected party could know at that moment. [\[FN 81\]](#)

For every consequential event, ORACLE separates four questions. First, what occurred as established by a source? Second, what institutional or record state changed? Third, what technical or procedural mechanism could produce that change? Fourth, what person, account operator, customer, insider, or threat group can be attributed at the level supported by evidence? Keeping those questions separate prevents a familiar technique label from being treated as proof of a particular actor. [\[FN 82\]](#)

Comparator analysis is used for a limited purpose. A comparator does not prove that an outlier is fraudulent merely because it is unusual. It identifies the ordinary control path and tests whether the subject record contains the instrument, notice, assignment, version history, or publication practice expected for that transition. Where the defined control population is uniform and the subject path differs, the report describes the structural divergence and the evidence needed to explain it. [\[FN 83\]](#)

The report also distinguishes corroboration from repetition. A later authority is independent only when it derives from a separate evidence object or investigation. A newspaper repeating an order, a regulator profile repeating a sanction, and a later court repeating the newspaper do not create three proofs if all depend on one upstream proposition. They create three authority handoffs. [\[FN 84\]](#)

C. Citation, Peer Review, and Correction

Every material factual and technical proposition in this redraft is supported at the sentence or closely bounded paragraph level by a numbered endnote. The notes identify the source and the specific application for which it is used. Public sources include live URLs; Project materials are described by human-readable title, date, case or file number, and page or paragraph when available. This structure allows a reviewer to test the report proposition by proposition. [\[FN 85\]](#)

ORACLE is versioned because the evidence environment is dynamic. Provider logs can arrive later; public pages can change; archived versions can surface; a native message can permit header analysis unavailable from a screenshot; and a later court record can clarify an earlier procedural transition. A correction must identify the prior state, the new source, and the reason the determination changed. That form of correction strengthens rather than weakens a source-driven report. [\[FN 86\]](#)

With the method established, the report next explains how authority ordinarily moves through legal and quasi-judicial systems. That ordinary path is the control against which later deviations are measured. [\[FN 87\]](#)

IV. How Authority Normally Moves Through Legal and Quasi-Judicial Systems

A reader cannot evaluate an authority-rail failure without first understanding the ordinary work performed by the rail. Legal systems operate through a sequence of representations that are accepted because each actor and system is assigned a defined role. The sequence is not unique to courts. Regulators, licensing bodies, arbitration programs, media organizations, and corporate legal departments all convert identity and documentation into institutional action. [\[FN 88\]](#)

A. From Identity to Filing, Service, and Decision

The ordinary legal sequence begins with an actor whose identity and authority have been established. A lawyer appears for a client, a regulator assigns counsel or an investigator, a clerk operates within ministerial authority, and a judge or referee exercises adjudicative authority. Credentials allow those actors to use filing, email, case-management, or document systems, but the credential is only the technical representation of a preexisting legal relationship. [\[FN 89\]](#)

A filed document then passes through intake. In federal court, an authorized CM/ECF user uploads an object, selects a case and event, and triggers docketing and a Notice of Electronic Filing. In Florida, the statewide portal routes a filing to the selected clerk and creates filing and service records. The system records what account acted and what event was selected. The legal system attributes those technical acts to the lawyer or filer because the account is registered to that professional. [\[FN 90\]](#)

Service carries the filed event to identified recipients. The recipient population matters because notice is the bridge between a filed object and a binding deadline. A correct filing associated with the wrong case, an altered service list, or an unverified address can produce a real docket event without producing meaningful notice to the person expected to respond. [\[FN 91\]](#)

The decisionmaker ordinarily receives a defined record. A judge, grievance committee, referee, or regulator may rely on pleadings,

testimony, affidavits, admitted exhibits, stipulations, judicially noticed material, and prior orders. Each source category carries a different foundation. The integrity of adjudication depends on preserving those distinctions so that an allegation does not silently become a finding, a summary does not replace direct evidence, and a later document does not appear to have existed earlier. [\[FN 92\]](#)

B. From Institutional Decision to Public and Professional State

A decision changes procedural state. A response may be accepted or deemed deficient; a committee may find probable cause; a court may enter default; a referee may recommend discipline; a supreme court may impose a sanction; and a licensing body may publish the resulting status. Each change should be connected to the previous state by an identifiable act—notice, assignment, hearing, vote, order, report, or final disposition. [\[FN 93\]](#)

Publication extends the effect beyond the deciding institution. Docket text, public orders, lawyer profiles, disciplinary reference pages, press releases, media articles, and search indexes become shortcuts through which later actors understand the person's legal or professional state. That public layer often carries more practical weight than the underlying record because employers, clients, insurers, counterparties, and journalists rarely reconstruct the full adjudicative history. [\[FN 94\]](#)

The ordinary system therefore relies on transitive trust. The recipient of a service notice trusts the filing account and clerk process. The decisionmaker trusts the record assembled through those processes. The public trusts the decision and the profile that reports it. The next actor rarely begins again at the original source. That efficiency is necessary, but it gives a threat actor extraordinary leverage if an upstream identity, role, message, or state can be substituted. [\[FN 95\]](#)

The Authority-Rail Model formalizes those connections. It does not ask institutions to distrust every familiar object. It identifies the points at which trust should be independently re-established because the consequence is high, the channel is disputed, or the represented relationship cannot be reconciled with the governance record. [\[FN 96\]](#)

The next Part develops each rail in detail: what it normally does, how it can be abused, what evidence authenticates it, and what legal or professional consequence follows when the rail carries a corrupted state. [\[FN 97\]](#)

V. The ORACLE Authority-Rail Model

The Authority-Rail Model treats a consequential institutional act as a chain rather than a single object. The model asks whether the identity, credential, communication, role, procedural state, intake path, public representation, and timing all authenticate to the source event that should have created the result. A failure at one rail can be contained; coordinated failures across several rails can create a complete accepted state. [\[FN 98\]](#)

A. Identity and Credential: Who Appears to Act, and What the System Accepts

The identity rail answers the first question every trusted system implicitly asks: who is acting? In ordinary life the answer may be a name. In a legal control plane it is a composite of name, professional number, employer, office, biography, photograph, email address, telephone number, directory listing, device, account, and prior institutional history. The composite is persuasive because no one field carries the entire burden of trust. [\[FN 99\]](#)

Threat actors exploit that distribution. They can fabricate a person, steal an existing identity, blend real and false attributes, or leave the person's identity untouched while substituting the account operator. Government false-worker cases demonstrate the strongest version: a stolen or fabricated identity passes interviews, receives a real device and credentials, and then operates inside the enterprise as an authorized employee. [\[FN 100\]](#)

In legal systems, the identity rail includes attorneys, clients, complainants, witnesses, investigators, legal assistants, Bar counsel, grievance members, reporters, clerks, judicial assistants, experts, and service recipients. The identity question must be answered at the event level: even if the natural person exists, did that person authorize this act, use this account, hold this role, and communicate through this path at this time? [\[FN 101\]](#)

A credential converts identity into executable authority. Passwords are only one form. Modern systems also rely on session cookies, OAuth access and refresh tokens, API keys, device registrations, delegated roles, service principals, certificates, recovery addresses, mailbox permissions, and federated trust. A platform may continue to accept those forms of authority after the visible password has changed. [\[FN 102\]](#)

This explains why replacing a laptop or resetting a password may not restore control. If the adversary retains a refresh token, server-side mailbox permission, recovery method, cloud role, or signing material, the legitimate service continues to process requests as authorized. OWAReaper and Storm-0558 provide concrete examples: persistent permissions and stolen tokens survived visible remediation, while forged tokens were accepted because the services trusted the signing path. [\[FN 103\]](#)

For ORACLE, the credential rail separates real account from authorized human act. A message sent through a real institutional account can be counterfeit in purpose and authorship. A filing submitted through a real portal account can still require event-level authentication. A professional profile updated through a valid login can still express a state the natural person or institution did not authorize. [\[FN 104\]](#)

Identity proofing and authentication are related but different. Identity proofing asks whether the person presenting evidence is the person claimed. Authentication asks whether the claimant controls an enrolled authenticator at a later event. Federation allows one identity provider to assert information to another relying party. None of those functions, standing alone, proves that the authenticated person held the event-specific legal role or intended the specific act. [\[FN 105\]](#)

This distinction explains the strength of false-worker operations. The enterprise may perform interviews, ship a laptop, issue credentials, and create a genuine employee account. The infrastructure and access are real because the organization itself created them. The failure lies in the human principal and relationship represented by the identity. The same structure can appear in legal environments when a valid professional account is treated as conclusive proof of event-level authorship. [\[FN 106\]](#)

Detection therefore requires more than password validity. Investigators must examine enrollment, recovery, token issuance, registered devices, sign-in context, delegated roles, mailbox permissions, and behavioral history. MITRE's valid-account detection guidance likewise emphasizes anomalous logon type, time, geography, and cross-platform activity rather than assuming that a successful login is benign. [\[FN 107\]](#)

B. Communications and Role: What Was Represented, and Why the Recipient Was Expected to Act

The communications rail carries instructions and representations between actors. It includes email, text messages, calls, voicemail, collaboration platforms, attachments, service lists, reply chains, signature blocks, and recipient populations. The communication does more than transfer words. It tells the recipient who is speaking, who else received the message, and what institutional response is expected. [\[FN 108\]](#)

Technical email authentication answers limited questions. SPF tests whether a sending host is authorized for the envelope domain. DKIM tests a cryptographic signature over specified fields and body content. DMARC evaluates alignment and policy. None determines whether the person named in the signature block intended the message, whether the account was compromised, whether a mailbox rule redirected content, or whether the attachment is the version the sender approved. [\[FN 109\]](#)

The same separation applies to calls. A telephone number may be associated with a real person or business and still fail to authenticate the speaker. Caller ID can be spoofed, calls can be forwarded, accounts can be compromised, and AI-generated voice can imitate a trusted person. The FBI's impersonation warnings describe campaigns using text and AI-generated voice to build rapport and reach trusted contacts. [\[FN 110\]](#)

Identity answers who the actor is. Role answers why the actor is entitled to direct action. A lawyer may be real but not counsel in the matter. A Bar employee may exist but not be assigned as investigating member. A lawyer may once have chaired a committee but no longer hold that office. A clerk may possess ministerial authority but not authority to adjudicate a substantive motion. [\[FN 111\]](#)

The role rail is authenticated by appointment records, committee rosters, notices of appearance, representation records, assignment instruments, conflict rules, delegation, and the governing procedural framework. A familiar title in a letter does not create the office if the institutional control record identifies another person. [\[FN 112\]](#)

False relationships are effective because the underlying names can all be genuine. An official-looking communication may connect a Florida Bar email address to private representation of a law firm, or identify a lawyer as committee chair while the roster identifies someone else. The operator does

not have to fabricate the people. The operator fabricates the relationship among them. [\[FN 113\]](#)

Email authentication illustrates the boundary. SPF tests whether an envelope sender is authorized to use a domain. DKIM tests a cryptographic signature over selected message content. DMARC evaluates alignment and policy. Those controls can correctly report success when the message traveled through authorized infrastructure, even though the intended employee did not compose it, a token or mailbox rule was abused, the attachment was substituted, or the represented legal relationship was false.

[\[FN 114\]](#)

Role evidence answers a different question: why is the sender entitled to direct the recipient? Appointment records, notices of appearance, committee rosters, engagement records, delegations, and conflict controls establish that authority. A genuine name and institutional mailbox cannot create a role that the governance record does not support. [\[FN 115\]](#)

Telephone and video contact present the same separation. A known number, familiar voice, or recognizable face can support trust, but forwarding, caller-ID spoofing, account compromise, and AI-generated voice or video prevent those cues from serving as conclusive authentication. The FBI's impersonation warnings therefore emphasize independent verification through contact information obtained outside the disputed communication. [\[FN 116\]](#)

C. Procedural State and Adjudicative Intake: What Changed, and How It Reached the Decisionmaker

A legal proceeding is a sequence of states. A complaint is received. A response is due. A response is filed. A deficiency is identified. A committee acts. A petition is filed. A case is assigned. An answer is due. A default is entered. Evidence is admitted. A report is reviewed. A sanction is published. Each state should be connected to the next by a rule-governed, source-traceable event. [\[FN 117\]](#)

A record-state avatar occurs when the visible state no longer authenticates to the underlying source. A response is acknowledged but later treated as though it did not exist. A matter carries one committee suffix, then another, without a transfer instrument. A disputed review is labeled uncontested after the route to obtain the required transcript fails. The displayed state may be real in the sense that the system shows it. It is

counterfeit in provenance because the bridge that should have created it is absent, false, or inconsistent. [\[FN 118\]](#)

This rail is where cyber operations become legal consequences. The attacker does not need to write the final judgment. If the operator can corrupt the input state—service, notice, authorship, case association, response record, or evidence characterization—the institution may authentically produce the downstream order. [\[FN 119\]](#)

Courts and regulators receive information through controlled intake systems. In federal court, CM/ECF can turn an attorney's upload into a docket entry, service event, notice, and public-access object. In Florida, the statewide e-filing portal routes filings to clerks and service recipients. In discipline, complaint intake, branch assignment, committee routing, referee proceedings, and Supreme Court review form a comparable chain. [\[FN 120\]](#)

The intake rail includes every handoff: who submitted the object, which case received it, whether it was sealed, who was served, what version reached chambers, what PageID or filing number was assigned, and what later public copy appeared. RAPS treats those states separately because a discrepancy at one handoff can change legal meaning while the system remains operational. [\[FN 121\]](#)

The Judiciary's 2025 acknowledgment of sophisticated and persistent attacks against its case-management system confirms that this is not a speculative risk class. Subsequent modernization and MFA measures address identity, sensitive documents, and aging infrastructure, but they also demonstrate how deeply legal authority now depends on the integrity of the electronic control plane. [\[FN 122\]](#)

The procedural-state rail is where technical control becomes legal consequence. A portal or mailbox compromise is not outcome-determinative until it changes receipt, notice, case association, response status, hearing attendance, evidence availability, or the record considered by a decisionmaker. The attack therefore can succeed without altering the final order if it corrupts the inputs from which the institution lawfully generates that order. [\[FN 123\]](#)

Intake and routing must be reconstructed as separate objects. The filer copy, uploaded object, clerk-received object, docket entry, service notice, chambers copy, restricted copy, and public copy are related but not

necessarily identical. When integrity is contested, a successful filing receipt does not establish that each later state preserved the same document, metadata, recipients, and case association. [\[FN 124\]](#)

Court systems have recognized the risk. The federal Judiciary publicly acknowledged sophisticated and persistent attacks against case-management infrastructure, expanded sensitive-document protections, required stronger account security, and accelerated replacement of the aging CM/ECF environment. Those measures establish that filing identity and case-management state are active security concerns, not hypothetical extensions of ordinary endpoint risk. [\[FN 125\]](#)

D. Publication and Time: What Becomes Canonical, and Whether the Transition Was Possible

Legal authority does not end at the docket. Courts, regulators, law firms, professional directories, media organizations, and search engines publish states that others use as shortcuts for trust. A Bar profile can determine whether a lawyer appears eligible. A court order can become a search result. A news article can be cited by opposing counsel and then by a judge. A biography can support hiring, credential verification, or expert qualification. [\[FN 126\]](#)

Publication can amplify a corrupted source state. Once a proposition appears in an official report, later readers often stop asking where it originated. A derivative website can reproduce an authentic article and byline while inserting its own graphic or commentary. A search engine can bind an image, title, and identity incorrectly. A public profile can report a terminal sanction while linking a different order. The publication object becomes the canonical answer unless someone reconstructs the chain. [\[FN 127\]](#)

Time determines whether authority is possible. An event can support a decision only if it existed, was available, and was lawfully incorporated before the decision. A deadline can produce nonresponse only if the recipient had notice and a meaningful interval to respond. A committee can evaluate a response only after the response period has ended and the material has been received. [\[FN 128\]](#)

Temporal analysis fixes each event to a source timestamp and asks what the institution knew at that moment. The Sept. 30 Strenger disposition cannot be treated as part of the June 18 emergency-petition showing. It can

enter the later sanctions record only through an identified evidentiary or judicial-notice event, with corresponding notice and opportunity consequences. [\[FN 129\]](#)

The temporal rail is also critical in media analysis. A publication following a public filing has one evidentiary meaning. A purported author or article demonstrating knowledge before the fact became public has another. ORACLE calls that difference information exclusivity: the analyst must identify the earliest lawful public source for each material fact before assigning significance to timing. [\[FN 130\]](#)

Publication transforms internal process into durable public authority. A licensing profile, order, article, author page, press release, or search result may become the practical answer to who a person is and what occurred. Because downstream users rely on the apparent authority of the publisher, a wrong link, altered biography, derivative wrapper, or expanded source proposition can cause the public record to carry a state unsupported by the originating source. [\[FN 131\]](#)

Time supplies the final control. A source must exist before it can support a decision; notice must precede a binding response obligation; an assignment must precede the act performed under it; and a later correction must preserve the fact that an earlier version governed prior deadlines. Temporal analysis therefore asks not only what the current record shows, but what each actor could know and answer at the moment the consequence was imposed. [\[FN 132\]](#)

The model is now complete. The next Part shows how an operator can move through these rails as a repeatable sequence, turning reconnaissance and credential access into institutional reliance, recursive amplification, and persistence. [\[FN 133\]](#)

VI. How cAPTure-to-Kill Uses Authority in a Templated Sequence

The Authority-Rail Model describes the components of trust. The cAPTure sequence explains how those components can be used operationally. The sequence is templated because the specific court, regulator, firm, or publication can change while the underlying progression remains recognizable: map the trust environment, establish a usable identity or role, obtain executable authority, enter a trusted channel,

change state, induce institutional reliance, amplify the result, and adapt when exposed. [\[FN 134\]](#)

A. From Reconnaissance to Trusted-Channel Insertion

Authority-avatar operations begin by mapping the target's trust environment. The operator identifies clients, counsel, staff, regulators, courts, reporters, providers, family contacts, professional programs, and recurring communications. Email collection and stolen files reveal not only information but relationships: who responds quickly, who can change a deadline, who controls credentials, and whose name will cause action. [\[FN 135\]](#)

Reconnaissance also identifies procedural clocks. Court calendars, docket events, committee meetings, filing deadlines, publication schedules, and travel create windows in which a short communication failure can produce a disproportionate result. [\[FN 136\]](#)

In the field case, the cyber-incident record preceded the later disciplinary sequence. June and July 2024 filings described communication interference, account problems, court-themed messages, and the need for a controlled evidentiary setting. By September, federal agents had received devices and material while Bar communications began through new identity and contact paths. [\[FN 137\]](#)

The operator next establishes a usable identity or authority relationship. For a synthetic person, this may involve social accounts, professional directories, domains, biographies, and staged activity. For a real person, the operator may need only the account, signature image, title, or history already associated with the name. [\[FN 138\]](#)

Role seeding can occur through official-looking documents. A letter identifies a person as chair. A notice names an investigating member. A signature block places a government lawyer in a private representation. A byline and biography bind a derivative article to a known journalist. The receiving actor often treats the document itself as proof of the relationship. [\[FN 139\]](#)

A mature operation may age the role before use. Repeated references in directories, articles, and public records create an echo chamber that makes later appearance seem ordinary. ORACLE evaluates whether that footprint

developed organically, was copied from genuine sources, or appeared in a synchronized window around the operation. [\[FN 140\]](#)

The operator must acquire executable authority. That authority may be a password, token, mailbox rule, signing key, telephone path, portal credential, or access to a document library containing official forms and signatures. [\[FN 141\]](#)

In some operations the key act is relationship substitution rather than credential theft. A real institution is told that a real person holds a role the governance record does not support. A real recipient is instructed to communicate through a different person or address. The adversary's power comes from the recipient's reliance on the claimed relationship. [\[FN 142\]](#)

The false identity or role is inserted into a trusted channel. The message arrives from an institutional domain, appears in an existing thread, is attached to a court filing, or is copied to familiar actors. The channel supplies credibility the content could not obtain alone. [\[FN 143\]](#)

Insertion can occur through publication. An article appears on a recognized domain, a derivative site reproduces a genuine byline, or a profile page reflects a disputed state. The reader receives the proposition through the authority of the platform. [\[FN 144\]](#)

Reconnaissance is relationship mapping, not only network scanning. Stolen email, calendars, pleadings, client lists, social profiles, committee rosters, and publication histories reveal who can create action. The operator learns which assistant controls scheduling, which counsel is trusted, which official can change status, which provider responds to legal process, and which reporter or public page can shape reputation. [\[FN 145\]](#)

Role seeding can be technical or documentary. A new account may be cultivated over time; a real person's biography may be copied; a signature image may be taken from a form library; a title may be inserted into an official-looking notice; or a genuine relationship may be represented where none exists. The recipient often treats the document or platform as proof of the relationship rather than verifying the source appointment. [\[FN 146\]](#)

Executable authority may come from credentials, tokens, device registration, mailbox delegation, cloud roles, portal access, or control of a publication account. It can also come from a false relationship that causes a real person to act. In that form, the operator does not need to compromise

the institution's systems; the recipient supplies the action because the asserted relationship appears authoritative. [\[FN 147\]](#)

B. From State Transition to Institutional Persistence

The inserted authority changes a state. A recipient stops using physical delivery. A response is treated as absent. A committee identity changes. A filing becomes associated with a case. A default is entered. An affidavit transforms summaries into sworn evidence. A public page changes professional status. [\[FN 148\]](#)

This is the operational center of the sequence. The state change should be documented by a source event. ORACLE compares the before state, transition instrument, and after state. Where the transition instrument is missing or conflicts with the governance record, the accepted state becomes the forensic anomaly. [\[FN 149\]](#)

A legitimate actor then relies on the new state. The judge treats the matter as uncontested. The referee treats a later order as proof. A regulator publishes the sanction. A media outlet cites the court. A search engine elevates the official result. [\[FN 150\]](#)

Institutional reliance makes the operation difficult to reverse because later actors are not merely trusting the original attacker. They are trusting the intervening institution. The adversary's proposition gains a new signature at each handoff. [\[FN 151\]](#)

Recursive amplification occurs when the downstream authority is fed into another proceeding or publication as independent confirmation. An article is cited in an order; the order is cited in a referee report; the referee report is approved; the public profile publishes the result; media and search index the profile. [\[FN 152\]](#)

The chain can create an apparent mountain of evidence even when several items trace to the same source. ORACLE therefore identifies dependency. Independent corroboration must arise from a separate source object, not merely from a later authority repeating the earlier proposition. [\[FN 153\]](#)

When one pathway is exposed, the operator can rotate infrastructure or identity. A new account replaces the old account. A different counsel name appears. A derivative site republishes content. A corrected order replaces the earlier public object. A new service address is added. [\[FN 154\]](#)

Persistence is also institutional. Once the state has been accepted, the adversary may no longer need access. The default, public status, search result, or adverse order continues to operate without further intrusion. Incident response must therefore include correction and recovery in addition to technical containment. [\[FN 155\]](#)

The decisive event is the state transition. A message changes the service address; a committee designation changes who appears authorized; a response is omitted from a petition; an affidavit converts a disputed summary into sworn evidence; a default changes allegations into an admitted state; or a public profile converts a complex record into one terminal status. The operator's objective is achieved when the institution accepts that new state. [\[FN 156\]](#)

Institutional reliance then gives the state a new signature. A judge relies on an affidavit, a referee relies on an order, a regulator relies on a committee file, a journalist relies on a court record, or a search engine relies on an official profile. The downstream actor may be entirely innocent. The threat actor's leverage comes from the institution's ordinary presumption that the upstream process was authentic. [\[FN 157\]](#)

Recursive amplification occurs when the institutional output returns as input elsewhere. A news article enters a hearing; the hearing is described in an order; the order is repeated in a referee report; the report is approved; the sanction is published; and the profile dominates search results. The chain can look like independent corroboration even when several nodes depend on the same proposition. [\[FN 158\]](#)

Persistence can outlive access. Once default, sanction, profile status, search ranking, or published finding is accepted, the operation no longer needs the original mailbox or token. Technical remediation that leaves the institutional state untouched therefore restores the device while preserving the attacker's result. [\[FN 159\]](#)

The next Part tests the sequence against independent sources. The purpose is not to claim that every external incident is the same operation. It is to establish that the individual capabilities used by the Authority-Rail model are documented, operational, and increasingly directed at identity, cloud, legal, and public-trust systems. [\[FN 160\]](#)

VII. Independent Evidence That the Tradecraft Exists

ORACLE's field determinations do not stand on analogy. The subject artifacts establish the field events. Independent sources establish the capability environment in which those events must be evaluated. This Part therefore moves from general impersonation to the specific mechanisms by which false identity, valid credentials, cloud persistence, legal-sector targeting, and case-management compromise are converted into trusted action. [\[FN 161\]](#)

A. Synthetic Identity, False Workers, and AI-Assisted Impersonation

The DPRK false-worker record is the clearest external demonstration that synthetic or stolen identity can be converted into genuine enterprise authority. Operators used stolen identities, fabricated profiles and websites, remote interviews, U.S.-based facilitators, laptop farms, and remote-access software to obtain employment. Once hired, they received legitimate devices, credentials, and access to corporate systems. [\[FN 162\]](#)

The security failure did not occur because the corporate laptop was fake. It occurred because the laptop and credentials were issued to the wrong operator. The system's logs correctly recorded activity by the assigned account while misidentifying the human principal. [\[FN 163\]](#)

Follow-on FBI reporting shows that legitimate access can progress into data theft and extortion. The false identity is not only an entry technique. It becomes a persistent insider platform from which the operator can collect information, create additional access, and threaten the organization. [\[FN 164\]](#)

The legal-sector analogue is direct. A professional number, portal credential, official mailbox, or represented role can give the wrong operator the ability to make actions appear institutionally ordinary. The external cases establish the mechanism; field artifacts determine whether it was used in a specific event. [\[FN 165\]](#)

Generative AI changes the economics of impersonation. An operator can create profile images, voice, text, translated correspondence, biographical content, and social activity at a scale that previously required several people. The technology does not need to produce a perfect deepfake. It needs to survive the limited verification applied in a particular workflow. [\[FN 166\]](#)

Realism is only one dimension. Personalization allows the operator to incorporate stolen case details, family relationships, professional contacts, and current events. Automation allows the persona to respond, repost, maintain profiles, and operate across time zones. The combination supports a persistent identity that appears responsive and socially embedded. [\[FN 167\]](#)

Legal and regulatory environments are vulnerable because verification is often remote and document-centered. A profile photograph, video call, scanned license, signature block, and email domain may be accepted as cumulative proof. False-worker operations demonstrate that mature organizations can complete interviews, ship devices, and issue credentials before detecting the operator. [\[FN 168\]](#)

The defensive response is not universal suspicion. It is event-appropriate proof. High-consequence role changes, new counsel relationships, emergency filing instructions, settlement terms, sanctions communications, and account recovery should be verified through an independently obtained contact path and preserved audit evidence. [\[FN 169\]](#)

The Department of Justice, FBI, and CISA have documented remote-worker schemes in which operators used stolen identities, fabricated employment histories, U.S.-based facilitators, laptop farms, remote-access tools, and false websites to obtain genuine employment. Once hired, the operator received a real device, real account, and real access because the victim organization itself completed the authority transition. [\[FN 170\]](#)

The KnowBe4 incident provides a concrete enterprise example: the applicant passed interviews, was hired, and received a corporate laptop before the organization identified the false-worker scheme. The event demonstrates that mature screening can authenticate the presented package while misidentifying the human principal. [\[FN 171\]](#)

Recorded Future's synthetic-identity research describes the same risk at scale: blended identity material, deepfake-assisted verification, remote employment, and legitimate credentials can produce a durable foothold that is difficult to distinguish from ordinary insider access. [\[FN 172\]](#)

Peer-reviewed research supplies the human component. The DeepPhish study measured continuing vulnerability to artificially generated social-media profiles even under favorable detection conditions. Later research

examined synthetic profiles designed to imitate legitimate behavior and the convergence of realism, personalization, and automation in AI-enabled social engineering. [\[FN 173\]](#)

The FBI's senior-official impersonation warning adds operational context. The campaign used text and AI-generated voice to build rapport, exploit the authority of senior officials, and reach accounts or trusted contacts. The relevant security failure was not only the synthetic voice. It was the recipient's reasonable reliance on the official relationship represented by the voice and message. [\[FN 174\]](#)

B. Valid Accounts, Tokens, Mailboxes, and Cloud Authority

A valid account is an account the target system recognizes as legitimate. It may belong to an employee, attorney, contractor, administrator, service account, cloud application, or professional user. Threat actors value valid accounts because actions performed through them blend into ordinary activity and inherit the permissions already granted to the user. [\[FN 175\]](#)

Credential theft can occur through phishing, malware, infostealers, password reuse, session capture, browser data theft, remote-management abuse, help-desk manipulation, exposed secrets, or compromise of a trusted third party. The initial password is often only the first foothold. Once inside, the operator may register a new device, create a forwarding rule, add an OAuth application, generate an API key, or establish another persistence mechanism that survives password rotation. [\[FN 176\]](#)

The legal consequence of valid-account abuse is unusually severe because professional systems often map account possession directly to personal authority. A court portal may treat the registered credential as the attorney. A Bar system may treat the authenticated user as the member or employee. A law firm's document system may treat the session as the lawyer or staff member. The system records a successful authentication event; the legal environment attributes the event to the named professional. [\[FN 177\]](#)

That attribution is a presumption, not a forensic conclusion. When the consequence is material, the investigator must examine device history, IP addresses, session identifiers, token issuance, MFA events, account recovery, forwarding rules, delegated permissions, file hashes, and user behavior. Logging is the bridge between “the account acted” and “the intended human acted.” [\[FN 178\]](#)

A user can authenticate once and receive a session cookie or token allowing later requests without reentering a password. OAuth allows a user or administrator to authorize an application to access defined resources. Refresh tokens can obtain new access tokens after the original token expires. These mechanisms are necessary for modern cloud services, but they also allow access to persist after the visible password has changed. [\[FN 179\]](#)

A mailbox can be controlled without an obvious endpoint implant. Server-side forwarding, delegate permissions, inbox rules, application consent, token theft, or administrative access can redirect or read communications inside the provider environment. The victim may replace the computer and still lose messages because persistence exists upstream of the device. [\[FN 180\]](#)

That distinction is central to cryptographically counterfeit communications. The provider may sign the message correctly because the message originated through an authorized tenant or mailbox. The recipient's system may report SPF, DKIM, and DMARC pass. Yet the intended sender did not compose, approve, or see the message. The technical authentication is accurate at the infrastructure layer and false at the human-authority layer. [\[FN 181\]](#)

ORACLE therefore treats account remediation as incomplete until the organization reviews tokens, app consents, mailbox delegates, forwarding rules, registered devices, recovery methods, privileged roles, and sign-in history. Password rotation alone repairs only the credential the defender can see. [\[FN 182\]](#)

The Domain Name System, or DNS, translates a human-readable domain into the technical destinations used for websites, email, and other services. MX records identify the mail servers responsible for receiving email. Cloud platforms and DNS providers expose consoles and APIs that authorized administrators use to change those records quickly. [\[FN 183\]](#)

A hostile change and a legitimate administrative change can look identical to the provider. If the operator possesses a valid registrar account, API key, IAM role, delegated administrator credential, or cloud session, the provider processes the instruction through the same interface used by an authorized employee. The evidentiary question is customer-specific: which

identity changed which record, from what session, at what time, and with what surrounding event. [\[FN 184\]](#)

DNS control can redirect websites, alter email delivery, point users to a clone, change a certificate-validation path, or place a trusted domain behind an attacker-controlled origin. MX control can divert incoming mail before it reaches the intended mailbox. A compromised relay can preserve the appearance of institutional delivery while changing content or recipients. [\[FN 185\]](#)

Common provider names do not prove common control. AWS, Azure, Cloudflare, Microsoft, Google, and commercial DNS services support millions of unrelated customers. ORACLE assigns weight to exact hosted zones, customer identifiers, record changes, timing, message IDs, certificate relationships, and credential evidence—not to provider presence alone. [\[FN 186\]](#)

A portal is not merely a website. It is a workflow engine. It determines who can submit an object, which case receives it, how fees are paid, whom the system serves, what docket text is generated, and which version later becomes public. [\[FN 187\]](#)

The Florida portal datasets preserve identity-bearing events across employee, membership, and e-filing systems. The public report does not reproduce passwords or sensitive values. Their value lies in demonstrating that professional identity and filing authority are represented by structured fields—usernames, email addresses, URLs, timestamps, source addresses, and account events—that can be compared across systems. [\[FN 188\]](#)

A portal compromise can produce several classes of effect. An attacker can file under another identity, alter a service list, suppress or redirect notice, associate an object with the wrong case, change a public profile, or cause the filed object seen by one participant to differ from the object preserved elsewhere. The effect does not require destruction of the portal. It requires control over one trusted transaction or identity state. [\[FN 189\]](#)

Restricted systems demand stronger evidence preservation because public reconstruction may be impossible later. Native receipts, filing numbers, local copies, service emails, timestamps, PageIDs, and screenshots should be preserved immediately and reconciled with the official docket and recipient copies. [\[FN 190\]](#)

Modern identity attacks increasingly avoid noisy exploitation. Device-code phishing, OAuth consent, access and refresh tokens, registered devices, service principals, and hybrid-cloud privilege create persistence through ordinary platform functions. [\[FN 191\]](#)

Storm-0558 demonstrated that stolen or exposed signing material can generate tokens accepted by services. The incident is a direct warning against equating a service-accepted token with the intended human authority. [\[FN 192\]](#)

Storm-0501 and SCARLETEEL demonstrate the endpoint-to-cloud pivot. Operators used credential theft, cloud secrets, infrastructure-as-code artifacts, and hybrid identity to move from one compromised system into broader administrative authority. [\[FN 193\]](#)

These comparators explain how a legal professional can replace a device and still experience continued control of email, DNS, shared files, or portal access. Persistence may reside in the tenant, token, delegated role, or cloud account rather than on the replacement endpoint. [\[FN 194\]](#)

MITRE ATT&CK treats valid accounts, account manipulation, email collection, adversary-in-the-middle positioning, trusted relationships, data manipulation, and acquired infrastructure as distinct techniques because an operator can remain inside ordinary administrative and communication paths rather than deploy conspicuous malware. [\[FN 195\]](#)

Microsoft's identity research describes device-code phishing, malicious OAuth consent, stolen access and refresh tokens, device registration, internal phishing, and hybrid-cloud pivots. These mechanisms explain why password rotation or endpoint replacement can fail when persistence resides in the tenant, application grant, service principal, mailbox, or cloud role. [\[FN 196\]](#)

Storm-0558 provides a direct warning against treating a service-accepted token as conclusive human authority. Stolen signing material and validation failures allowed forged tokens to be accepted by services. The infrastructure's authentication result was genuine at the validation layer while false at the authorization and human-principal layer. [\[FN 197\]](#)

CISA's cloud identity guidance and logging guidance emphasize privileged identity, federation, tokens, role review, and records showing who accessed or changed what, when, and from where. Those logs are the bridge between an account event and an attribution conclusion. [\[FN 198\]](#)

AWS Route 53 documentation shows how authorized identities can change DNS records transactionally through ordinary APIs. Sysdig's SCARLETEEL research shows how temporary cloud credentials and Terraform-state secrets can support broader access. Infoblox's Vacant Viper research shows how domain and DNS weaknesses can be converted into traffic distribution and malicious operations. Common provider presence proves nothing by itself; customer-specific credentials, zones, record changes, and timing are the evidence. [\[FN 199\]](#)

BleepingComputer's 2026 reporting on OWAReaper described server-side mailbox permissions, OAuth-token theft, and persistence that survived endpoint reimaging and password rotation. The example is useful because it demonstrates why a victim can replace devices yet continue losing control of communications from upstream provider state. [\[FN 200\]](#)

C. Legal-Sector Targeting and Judicial-System Risk

Business Email Compromise is often described through fraudulent payment requests, but the underlying technique is broader. The actor compromises or imitates a trusted account, studies the relationship, and sends a contextually plausible instruction at a moment when the recipient expects action. [\[FN 201\]](#)

The FBI's senior-official campaign warning illustrates professional echo-chamber exploitation. The impersonator used text and AI-generated voice to establish rapport and then sought access to accounts or trusted contacts. The identity of the senior official functioned as a bridge into the recipient's network. [\[FN 202\]](#)

Legal communications create comparable opportunities. Settlement, service, filing, disciplinary, and scheduling messages direct immediate action. An operator controlling the account or thread can create consequences without deploying a visible payload. [\[FN 203\]](#)

Reuters and government reporting have documented mercenary hackers targeting lawyers and litigation participants to obtain documents, intelligence, or advantage in disputes. The legal sector is attractive because a small number of compromised professionals can expose multiple clients, cases, experts, and counterparties. [\[FN 204\]](#)

The compartmented service model matters. One actor may steal credentials, another maintain infrastructure, another conduct social

engineering, and another deliver the result to a customer. DOJ's 2025 Chinese contract-hacker cases describe an ecosystem in which private operators served government and profit objectives through reusable capabilities. [\[FN 205\]](#)

Litigation-related allegations concerning hired hackers and law-firm conduct further demonstrate that cyber operations can become entangled with discovery, privilege, evidence, and judicial remedies. The external record does not prove any particular field actor; it confirms that legal advantage is a documented customer objective for private cyber operations.

[\[FN 206\]](#)

The Administrative Office of the U.S. Courts acknowledged in August 2025 that the Judiciary's case-management system had been subjected to sophisticated and persistent attacks. The Judiciary strengthened handling for sensitive documents and later accelerated modernization of CM/ECF and public-access infrastructure. [\[FN 207\]](#)

That official record changes the baseline. Identity, filing, service, and case-management compromise are not hypothetical attack classes. They are recognized risks inside the federal judicial environment. [\[FN 208\]](#)

CM/ECF's efficiency explains the potential blast radius. One authenticated filing event can create a docket entry, notice, service, recipient copies, and public access. In a contested integrity event, those states must be preserved separately and reconciled. [\[FN 209\]](#)

The Judiciary's highly sensitive document procedures recognize that some evidence requires a controlled path outside ordinary electronic filing. That principle supports the Clean Adjudicative Environment: where the ordinary channel is credibly implicated, integrity evidence must have a known-clean route to a decisionmaker. [\[FN 210\]](#)

FBI business-email-compromise guidance describes actors who compromise or convincingly imitate trusted accounts, study ongoing relationships, and send contextually plausible instructions. The FBI's protection guidance is directly relevant to authority rails: independently obtain the contact path and verify consequential requests rather than relying on the number, address, or link supplied by the disputed message.

[\[FN 211\]](#)

Reuters documented hackers-for-hire targeting lawyers and law firms for information connected to litigation and disputes. The United Kingdom's

National Cyber Security Centre likewise identifies legal organizations as high-value targets because they hold sensitive client, litigation, and commercial information. Microsoft separately expanded cybersecurity assistance for attorneys targeted by nation-state actors. [\[FN 212\]](#)

The Department of Justice's 2025 charges against Chinese contract hackers describe a compartmented ecosystem serving state and private objectives. Reuters' reporting on Dechert-related litigation illustrates how alleged mercenary hacking can become entangled with privilege, discovery, and judicial remedies. These sources establish legal advantage as a documented customer objective for private cyber capability. [\[FN 213\]](#)

The federal Judiciary's own record is equally important. In August 2025 it acknowledged sophisticated and persistent attacks on the case-management system. In 2026 federal judges described acute and persistent risk in the aging CM/ECF environment, and the Judiciary approved major funding to accelerate secure modernization. PACER also implemented MFA and stronger password standards for filing-level users. [\[FN 214\]](#)

The highly sensitive document procedures recognize that ordinary electronic filing is not appropriate for every high-risk evidence object. The Microsoft/Fortra/Health-ISAC civil disruption record similarly shows that courts can translate technical evidence into precise provider commands when a trusted evidentiary and procedural path exists. Together, those sources support the need for a Clean Adjudicative Environment when the ordinary filing or service path is itself credibly implicated. [\[FN 215\]](#)

The external record establishes the individual capabilities ORACLE examines. It does not prove the Florida field events by analogy. The field case begins in Part VIII because it supplies its own source objects, chronology, and institutional consequences. [\[FN 216\]](#)

VIII. Why the Florida Disciplinary Record Is a Field Validation Case

The report now turns from general mechanism to field validation. The Florida disciplinary record is not included because it is the only legal matter in which identity and authority can be disputed, and it is not offered as a substitute for broader research. It is included because it preserves an unusually dense longitudinal record across a law firm's collapsing communications environment, federal evidence channels, Florida Bar complaint and committee processes, Supreme Court dockets, referee proceedings, media publication, and a final public professional profile. [\[FN 217\]](#)

A. Why This Record Can Test the Authority-Rail Model

A useful field case must allow the investigator to see more than one suspicious event. It must preserve a before state, a series of transitions, institutional reliance, and a terminal consequence. The Florida corpus contains those layers: a conventional uL response through independent counsel; documented cyber-interference filings before the later disciplinary petitions; a replacement communication path; complaint and committee identity changes; acknowledged receipt followed by nonresponse allegations; disputed authorship; a sworn emergency petition; notice, consolidation, and default events; source-order changes; review chokepoints; and a public permanent-disbarment status. [\[FN 218\]](#)

The record is also temporally useful. June and July 2024 filings described communications interference, account loss, court-themed messages, and the need for a controlled evidentiary setting before the first Supreme Court disciplinary petition. Independent technical reports, portal datasets, FBI communications, hand deliveries, and later specialist work were preserved before the final disciplinary outcome and public status. That sequence reduces the risk that the cyber-integrity theory was selected after the result. [\[FN 219\]](#)

The case therefore permits the model to be tested across all eight rails. Identity appears in professional names and complainant states. Credentials appear in email, portal, cloud, and public-profile access. Communications appear in changed messages, disputed sender paths, physical delivery, and service. Role appears in committee chair and investigating-member designations. Procedural state appears in received response, nonresponse, default, and uncontested review. Intake appears in dockets, filing routes,

and the original-writ path. Publication appears in media and Bar profile states. Time determines whether each later event could have supported the earlier one. [\[FN 220\]](#)

B. The Lead Author's Relationship to the Field Record

Jay Lewis Farrow is the lead author and the legal professional whose law practice and disciplinary record supply part of the longitudinal field case. That fact is stated plainly because the reader should understand both why the evidence is unusually detailed and how the report controls for the author's participation. [\[FN 221\]](#)

The report does not treat Farrow's recollection as independent corroboration. First-person statements are used as evidence only in the capacity they actually possess: they can establish what he reported, requested, understood, or did at a particular time. Material findings are anchored to contemporaneous filings, acknowledged communications, affidavits, official dockets, public records, source documents, independent expert reports, datasets, FBI communications, or separately verifiable open sources. [\[FN 222\]](#)

The field case is also bounded. ORACLE does not ask the reader to re-adjudicate every grievance or civil allegation. It asks whether each outcome-determinative identity, role, response, notice, evidence, and publication state authenticates to the source event that should have created it. That narrower inquiry is what makes the record useful to courts, regulators, cyber responders, and institutions beyond the individuals involved. [\[FN 223\]](#)

Before presenting any deviation, the next Part teaches the Florida lawyer-discipline process in ordinary language. A reader cannot understand why a committee identity, referee order, evidentiary omission, or review-state change matters until the ordinary institutional path has been established. [\[FN 224\]](#)

IX. Florida Lawyer Discipline Before the Anomalies: The Process the Reader Must Understand

Florida lawyer discipline is a specialized judicial system. It is administered through The Florida Bar, local grievance committees, circuit and county judges serving as referees, the Bar's Board of Governors, and the Supreme Court of Florida. A cybersecurity expert may know how a mailbox or token is compromised and still have no reason to know what a grievance committee does. A lawyer from another jurisdiction may know professional discipline generally and still not understand Florida's file suffixes, designated reviewers, referee procedure, or Supreme Court review. This Part establishes the ordinary process before the field record is measured against it. [\[FN 225\]](#)

A. Intake, Investigation, and the Grievance-Committee Stage

The Supreme Court of Florida has constitutional authority over the admission and discipline of Florida lawyers. The Florida Bar operates as an official arm of the Court and performs the investigation and prosecution functions assigned by the rules. The Court ultimately determines final discipline, while the Bar, grievance committees, referees, and Board participants perform different stages of intake, investigation, charging, trial, and review. [\[FN 226\]](#)

The ordinary process begins when the Bar receives an inquiry concerning a lawyer. The Attorney Consumer Assistance Program, commonly called ACAP, performs the initial intake function. Intake counsel can close matters that do not warrant discipline, request additional information, refer fee or cost disputes to appropriate programs, or send a matter to one of the Bar's branch offices for additional investigation. The branch and circuit structure matters because the later grievance committee ordinarily comes from the circuit or jurisdiction assigned to the matter. [\[FN 227\]](#)

A Florida Bar file number identifies the matter, and the suffix can communicate circuit, committee, office, or procedural information. The suffix is not merely decorative if the later process depends on which committee's members, chair, conflicts, and designated reviewer possess authority. A change from an Eleventh Circuit lane to a Seventeenth Circuit committee or branch therefore requires a source-traceable institutional act rather than an unexplained caption change. [\[FN 228\]](#)

During the investigation, Bar counsel ordinarily identifies the allegations and requests a written response from the respondent lawyer. The response becomes part of the investigative record. If the response is incomplete, nonresponsive, or additional information is needed, the process ordinarily creates a further request, deadline, or deficiency state. A later allegation of nonresponse should therefore preserve whether a response was received, which file it addressed, what deficiency remained, what supplemental request issued, and when the response period expired. [\[FN 229\]](#)

If additional investigation or prosecution is warranted, Bar counsel presents the matter to a grievance committee. Florida's local grievance committees contain lawyers and nonlawyers and function in a role often compared to a grand jury: they investigate and decide whether probable cause exists to believe the lawyer committed misconduct warranting disciplinary action. The committees can also recommend no probable cause, no probable cause with a letter of advice, diversion, or minor misconduct, depending on the rules and posture. [\[FN 230\]](#)

The committee chair has governance responsibilities, including assignment and management of investigative work. An investigating member may gather facts, communicate with participants, and report to the committee. Bar counsel can perform investigative functions when properly assigned. The authority question is therefore not whether a Bar lawyer can ever investigate. It is which chair, committee, assignment, and source instrument conferred the role in the matter at the relevant time. [\[FN 231\]](#)

Committee action is not ordinarily the end of institutional review. A designated reviewer from the Board of Governors reviews committee outcomes and can approve, return, or refer the matter for additional Board-level consideration. The checks are important because probable cause, no probable cause, diversion, and minor-misconduct decisions determine whether a confidential investigation closes or moves toward public formal prosecution. [\[FN 232\]](#)

B. Formal Proceedings, Referees, Evidence, and Default

When the matter proceeds to formal prosecution, The Florida Bar files a formal complaint in the Supreme Court of Florida, unless a rule supplies a different direct path. The Supreme Court does not ordinarily conduct the evidentiary trial itself. It appoints or directs the appointment of a referee, typically a circuit or county judge, to preside over the disciplinary

proceeding, manage the case, receive evidence, make findings of fact and guilt, and recommend a sanction. [\[FN 233\]](#)

The referee is therefore the trial-level factfinder within the disciplinary system, but not the final disciplinary authority. The referee's orders can control scheduling, pleadings, discovery, hearings, and evidentiary procedure. At the end of the case, the referee submits a report to the Supreme Court containing findings, rule-violation determinations, aggravating and mitigating factors, recommended discipline, and costs. The Supreme Court retains final authority to approve, reject, or modify the recommendation under the governing standards and precedent. [\[FN 234\]](#)

A case-management conference ordinarily identifies the governing pleadings, deadlines, discovery path, hearing dates, and unresolved procedural issues. Notice is indispensable because absence from a conference or failure to meet a deadline can later support default or sanctions. When the proceeding contains more than one Supreme Court case, consolidation can change the operative complaint, answer obligation, service population, discovery record, and relationship between earlier and later filings. That is why the timing and source instrument for consolidation matter. [\[FN 235\]](#)

The Bar and respondent can obtain discovery and present evidence under the disciplinary rules. The evidence at a final hearing can include testimony, affidavits, admitted exhibits, stipulations, prior orders, and matters subject to judicial notice. Those categories should remain distinct. An affidavit based on personal observation has a different foundation from an affidavit reporting what another employee or federal agent allegedly said. Judicial notice can establish the existence and contents of a court record, but it does not automatically transform every allegation or broad characterization within another proceeding into an adjudicated fact for a different purpose. [\[FN 236\]](#)

Default has a specific procedural consequence. If a respondent fails to answer an operative complaint after valid notice and a properly created obligation, the referee can treat allegations as admitted and limit the remaining hearing to discipline. That change is profound: the proceeding moves from contested liability to sanction. The authority-rail questions therefore begin before the default itself—what pleading was operative, what case identity governed, what notice issued, what address or account

was served, what response already existed, and what order created the answer obligation. [\[FN 237\]](#)

At the sanctions stage, the referee considers aggravating and mitigating factors, discipline in comparable cases, the Florida Standards for Imposing Lawyer Sanctions, and the record developed in the proceeding. Mitigation includes matters such as absence of prior discipline, personal or emotional problems, cooperation, good character, rehabilitation, other penalties, and delay, while aggravation includes prior discipline, dishonest motive, pattern, multiple offenses, obstruction, and refusal to acknowledge wrongdoing. The integrity of the evidence supporting those findings directly affects the sanction recommendation. [\[FN 238\]](#)

C. Emergency Suspension Under Rule 3-5.2

Rule 3-5.2 creates an extraordinary path. Rather than wait for the complete ordinary disciplinary process, The Florida Bar may petition the Supreme Court for emergency suspension when the petition is properly authorized and supported by one or more affidavits containing facts personally known to the affiants that, if unrebutted, would establish clearly and convincingly that the lawyer appears to be causing great public harm. The reduced pre-suspension process gives the petition and supporting affidavits exceptional authority. [\[FN 239\]](#)

Under the rule governing the relevant period, the Supreme Court could issue an emergency suspension order, and the petition then functioned as the formal complaint. The respondent had a defined period after docketing of the suspension order to answer and assert defenses. The Court was to appoint or direct appointment of a referee promptly, and the referee was to hear the merits and sanction issues under the disciplinary-trial procedure on an expedited schedule. [\[FN 240\]](#)

The rule also allowed the suspended lawyer to seek dissolution or modification. A motion for dissolution did not automatically stay the suspension, but the rule contemplated prompt assignment to a referee and expedited findings and recommendations. The emergency structure therefore depended on traceable authorization, personal-knowledge affidavits, a clearly identified operative petition, notice, an answer opportunity, a prompt referee process, and a final report within the prescribed framework. [\[FN 241\]](#)

Because the petition can change professional status before a full merits trial, source discipline is particularly important. A summary attributed to another employee, an oral statement attributed to law enforcement, a collateral order, or an email-authorship assertion should be identified by source class. An affidavit's signature and filing status give the document institutional authority, but they do not eliminate the need to distinguish personal knowledge from file review, hearsay, and technical conclusion. [\[FN 242\]](#)

D. Supreme Court Review, Terminal Discipline, and Public Record

After the referee files a report, a party can seek review under the applicable disciplinary rules. Review ordinarily requires timely procedural steps, including identifying disputed findings or recommendations, obtaining the hearing transcript when necessary, and submitting the record and briefing required by the Court. If no review is properly pursued, the report can be treated as uncontested. The distinction matters because a contested report invites judicial examination of challenged findings, while an uncontested report follows a different decisional path. [\[FN 243\]](#)

The Supreme Court is the final disciplinary decisionmaker. It can approve or disapprove findings and impose a sanction that differs from the referee's recommendation when the governing law and record require it. Disbarment terminates membership and ordinarily permits a future readmission application only after the period specified by rule or order. Permanent disbarment is categorically more severe because it precludes readmission. The terminal order therefore matters independently from an earlier suspension order or referee recommendation. [\[FN 244\]](#)

Costs, restitution, and other obligations must be traced to the order or incorporated source that imposes them. The final public state is then published through the lawyer's membership profile and discipline-document reference page. The Bar's own instructions tell the public that the discipline reference opens the court documents, including the Supreme Court order and report of referee. The profile and document page therefore operate as a professional-identity system relied upon by courts, employers, clients, insurers, banks, media, and other licensing bodies. [\[FN 245\]](#)

This ordinary process supplies the control for the field analysis that follows. The question is not whether a disciplinary institution can ever transfer a file, assign Bar counsel as investigator, consolidate cases, enter

default, take judicial notice, or impose severe discipline. The question is whether the source record shows the required authority, notice, sequence, and evidentiary bridge in the specific event. [\[FN 246\]](#)

X. Field Validation One: How Complaint Identity, Committee Authority, and Role Assignment Entered the Rail

With the ordinary process established, the report can now evaluate the first field sequence without requiring the reader to supply Florida disciplinary knowledge. This sequence tests three connected rails: the identity assigned to each complaint file, the committee and chair represented as holding authority, and the investigating role through which later committee action purportedly occurred. [\[FN 247\]](#)

A. The 11L Baseline and the September 17 Communication

The field chronology begins before the cAPtUre event sequence with Florida Bar File No. 2024-70,126(11L). In November 2023, independent counsel responded on behalf of the attorney through a conventional Bar process. The file carried an 11L suffix, corresponding to a Miami-Dade/Eleventh Circuit grievance lane, and the response addressed the source orders and requested closure. [\[FN 248\]](#)

This baseline matters because it fixes the original identity of the matter. The suffix was not merely a decorative code. It identified the committee lane, branch relationship, membership, conflicts, quorum, and authority through which later action would occur. [\[FN 249\]](#)

The 2023 event also establishes behavior. The attorney had previously received a Bar inquiry and responded through counsel. The later disciplinary story did not begin with a person who had never engaged with the regulator. It began after a conventional response history and during a documented breakdown of the law firm's communications environment. [\[FN 250\]](#)

On Sept. 17, 2024, an email attributed to John Derek Womack acknowledged receipt of messages and listed open Bar matters by base file number. It identified two matters in which no further response was then required, including 2024-70,126, and identified eleven marked matters requiring responses. It stated that the underlying complaints and Number 1 letters would follow through a legal assistant. [\[FN 251\]](#)

The signature block identified “J. Derek Womack” as “Senior Litigation Attorney,” located at The Florida Bar's Tallahassee headquarters. No committee suffix appeared beside the listed base file numbers in the email text. The communication established a represented state: specified matters existed, specified matters required responses, one prior matter did not then require further response, and source complaint packages would be supplied. [\[FN 252\]](#)

The attorney's reply described a zero-trust protocol, identified federal-law-enforcement communications, and questioned which office or person held jurisdiction over matters that had previously been handled elsewhere. That reply did not refuse regulation. It placed the sender on notice that the target did not regard ordinary electronic appearance as sufficient authentication. [\[FN 253\]](#)

The November 2023 11L matter is an authenticated control because independent counsel responded through an ordinary Bar path before the later cAPTURE sequence. It establishes that the affected attorney did not enter the disciplinary record as a person who categorically refused to respond. It also fixes a Miami-Dade/Eleventh Circuit identity against which the later Seventeenth Circuit designations can be compared. [\[FN 254\]](#)

The September 17 communication then created a represented inventory of matters and response obligations. It stated that no further response was then required in the prior matter, identified other base file numbers requiring responses, and represented that complaints and initial inquiry letters would follow. The email did not display the later 17F suffix beside the listed base files. [\[FN 255\]](#)

The authority-rail significance is straightforward. The communication fixed the state from which later changes must proceed. If a file later moved to another circuit or committee, a source instrument should identify the transfer. If a matter later became nonresponse, the record should identify the request, deadline, response, deficiency, and committee action that produced that state. [\[FN 256\]](#)

B. The 17F Assignment Documents and Weiss Chair Representation

Within hours and days of the acknowledgment, letters dated Oct. 15-18 routed matters to Grievance Committee 17F and addressed Richard Jay Weiss as Chair. The documents used several formulations. One said, “I have appointed myself as Investigating Member.” Another said, “I will serve as

the Investigating Member and will report to the committee when my investigation is complete.” The accompanying notices identified Womack as investigating member and copied Weiss as chair. [\[FN 257\]](#)

The ordinary process must be explained before the anomaly. A grievance committee chair assigns investigative duties within the committee structure, and Bar counsel may serve in an investigating capacity when properly assigned. The question is not whether Bar counsel can ever perform investigative work. The question is what authenticated chair or committee act assigned the role in these files and why the source documents tell materially different stories about how the role arose. [\[FN 258\]](#)

The variants extend beyond wording. The correspondence changes typeface, line spacing, phone-number format, signature placement, name form, and whether the document says “appointed myself” or “will serve.” Those features do not independently prove forgery. Their value is comparative: a high-volume set of form instruments purporting to create the same role did not preserve one stable template or authority explanation. [\[FN 259\]](#)

The letters also reused the attorney's former firm email and telephone information after the attorney had disclosed new Proton-based channels and a replacement number in the October response. In an ordinary system, outdated contact data can result from template reuse. In a compromised authority rail, it can cause service to continue through a channel already reported as unavailable or untrusted. The evidentiary point is that contact state, role state, and committee state changed together. [\[FN 260\]](#)

The Oct. 15-18 instruments identify Richard Jay Weiss as chair of 17F. The Project's archived roster research places Marcela Gyires in the 17F chair position during the relevant late-2024 period and identifies Daniel Forrest as chair of 17A; Weiss was not listed as chair or member of either committee in the preserved control. [\[FN 261\]](#)

The authority representation is binary at the event level. Either Weiss held the chair position required to receive and act on the matters at that time, or he did not. The letter does not become authoritative merely because it uses Bar letterhead and a familiar title. The institutional roster is the control designed to answer who possessed that role. [\[FN 262\]](#)

The same period created a conflict collision. Weiss Serota, Weiss's firm, issued a three-day default and possession notice concerning Farrow Law's

Coral Gables office. In the same hours, 17F disciplinary materials were being sent to Weiss in the represented chair capacity. The field record contains no contemporaneous recusal, substitution, conflict determination, or role correction explaining how the two positions were reconciled. [\[FN 263\]](#)

ORACLE does not need to determine that Weiss personally authored or approved every instrument. The Authority-Rail finding is that the materials carried his name and firm into a committee-chair role the archived governance record did not support and that overlapped with adverse law-firm activity. [\[FN 264\]](#)

The Nov. 25 Supreme Court petition and acknowledgment used 17F. Later referee and emergency-suspension materials used 17A for the same base matters. The June 18, 2025 venue filing listed Miami-Dade residence and office, “Offense: Unknown,” and multiple 17A files. [\[FN 265\]](#)

A file may be transferred or reassigned through lawful process. The forensic question is the source instrument accomplishing the transfer. The defined record contains the before state and after state but no complete file-specific bridge showing who reassigned each matter, on what date, under what authority, and with what effect on the prior 17F acts. [\[FN 266\]](#)

The transition matters because committee identity carries more than geography. It determines members, chair, investigating assignment, conflicts, quorum, and the institutional basis for a probable-cause or referral act. A later caption cannot retroactively authenticate an earlier role assignment. [\[FN 267\]](#)

The October documents did not merely add a committee code. They represented that Grievance Committee 17F possessed the matters, that Richard Jay Weiss was its chair, and that John Derek Womack would act as investigating member. Those representations carried institutional consequences because the committee identity determines members, conflicts, assignment authority, quorum, and the path to probable cause. [\[FN 268\]](#)

The source variants tell different authority stories. One states that Womack appointed himself; another states that he would serve and report to the committee; accompanying notices identify him as assigned. The ordinary process permits Bar counsel to investigate when properly assigned, but the record must still identify the chair or committee act that created the assignment. The variation therefore matters not as typography

alone but as evidence that the represented source of authority changed within the same document series. [\[FN 269\]](#)

Archived governance evidence placed another lawyer in the 17F chair position during the relevant period and did not place Weiss in the represented role. At the same time, Weiss Serota was acting adversely to the affected law practice regarding its office premises. The defined record contains no contemporaneous recusal, substitution, or authenticated committee correction reconciling the represented chair role before the disciplinary sequence advanced. [\[FN 270\]](#)

The later shift from 17F to 17A presents the same source-state question. A lawful reassignment is possible. The evidentiary issue is the missing file-specific bridge: who reassigned the matter, when, under what authority, and with what effect on the prior 17F role, committee, and conflict states? A later caption cannot retroactively authenticate an earlier assignment. [\[FN 271\]](#)

Field Validation One therefore establishes the first complete Authority-Rail pattern: a stable file identity gave way to new committee and role representations; those representations carried authority into later proceedings; and the defined record did not preserve one consistent appointment and transfer path. The next sequence asks how the response state moved through that same rail. [\[FN 272\]](#)

XI. Field Validation Two: How an Acknowledged Response Became a 'Nonresponse' State

A disciplinary system can evaluate, reject, or demand supplementation of a response. It cannot accurately narrate the matter as nonresponse without accounting for a response the institution acknowledged receiving. This Part reconstructs the transition from the October 14 submission to the November 25 petition and explains why the missing bridge matters more than the label ultimately applied. [\[FN 273\]](#)

A. The October 14 Submission and October 15 Institutional Receipt

The attorney and Womack had discussed overlap among the inquiries and a consolidated response format. On Oct. 14, the attorney transmitted the package. On Oct. 15, Christine Mitchell replied: “We have received the email that you sent last night at 7:20pm. Thank you.” [\[FN 274\]](#)

That sentence is the controlling state. The institution's communication stream recorded receipt. A later reviewer may assess whether the package

was complete, responsive, privileged, or deficient. Those are separate states. The record cannot accurately move directly from acknowledged receipt to nonresponse without an intervening act identifying the deficiency, file, deadline, and consequence. [\[FN 275\]](#)

No complete file-by-file transition appears in the defined record after Oct. 15. The Nov. 25 petition alleged that thirteen official inquiries remained unanswered, but it did not integrate the consolidated response, Mitchell's acknowledgment, physical deliveries, or the cybersecurity context into its nonresponse narrative. [\[FN 276\]](#)

This is the first full Authority-Rail conversion in the field case: response received → response omitted → nonresponse alleged → Supreme Court proceeding initiated. Each downstream act may have been processed by a real institution, but the state carried into the petition did not preserve the acknowledged source event. [\[FN 277\]](#)

The October 15 acknowledgment is the controlling source state because it was generated inside the represented institutional communication stream. It did not determine that every complaint had been fully answered. It did establish that a package existed, arrived, and was recognized by the Bar legal assistant. Any later conclusion of nonresponse therefore required a file-specific institutional act explaining what remained unanswered and what the respondent was required to do next. [\[FN 278\]](#)

The distinction among received, deficient, incomplete, rejected, and absent is essential. Those states carry different notice and intent implications. A person who sends a package later deemed insufficient is not in the same evidentiary position as a person who sends nothing. A source-driven record must preserve which state existed before escalating to committee action or Supreme Court process. [\[FN 279\]](#)

B. Later Deadlines, Committee Timing, and Physical Delivery

At least two Oct. 31 letters gave the attorney until Nov. 12 to respond and stated that only after nonresponse would the matters be forwarded to the grievance committee. Committee material identifies a Nov. 12 meeting. The Nov. 25 petition later represented that the committee met on Nov. 13. [\[FN 280\]](#)

The date difference is outcome-determinative. A deadline expiring Nov. 12 ordinarily permits a response through the deadline. A committee acting

that same day has no ordinary interval to receive, distribute, review, and evaluate a timely response before deciding the next step. Moving the meeting to Nov. 13 in the later narrative supplies an interval the earlier materials do not show. [\[FN 281\]](#)

The collision also interacts with the Oct. 14 response. The institution had acknowledged a consolidated response. Later letters created additional file-specific deadlines while the committee narrative advanced toward a nonresponse theory. ORACLE treats these as connected procedural-state changes, not isolated clerical imperfections. [\[FN 282\]](#)

The October 31 letters created additional file-specific response periods ending November 12 and represented that the matters would be forwarded only after nonresponse. Committee material identified a November 12 meeting, while the November 25 petition later stated November 13. The difference supplies or removes the interval in which a timely response could be received, distributed, reviewed, and considered before committee action. [\[FN 283\]](#)

The affected attorney also attempted to create a redundant physical channel. On November 4 he traveled from Miami to Florida Bar headquarters in Tallahassee and delivered updated responses and FBI-related correspondence. Later physical deliveries included forensic material and portal reports. Those acts do not by themselves prove how each document was processed, but they directly contradict a simple abandonment narrative and demonstrate that the target was attempting to bypass a disputed electronic rail. [\[FN 284\]](#)

Out-of-band conduct is particularly significant in an authority-rail incident. When the ordinary mailbox or portal is disputed, physical delivery can create an independently witnessed custody event. The receiving institution must then preserve who accepted the material, how it was routed, what file states were updated, and whether the later petition or committee record accounted for the delivery. [\[FN 285\]](#)

C. The November 25 Aggregated Nonresponse Petition

The November 25 petition aggregated thirteen inquiries into a single nonresponse theory and initiated the Supreme Court proceeding. The petition did not integrate the October 14 package, the October 15 acknowledgment, the physical deliveries, or the communicated cybersecurity context into the nonresponse narrative. It also used the 17F

identity whose chair and assignment path were already disputed in the source record. [\[FN 286\]](#)

The Authority-Rail conversion can therefore be stated precisely: acknowledged response became omitted response; omitted response became alleged nonresponse; alleged nonresponse became a Supreme Court petition; and the petition became the institutional source through which later readers understood the respondent's participation. Each downstream act carried genuine institutional authority. The unresolved issue is the missing transition from the acknowledged source state to the state presented in the petition. [\[FN 287\]](#)

That finding does not decide whether the response was substantively sufficient. It establishes that the later record did not preserve the prior state or identify the file-specific act by which receipt became nonresponse. The distinction is central to intent, notice, committee authority, and the reliability of every later characterization of nonparticipation. [\[FN 288\]](#)

The next Part moves from response accounting to authorship. By March 2025, the institutional communication stream itself contained direct statements that attributed messages had not been sent or had changed. That event converted the communication channel from a presumed neutral conduit into evidence requiring forensic authentication. [\[FN 289\]](#)

XII. Field Validation Three: When the Institutional Communication Channel Itself Became Evidence

The March 2025 sequence is not merely a dispute over whether one email was authentic. It is a test of what a legal system must do when an institutional participant repudiates one message and states that another message changed. At that point, sender display, domain, and visual appearance can no longer support ordinary presumptions of authorship without examining the native and provider-side evidence. [\[FN 290\]](#)

A. The Proposed Dismissal, Repudiation, and Immediate Disclosure

By January 2025, Randall L. Berman had replaced Womack in the Supreme Court matter. In March, a communication attributed to Berman proposed dismissal without prejudice on defined conditions, including an in-person meeting at the Fort Lauderdale branch and a short cure period for remaining materials. The attorney accepted the proposal and filed a motion seeking approval. [\[FN 291\]](#)

The Bar then disputed the communication. Berman denied creating or authorizing it. That denial establishes a contested-authorship event. It does not, without an attribution bridge, establish who created or altered the message. [\[FN 292\]](#)

The distinction became crucial because the later referee report converted the disputed communication into an affirmative finding that the attorney fabricated emails and a stipulation to mislead the Court. A finding of creation requires evidence connecting the message's origin or alteration to the accused actor. [\[FN 293\]](#)

The attorney's conduct after the dispute is directly material to intent. He did not conceal the disagreement or insist that the purported dismissal remain effective. He placed the authenticity problem before the Florida Supreme Court and requested a physical, source-traceable meeting to reconcile files and cure any identified deficiency. [\[FN 294\]](#)

That sequence is inconsistent with a plan to rely secretly on a knowingly fabricated agreement. It is consistent with a party who believed a message was genuine, learned that authorship was disputed, and sought an out-of-band method to determine which version was authentic. [\[FN 295\]](#)

The proposed in-person process also had a containment function. It would have allowed participants to compare source copies, identify missing matters, establish which addresses and accounts were controlled, and create a new acknowledged state outside the disputed mailbox stream. [\[FN 296\]](#)

The message attributed to Randall Berman proposed dismissal without prejudice on defined conditions, including an in-person meeting and a short cure process. The affected attorney accepted the represented terms and placed them before the Florida Supreme Court. When the Bar disputed authorship, he did not conceal the dispute or insist on the benefit of the purported dismissal. He informed the Court and requested a physical, source-traceable reconciliation. [\[FN 297\]](#)

That conduct is analytically important because authorship disputes often become intent disputes. A party attempting to exploit a knowingly fabricated agreement would be expected to conceal the uncertainty or force the benefit. Here the record shows disclosure of the dispute and a request for a process capable of comparing source copies, identifying missing files, and curing any remaining deficiency. [\[FN 298\]](#)

B. Berrena's Changed-Email Statement and the Missing Attribution Bridge

On Mar. 17, 2025, Berrena wrote that an email in the attorney's submission “was not the email I sent you” and “has been changed.” This is not an inference from formatting. It is an institutional participant's direct statement that the version in circulation differed from the message he said he sent. [\[FN 299\]](#)

That statement changes the proof environment. It establishes that alteration, substitution, unauthorized account use, or incompatible versions were active possibilities within the same stream. From that point forward, no later email-dependent finding could rest solely on ordinary assumptions about sender display, domain, or appearance. [\[FN 300\]](#)

The Bar's own public scam warnings reinforce the correct response: independently verify communications attributed to officials. The field response sought an in-person meeting and physical file reconciliation, which would have separated the human participants from the contested electronic path. [\[FN 301\]](#)

The disclosed sanctions record identifies no email-authorship expert, native-header attribution, provider-side mailbox audit, server log, endpoint artifact, or comparable forensic opinion tying creation or alteration of disputed messages to the attorney. [\[FN 302\]](#)

That absence does not prove the messages were genuine. It proves that affirmative attribution required a bridge the disclosed record did not identify. Berman's denial proves attributed authorship was disputed. Berrena's changed-email statement proves communications integrity was already compromised or irreconcilable. Neither identifies the attorney as creator. [\[FN 303\]](#)

ORACLE's determination is precise: the communications stream failed human-authorship authentication, and the later fabrication finding exceeded the disclosed technical attribution evidence. [\[FN 304\]](#)

Berrena's statement that an email was not the email he sent and had been changed established an integrity failure inside the same institutional stream later used to support a fabrication finding. The possible mechanisms included message alteration, unauthorized account use, storage divergence, substituted copies, or internal misunderstanding. The statement did not

identify which mechanism occurred, but it eliminated the premise that the channel could be treated as ordinary without further proof. [\[FN 305\]](#)

A categorical finding that a particular person created or altered the disputed communication required an attribution bridge. Relevant evidence could include native headers, message IDs, tenant audit logs, provider copies, mailbox access records, endpoint artifacts, file metadata, or expert analysis. The disclosed sanctions record did not identify such a bridge tying creation or alteration to the affected attorney. [\[FN 306\]](#)

Berman's denial established that the represented authorship was contested. Berrena's changed-email statement established that integrity failure was a live possibility. Neither fact, alone or together, identified the affected attorney as creator. ORACLE therefore finds that the communications stream failed human-authorship authentication and that the later fabrication finding exceeded the disclosed technical attribution evidence. [\[FN 307\]](#)

The field significance extends beyond this one email. Once an institution knows that its communication stream contains repudiated or changed messages, later findings concerning nonresponse, dishonesty, notice, or willfulness must account for that state. The appropriate response is preservation and independent verification, not continued reliance on the same disputed channel. [\[FN 308\]](#)

The next Part examines how disputed communications and attributed oral statements were converted into sworn emergency authority through the Berrena affidavit. [\[FN 309\]](#)

XIII. Field Validation Four: How Sworn Authority Amplified a Disputed Source Record

A sworn affidavit is an authority-bearing object. It tells the court that the affiant has taken responsibility for identified facts under oath, and it often allows the court to act without receiving live testimony at the initial stage. In an emergency-suspension proceeding, the affidavit can therefore transform disputed summaries and attributed statements into the evidentiary predicate for immediate professional exclusion. [\[FN 310\]](#)

A. Separating Personal Knowledge, File Review, and Attributed Statements

The June 18 Berrena affidavit was filed in support of an emergency-suspension petition. In that posture, the affidavit was not background commentary. It was an authority-bearing object used to convert disputed communications, collateral orders, complaints, and investigative summaries into a showing of present great public harm. [\[FN 311\]](#)

The affidavit combines several source classes. Berrena states personal facts about his employment. He reports what Berman told him about the disputed email. He reports what FBI agents allegedly told him. He authenticates documents in the Bar's possession. Each class has a different foundation and must be evaluated separately. [\[FN 312\]](#)

This separation matters because a sworn statement can cause downstream readers to treat every paragraph as direct knowledge. ORACLE reconstructs the provenance of each proposition rather than allowing the affidavit's form to flatten hearsay, file review, and personal observation into one evidentiary state. [\[FN 313\]](#)

The Berrena affidavit combined several source classes. Some paragraphs concerned the affiant's employment and tasks. Others reported what Berman said about the disputed email. Others reported what FBI agents allegedly said. Still others authenticated documents in the Bar's possession. Those categories did not share the same foundation merely because they appeared in one signed document. [\[FN 314\]](#)

The distinction matters because a decisionmaker can unconsciously treat an affidavit as one block of personal knowledge. ORACLE instead asks what the affiant observed, what he learned from another employee, what he derived from file review, what he attributed to federal agents, and what technical conclusion he drew. Each proposition should be tested against the most direct available source. [\[FN 315\]](#)

B. The FBI Summary Compared With Direct FBI Communications

The affidavit states that FBI agents advised the attorney that he had “no case” and that “no investigation was conducted.” It further states that the agents asked the attorney to stop copying them and that no investigation then existed. [\[FN 316\]](#)

Direct FBI communications from September 2024 document a different historical state. Federal agents met with the family, received devices and documentary material, provided or used a Teleporter upload path, discussed moving telephones to a computer-analysis response team, and indicated that uploaded material still required review. [\[FN 317\]](#)

Those communications do not establish that a formally numbered criminal investigation remained open on May 5, 2025. They establish investigative activity in ordinary language: meetings, intake, device-review planning, and continued examination of submitted evidence. The affidavit's categorical historical statement that no investigation was conducted is therefore impeached by the direct record. [\[FN 318\]](#)

The distinction is not semantic. The emergency petition used the affidavit to characterize repeated references to FBI involvement as false or unsupported. The direct communications show that the references were grounded in actual contacts and evidence intake, even if the Bureau later declined, closed, or never opened a formal case. [\[FN 319\]](#)

The affidavit also used the Berman email episode as proof of falsity without disclosing Berrena's own contemporaneous statement that another Bar email had changed. [\[FN 320\]](#)

That omission changes the reader's understanding. A decisionmaker told only that Berman denied the message may infer that the recipient invented it. A decisionmaker also told that the Bar investigator identified changed content inside the same stream must consider unauthorized account use, message alteration, storage divergence, or other integrity failures. [\[FN 321\]](#)

The omitted statement was material to the attorney's insistence on physical verification. It supplied institutional confirmation that the communication problem was not merely a subjective fear. [\[FN 322\]](#)

The affidavit stated that FBI agents told the affiant the attorney had no case and that no investigation was conducted. Direct September 2024 FBI communications document meetings, evidence intake, Teleporter uploads, contemplated transfer of telephones to a computer-analysis response team, and continuing review of submitted material. Those records establish investigative activity in ordinary language. [\[FN 323\]](#)

The direct record does not establish that a formally numbered criminal case remained open in May 2025 or that federal agents accepted every theory advanced by the reporting party. It establishes a narrower but

decisive fact: meetings, intake, planned device review, and continuing examination occurred. The categorical historical proposition that no investigation was conducted cannot be reconciled with that source record. [\[FN 324\]](#)

The affidavit also used the Berman-message episode as proof of falsity without disclosing Berrena's own contemporaneous statement that another email in the same stream had changed. A decisionmaker told only that counsel repudiated a message may infer recipient fabrication. A decisionmaker also told that the institution's investigator identified changed content must consider account misuse, message alteration, or version divergence before assigning authorship. [\[FN 325\]](#)

C. From Sworn Summary to Emergency Petition and Later Guilt State

Rule 3-5.2 is an extraordinary procedure because the Court may suspend before a full adversarial hearing when affidavit facts establish apparent great public harm. The reduced pre-suspension process gives the petition and affidavits exceptional authority. [\[FN 326\]](#)

Once the petition was approved, it became the formal complaint in the emergency case. Disputed summaries were converted into charging predicates; the case entered a referee process; and later default treated allegations as admitted. The affidavit therefore amplified upstream provenance decisions into downstream guilt and sanction states. [\[FN 327\]](#)

ORACLE does not ask whether an emergency procedure can ever rely on collateral orders or investigator affidavits. It finds that where an affidavit omits contradictory direct evidence and collapses source layers, the resulting authority rail carries a distorted state into every later step. [\[FN 328\]](#)

Rule 3-5.2 gave the affidavit exceptional downstream force. The petition and affidavits supported immediate suspension, became the operative formal complaint, and entered the referee process. After default, the allegations were treated as admitted and the final hearing focused on discipline. Upstream source choices therefore migrated into guilt and sanction states without a later merits record capable of correcting them. [\[FN 329\]](#)

ORACLE does not contend that an emergency petition can never rely on investigator affidavits, collateral orders, or attributed statements. It

determines that when the affidavit collapses source classes, omits contradictory direct evidence, and treats a disputed communication as proof of the recipient's fabrication without forensic attribution, the authority rail carries a distorted state into every later stage. [\[FN 330\]](#)

The next Part follows that authority into the referee proceeding, where notice, consolidation, case identity, default, a newly entered collateral order, and the final evidentiary record changed in a compressed sequence. [\[FN 331\]](#)

XIV. Field Validation Five: How Notice, Consolidation, Default, and New Evidence Changed the Adjudicative State

A referee proceeding is not a technical backend process. It is the trial-level environment in which pleadings become operative, deadlines become binding, evidence is received, default can determine guilt, and a report becomes the principal record presented to the Supreme Court. This Part reconstructs how the adjudicative state changed from emergency suspension to default and sanction. [\[FN 332\]](#)

A. Notice, Case Management, Consolidation, and Default

The two Supreme Court docket exports must be read together. The defined public entries show a July 1 notice of status conference in the earlier matter, the Aug. 4 emergency disposition, Aug. 5 referee appointment, Aug. 7 correction motion, and an Aug. 8 notice of compliance with discovery. They do not show a separately docketed notice setting an Aug. 8 case-management conference in the emergency matter. [\[FN 333\]](#)

The Aug. 11 order nevertheless states that a case-management conference occurred on Aug. 8 and that the attorney failed to appear. It then creates the answer and default architecture, treats the emergency petition as the operative formal complaint, and recites consolidation upon motion. [\[FN 334\]](#)

Notice is not a technical ornament when absence becomes the predicate for default. The source question is direct: what instrument told the respondent that a case-management conference would occur Aug. 8, through what service path, and to which verified address or account? The defined record contains the consequence and not the source notice. [\[FN 335\]](#)

The Aug. 11 order recites consolidation “upon motion” and governs the combined cases. The written Motion to Consolidate appears on the dockets

on Aug. 12, followed by an order and amended order granting consolidation. [\[FN 336\]](#)

The sequence matters because consolidation changed what pleading required an answer, which files were included, which prior response remained operative, which addresses were served, and how default would be measured. A consolidation cannot be treated merely as a caption change when the earlier case already contained responsive papers and a separate schedule. [\[FN 337\]](#)

The record also changes case identity during this period. The original emergency petition and order omitted 2025-70,622(17A)(FES). The Bar moved to correct on Aug. 7. The corrected public object and Sept. 30 clerk order added the identifier after the answer/default period and after the Sept. 3 default. [\[FN 338\]](#)

The Authority-Rail finding is not based on one typographical error. It is based on a sequence in which notice, consolidation, operative pleading, case identifier, service, and default changed in a compressed period without a single source-traceable bridge visible for the respondent. [\[FN 339\]](#)

The Sept. 3 default deemed matters admitted and limited the later hearing to discipline. Default converted allegations into established guilt without testimony from the respondent. [\[FN 340\]](#)

Correction of the emergency file identity followed that default. The current public order remains dated Aug. 4, is labeled “CORRECTED ORDER,” and carries a Sept. 30 footnote adding the FES file number. The Bar's public discipline page later labels that object an “Amended Supreme Court Order.” [\[FN 341\]](#)

A corrected case identifier can be administratively proper. The forensic issue is traceability: which version existed at each deadline, which version was served, how the original was preserved, and what authority changed the operative public object. The completed comparator work found that closest correction controls used a separately identified correction event, docket annotation, notice, or later instrument. [\[FN 342\]](#)

The two Supreme Court docket exports contain no separately docketed notice setting an August 8 case-management conference in the emergency matter. The August 11 order nevertheless states that the conference occurred, records the respondent's absence, establishes the answer and default structure, and recites consolidation upon motion. The written

Motion to Consolidate appears on August 12, followed by consolidation orders. [\[FN 343\]](#)

Notice is outcome-determinative because absence from the conference became part of the path to default. The source question is not whether a conference could be held. It is what instrument set the conference, how it was served, which verified address or account received it, and what record establishes that the respondent could know of the event. [\[FN 344\]](#)

Consolidation also changed more than the caption. It affected which petition operated as the formal complaint, which earlier responses remained relevant, which deadlines governed, which service population applied, and how default would be measured. An August 11 order that already treats consolidation as operative before the written motion appears therefore presents a state-sequence issue requiring a source explanation. [\[FN 345\]](#)

The September 3 default deemed allegations admitted and limited the final hearing to discipline. The emergency file identifier omitted from the June petition and August suspension order was later added through the correction sequence after default-related events had already occurred. The current public object remains dated August 4 while carrying the later correction footnote. [\[FN 346\]](#)

B. The September 30 Order, October 1 Hearing, and November 4 Report

The Middle District entered its dismissal/default disposition in Strenger on Sept. 30, 2025. The final disciplinary sanctions hearing occurred Oct. 1. The Nov. 4 referee report states that the referee took judicial notice that the federal court had imposed the ultimate sanction and entered default on the counterclaim. [\[FN 347\]](#)

The order could not have been part of the June 18 emergency petition because it did not exist. It could not have supported the Sept. 3 disciplinary default because it did not exist. It entered the disciplinary chronology after guilt had been established by default and one day before the sanctions hearing. [\[FN 348\]](#)

That timing affects notice and opportunity. A party cannot reasonably anticipate that a new collateral order will become a central feature of a sanctions report without an evidentiary or judicial-notice process identifying the order and permitting response. The Nov. 4 report's admitted-exhibit list identifies five affidavits and the S.D. Fla. dismissal

order; it does not list the Sept. 30 Middle District order among the six exhibits. [\[FN 349\]](#)

ORACLE therefore treats the Sept. 30 order as a temporal insertion into the authority rail. The later report used the order to reinforce the pattern narrative after the proceeding had already been defaulted and reduced to sanctions. [\[FN 350\]](#)

The Middle District entered the Strenger dismissal/default order on September 30, 2025. The disciplinary sanctions hearing occurred October 1. The order therefore did not exist when the June 18 emergency petition was filed and did not exist when guilt was established through the September 3 default. It entered the chronology after guilt and one day before the sanctions hearing. [\[FN 351\]](#)

The November 4 referee report states that the referee took judicial notice of the September 30 disposition. The report's admitted-exhibit list identifies five affidavits and a Southern District dismissal order; it does not list the September 30 Middle District order among the six admitted exhibits. The chronology therefore requires the reader to distinguish admitted evidence, judicial notice, and later narrative reliance. [\[FN 352\]](#)

The authority question is not erased by the fact that the September 30 document is a federal court order. The questions are when the order was introduced, what notice established its intended use, what opportunity existed to explain the circumstances, and how a post-default event became part of the basis for permanent professional exclusion. [\[FN 353\]](#)

By the time the report of referee was filed, disputed communications, investigator summaries, collateral orders, and source-order characterizations had acquired one integrated institutional signature. The next Part examines how the meaning of the underlying sources changed as they moved into that report and later public authority. [\[FN 354\]](#)

XV. Field Validation Six: How Authority Changes Meaning as It Is Repeated

Authority can be manipulated without altering the source document. A later actor can change the source's practical meaning by expanding, contracting, or reclassifying what the source said. This Part compares the originating texts with the propositions later attributed to them and then follows those derivative propositions into additional institutions. [\[FN 355\]](#)

A. From Draft Complaint to Filed-Litigation Conduct

The December 2024 Seminole judgment states that a written demand had a draft complaint attached that included relatives, a pastor, and a church as proposed parties. The Nov. 4 referee report later states that the attorney “filed frivolous lawsuits” against spouses, parents, and a pastor. [\[FN 356\]](#)

The propositions are materially different. A draft pleading attached to a demand is not the same event as filing separate lawsuits against each named person. The derivative report converted an unfiled draft-party list into filed litigation conduct and then used the expanded proposition within guilt and sanction analysis. [\[FN 357\]](#)

The Middle District comparison produces the same class of departure. The Feb. 18 and Mar. 19 orders criticized failures to appear and prosecute, rejected the authenticity challenge to the court's own order, and gave the client an opportunity to return the case to a merits path. The referee report attributed to the federal court an “ongoing pattern of weaponizing the court process,” filing frivolous claims to pressure settlement, and abandoning them. Those generalized settlement-pressure findings do not appear in the Feb. 18 or Mar. 19 source orders. [\[FN 358\]](#)

The source order contains strong criticism and must be stated accurately. Accuracy, however, does not authorize adding a separate scheme finding the source did not make. This is Recursive Institutional Authority Amplification in its clearest form: a later official report invokes the authority of an earlier court while changing the proposition attributed to that court, and the later report is then approved and published with a new institutional signature. [\[FN 359\]](#)

The December 2024 Seminole judgment described a demand accompanied by a draft complaint naming relatives, a pastor, and a church as proposed parties. The referee report later stated that the respondent filed frivolous lawsuits against spouses, parents, and a pastor. The first proposition concerns an unfiled draft attached to a demand; the second converts that draft-party list into completed filed litigation. [\[FN 360\]](#)

The transformation matters because filed litigation carries a different legal and reputational meaning from a draft pleading. Once the broader statement appears in an official disciplinary report, later readers are unlikely to return to the source judgment. The derivative proposition therefore becomes the practical institutional fact. [\[FN 361\]](#)

B. From Case-Specific Criticism to a Generalized Scheme

The February and March Middle District orders criticized failures to appear and prosecute, rejected the authenticity challenge to the court's own order, and provided a path to restore the case to a merits track. The referee report attributed to the federal court a broader finding of an ongoing pattern of weaponizing court process, filing frivolous claims to pressure settlement, and abandoning them. The completed source comparison found that the generalized settlement-pressure scheme did not appear in those source orders. [\[FN 362\]](#)

The source orders contain strong criticism, and the report must state it accurately. Accuracy does not authorize adding a separate behavioral scheme and assigning that scheme to the source court. The Authority-Rail issue is the transfer of judicial authority: the later report invokes the prestige of the federal court while expressing a proposition the source did not make. [\[FN 363\]](#)

C. Recursive Institutional Authority Amplification

Every authority chain begins with a proposition. It may be a fact observed by a witness, an allegation in a pleading, a statement in an affidavit, a finding in an order, or a representation in a news article. The first discipline of authority-rail analysis is to identify which category the source actually occupies. [\[FN 364\]](#)

A derivative authority changes the proposition when it converts allegation into finding, background into holding, draft conduct into completed conduct, or one-case criticism into a generalized behavioral scheme. The change can occur through paraphrase rather than quotation. It can also occur through omission, such as leaving out procedural posture, contrary evidence, or the time at which the source became available. [\[FN 365\]](#)

The resulting text may be persuasive because it carries a more authoritative signature than the original. A referee report summarizing a federal order appears to state what the federal court found. A Supreme Court order approving the report appears to adopt the summary. A public Bar page then presents the sanction as the profession's canonical state. [\[FN 366\]](#)

ORACLE therefore uses a source-to-derivative matrix. The first column reproduces the source proposition. The second reproduces the derivative proposition. The third identifies the change: expansion, contraction, omitted posture, altered timing, changed actor, or changed legal state. The fourth records the downstream consequence. [\[FN 367\]](#)

Official publication converts internal adjudicative state into public identity. The public rarely reads the complete record. It relies on the regulator's profile, court's docket text, final order, or first search result. [\[FN 368\]](#)

The Florida Bar profile reports permanent disbarment dated May 21, 2026. The associated discipline-document page lists the referee report, an item labeled “Amended Supreme Court Order,” and the emergency petition. The item labeled as the Supreme Court order opens the corrected Aug. 4, 2025 emergency-suspension order rather than the May 21 terminal instrument. [\[FN 369\]](#)

The completed comparator study inspected sixteen permanent-disbarment document pages and found that each supplied the terminal Supreme Court order. The field page was the only directly inspected permanent-disbarment page reporting the terminal status while omitting the terminal instrument. [\[FN 370\]](#)

This is not merely a broken web link. The profile is consumed as a professional identity source. Courts, employers, insurers, banks, clients, licensing bodies, reporters, and search engines use it to answer what happened and why. Directing those users to the interim corrected suspension order changes the publicly available provenance of the terminal state. [\[FN 371\]](#)

Search engines do not independently adjudicate source accuracy. They rank and summarize what authoritative pages publish. A regulator's profile, court order, or major newspaper article can therefore dominate exact-name results and become the practical identity record for people who never inspect the underlying sources. [\[FN 372\]](#)

Media can acquire authority from courts. In Strenger, the news report was brought to the court's attention by opposing counsel and later cited in the Mar. 19 order. The article's proposition thereby entered a judicial document. A later reader could treat the court's citation as independent confirmation

even though the order identified the report as background supplied during the conference. [\[FN 373\]](#)

The process can reverse. Media may report a court characterization, search engines may rank the story, and later litigants may cite the story or search result. The same proposition circulates through different institutional forms until its common origin is obscured. [\[FN 374\]](#)

The correct analysis is dependency mapping. A source is independent only if it derives from a separate evidentiary object or investigation. A newspaper repeating an order, a profile repeating a sanction, and a later court repeating the newspaper do not create three independent proofs. They create three authority handoffs. [\[FN 375\]](#)

Recursive amplification begins when the derivative authority is cited as independent confirmation. A media article can be introduced by opposing counsel and later cited in a judicial order. The judicial order can be quoted by another tribunal. A referee report can characterize the prior order. A Supreme Court disposition can approve the report. A licensing profile can publish the sanction. Search engines can rank the official profile, order, article, and derivative pages together. [\[FN 376\]](#)

The chain creates the appearance of a large and independent evidence stack. Dependency mapping often reveals that several nodes trace to the same upstream proposition or to a later paraphrase of it. ORACLE therefore asks not how many pages repeat the statement, but how many independent source objects establish it. [\[FN 377\]](#)

This analysis does not diminish the authority of courts or regulators. It protects that authority by distinguishing what the source actually decided from what a later actor attributed to it. The institution remains trustworthy when its findings can be traced to the evidence and procedural state that created them. [\[FN 378\]](#)

The next Part examines the final amplification layer: publication, media, professional profiles, and search systems that carry authority to readers who will never inspect the underlying record. [\[FN 379\]](#)

XVI. Publication, Media, and Search as Authority Multipliers

Legal consequences do not remain inside the adjudicative file. Public profiles, news articles, author pages, derivative websites, and search indexes become the interfaces through which most people encounter the result.

Those publication systems therefore operate as authority rails in their own right. [\[FN 380\]](#)

A. The Terminal Professional Profile

The public-profile anomaly is the final observable state in the field chronology. The earlier proceeding contains disputed complaint provenance, response accounting, committee authority, communications authorship, emergency-petition source layers, notice, consolidation, default, collateral-order use, review, and transcript issues. The public page compresses that path into one terminal status. [\[FN 381\]](#)

A complete terminal chain would allow the user to move from the status to the order imposing it and from that order to the record and findings supporting permanent exclusion. The current page instead supplies the corrected interim suspension order. [\[FN 382\]](#)

ORACLE finds that this is a publication-and-reputation rail failure. The defect does not erase the existence of a May 21 artifact elsewhere in the corpus. It means the authoritative public path through which the profession directs users to supporting documents does not provide the terminal instrument it reports. [\[FN 383\]](#)

The Florida Bar profile reports permanent disbarment effective May 21, 2026. The linked discipline-document page omits the May 21 terminal instrument and presents the corrected August 4, 2025 emergency-suspension order under the label 'Amended Supreme Court Order.' The direct comparator study found that each of the other inspected permanent-disbarment pages supplied the terminal Supreme Court instrument. [\[FN 384\]](#)

The issue is not whether a May 21 artifact exists elsewhere in the corpus. It is whether the authoritative public path through which the Bar directs users to supporting documents supplies the instrument imposing the terminal state it reports. That path is relied upon by courts, employers, clients, licensing bodies, insurers, banks, media, and search engines. [\[FN 385\]](#)

When the public status and supporting instrument do not match, the unresolved provenance state migrates beyond the disciplinary record. The public user receives the conclusion without the terminal source that should explain its legal basis, case identity, participating justices, costs, and relationship to the earlier emergency suspension. [\[FN 386\]](#)

B. Byline, CMS, Republished Content, and Search Authority

A journalistic byline operates as a credential. It tells the reader that a particular person, newsroom, and editorial process stand behind the article. A biography, photograph, email address, telephone number, social account, and publication history reinforce that trust. [\[FN 387\]](#)

The preserved Wieder materials contain several layers. They show an apparent McClatchy/Miami Herald professional identity, author pages, a Washington-bureau description, a public telephone contact, social-media presentation, a Proton tips address, and an email presentation using ben.wieder@mcclatchydc.com. They also preserve disputed calls, alternate numbers, derivative publication pages, and image associations requiring source-level reconciliation. [\[FN 388\]](#)

ORACLE does not reduce that record to a claim that the natural person is fictional. The correct question is event-specific: who controlled the telephone path, email account, social account, byline, article object, or derivative page at each time? [\[FN 389\]](#)

The April 2, 2024 social-media post is a source-state anchor. It records that the account represented that it had been investigating unusual foreclosure cases involving a Florida lawyer for months. The post establishes what the account publicly claimed on that date. It does not, standing alone, authenticate the human operator. [\[FN 390\]](#)

A content-management system controls article creation, author assignment, publication time, updates, images, and metadata. Access to a CMS account can therefore create genuine publication objects under a real outlet's domain and byline. [\[FN 391\]](#)

Syndication and republication create another mechanism. An authentic article can be copied to a derivative site with the original byline and biography intact. The derivative operator can insert a new graphic, headline, or contextual claim around the copied text. The real author and outlet supply the trust, while the wrapper supplies the new message. [\[FN 392\]](#)

The PPPFraudChronicle captures demonstrate this authority-transclusion problem. The page presented Miami Herald-derived content and Wieder's biography while displaying site-specific branding and a “Swindler Barbie” graphic concerning a member of Congress. The analytical question is which

components originated in the canonical article and which were added by the derivative site. [\[FN 393\]](#)

This mechanism does not require a newsroom compromise. It requires only the ability to copy authoritative content and bind it to new material in a way that causes the reader to attribute the entire package to the original author. [\[FN 394\]](#)

Professional directories, award pages, biographies, Bar profiles, and firm websites act as distributed identity proof. A hiring manager, client, court, or reporter rarely verifies every field with the original institution. Consistency across several sites creates confidence. [\[FN 395\]](#)

Threat actors can exploit that confidence through credential laundering. A weak or stolen credential is repeated across reputable platforms until the repetitions appear independent. Paid profiles, copied biographies, expired domains, and self-claimed admissions can form a professional echo chamber. [\[FN 396\]](#)

The defensive method is historical and relational. Investigators should establish the earliest archived appearance, source of each claim, profile-creation or modification date, domain ownership, organization confirmation, and same-name collisions. An isolated sparse profile is not proof of fraud. A synchronized cluster of new profiles, role changes, domains, and communications around an operational event carries greater weight. [\[FN 397\]](#)

Search engines stack authority by ranking repeated and high-reputation sources. A court, regulator, media outlet, directory, and social profile can occupy the first page for an exact name. The reader experiences the stack as corroboration. [\[FN 398\]](#)

ORACLE calls this authority stacking. It occurs when several ranked results express the same proposition but are not independent. One article may cite a court order; the profile may cite the discipline case; a derivative page may copy the article; and a later post may link them all. [\[FN 399\]](#)

The investigator must trace each result backward. Which source first introduced the proposition? Which later results copied it? Which source had access to primary evidence? Which changed the wording or image? Which became the canonical search result? [\[FN 400\]](#)

Authority stacking is especially damaging in cAPtUre-to-Kill because reputational harm reduces the target's ability to obtain counsel, clients, credit, employment, media attention, and institutional belief while the technical incident remains active. [\[FN 401\]](#)

The Wieder materials illustrate why the media rail must be analyzed event by event. The corpus contains evidence of an apparently real journalistic identity and history, together with disputed calls, alternate contact paths, derivative publication wrappers, and inconsistent image associations. ORACLE does not treat the natural person's existence as proof of each act. It asks which human, account, telephone path, byline, CMS credential, derivative site, or search result carried authority at the relevant time. [\[FN 402\]](#)

A content-management system can create genuine objects on a genuine outlet domain under a genuine byline. A derivative site can copy authentic reporting and biography while surrounding it with new graphics, headlines, or commentary. Those are different mechanisms, but both exploit the reader's reliance on the byline and publication brand. [\[FN 403\]](#)

The PPPFraudChronicle captures are useful because they preserve Miami Herald-derived content and author biography inside a separately branded site containing additional visual messaging. The forensic task is to separate canonical article content from material added by the derivative publisher. No newsroom compromise is required for the derivative wrapper to borrow the authority of the original journalist. [\[FN 404\]](#)

The media rail becomes recursive when reporting enters court. In Strenger, opposing counsel brought a news report to the court's attention, and the March order later cited the Miami Herald URL. A later reader can encounter the proposition inside a judicial document and treat it as court-supported, even though the order identifies the article as background supplied during the conference. [\[FN 405\]](#)

Search indexing completes the stack. The official profile, judicial orders, news article, derivative pages, and social posts can occupy the same exact-name results. Repetition appears to be corroboration, but the results may depend on the same upstream source or derivative characterization. Reputational containment therefore requires dependency mapping and correction of the authoritative source first. [\[FN 406\]](#)

The next Part addresses the institutional problem exposed by every field sequence: when the ordinary filing, service, or communication rail is itself disputed, the target needs a controlled path through which the integrity claim can be tested without depending exclusively on the challenged channel. [\[FN 407\]](#)

XVII. Why a Compromised Authority Rail Requires a Clean Adjudicative Environment

An authority-rail incident creates a circular procedural problem. The affected person must use a filing, service, identity, or communication system to prove that the same system is compromised. If the filing fails, the person appears noncompliant. If the filing arrives but is processed as ordinary advocacy, the integrity question can be rejected without source-object preservation or technical examination. If the person changes channels, the protective conduct can be characterized as irregular. [\[FN 408\]](#)

A. The Clean Adjudicative Environment

The Civil Cyber-Infrastructure report examined how private plaintiffs developed court-authorized methods to disrupt malicious infrastructure. Those cases succeeded because technical evidence was converted into precise commands for registries, registrars, hosts, cloud providers, and neutral intermediaries. [\[FN 409\]](#)

The same history exposes a modern vulnerability. The remedy depends on counsel communications, expert reports, sealed filing, clerk intake, service, provider instructions, publication, and later enforcement. Those trusted steps are observable and can become targets. [\[FN 410\]](#)

A Clean Adjudicative Environment is a narrow integrity bridge for the exceptional case in which credible evidence places the ordinary channel itself in dispute. It requires independent identity verification, source-object preservation, known-clean intake, controlled technical review, dual-channel confirmation, and reconciliation back into ordinary adversarial process. [\[FN 411\]](#)

The concept does not authorize a private party to bypass judges, filing rules, service, or due process. It gives the institution a controlled way to determine whether the channel carrying the integrity challenge is itself compromised. [\[FN 412\]](#)

A Clean Adjudicative Environment is a narrow integrity bridge. It preserves judicial control while allowing independent identity verification, known-clean intake, source-object preservation, controlled technical review, dual-channel confirmation, provider authentication, and reconciliation back into the ordinary adversarial record. It is not a private bypass around rules or decisionmakers. [\[FN 413\]](#)

The concept draws from two established practices. Civil cyber-disruption cases translate technical evidence into precise, court-authorized commands for neutral providers. Highly sensitive document procedures recognize that ordinary electronic filing is not appropriate for every evidence object. ORACLE applies the same institutional logic when credible evidence places the ordinary legal control plane itself in dispute. [\[FN 414\]](#)

B. Cross-Jurisdiction Field Tests

The S.D. Florida field record includes emergency filings seeking relief from active cyber interference, requesting controlled presentation, and later attempting to present broader cAPtUre evidence. The filings entered ordinary intake channels notwithstanding the allegation that communications and filing systems were being manipulated. [\[FN 415\]](#)

The operational problem is circular. To prove that the filing or service rail is compromised, the claimant must successfully use the same rail. A filing that is delayed, misrouted, rejected, associated with a different case state, or publicly dismissed before secure review can become evidence against the claimant rather than evidence about the channel. [\[FN 416\]](#)

The result is not simply denial of one motion. It is loss of a meaningfully timed containment opportunity while the operation continues. [\[FN 417\]](#)

The E.D.N.Y. field test attempted to use the standing permanent injunction in Microsoft/Fortra/Health-ISAC to address alleged successor infrastructure. The filing sought controlled technical review and coordination with the plaintiff-side capability that had developed the original disruption action. [\[FN 418\]](#)

The public docket documented the filing and a direction that plaintiffs respond. The defined search through the report cutoff did not locate a public technical adjudication of successor criteria, monitor process, or reproducible disposition explaining whether the later-victim evidence qualified. [\[FN 419\]](#)

The test demonstrates a State Four problem: a powerful permanent remedy can exist while later victims lack a visible, authenticated, and timely path to invoke it. [\[FN 420\]](#)

The D.D.C. field record sought a controlled evidence path for cyber-sensitive material. The issue was not a request for secret merits adjudication. It was a request to preserve and present integrity evidence without exposing it through the same channels alleged to be compromised. [\[FN 421\]](#)

The filed/unfiled boundary becomes decisive in such a case. A court can act only on a record it receives, but the claimant's allegation concerns whether the ordinary intake process will preserve the object and identity correctly. [\[FN 422\]](#)

The Florida field test included a Dec. 27, 2024 motion for protective order and confidentiality, physical delivery of portal reports, a Feb. 6, 2026 original-jurisdiction writ, and an emergency request for secure or in-camera handling. [\[FN 423\]](#)

The writ did not receive a separate original-proceeding identity in the defined record. The emergency secure-handling motion was denied inside the disciplinary docket, and later review proceeded through the same transcript, service, and case-identity environment challenged by the filing. [\[FN 424\]](#)

The field result is not silence in the sense of no effort. The attorney used electronic filing, physical filing, hand delivery, redundant addresses, an original writ, and a secure-handling request. The institution did not create an independently authenticated channel in which the integrity evidence could be tested outside the disputed rail. [\[FN 425\]](#)

Across the field tests, requested relief varied, but the operational condition repeated. The claimant alleged that filing, service, identity, routing, record custody, or communications were compromised and then had to use those systems to prove it. [\[FN 426\]](#)

The absence of an out-of-band rail benefits the attacker. If the filing fails, the target appears noncompliant. If the filing succeeds but is processed as ordinary advocacy, the technical allegation can be dismissed without controlled examination. If the target changes channels, the change can be characterized as unusual or evasive. [\[FN 427\]](#)

ORACLE finds that authority avatars reach maximum effectiveness when the institution accepts the false state and the target lacks a clean path to challenge it before default, sanctions, publication, or reputational propagation. [\[FN 428\]](#)

The Southern District filings sought emergency relief and controlled presentation while alleging that communications and filing systems were being manipulated. The Eastern District filing sought later-victim access to a standing civil cyber-disruption remedy and controlled technical review of alleged successor infrastructure. The District of Columbia matter sought a controlled path for cyber-sensitive material. The Florida Supreme Court record includes physical delivery, protective and confidentiality requests, portal reports, an original-jurisdiction writ, and a secure-handling request. [\[FN 429\]](#)

The specific relief and procedural posture differed, but the operational condition repeated: the integrity claim had to traverse the same intake, service, routing, or docket environment placed in dispute. The defined records did not produce one independently authenticated channel in which source objects could be compared and the resulting state reconciled before deadlines, default, sanction, or publication. [\[FN 430\]](#)

ORACLE therefore determines that the availability of a clean integrity path is itself a security control. Courts and regulators need not accept the claimant's attribution theory to preserve the evidence and authenticate the channel. They need a procedure capable of deciding whether the ordinary state can be trusted before that state becomes irreversible. [\[FN 431\]](#)

The next Part converts the report's findings into a repeatable Authority-Provenance Detection Method that can be used by lawyers, courts, regulators, and cyber responders before the incident reaches terminal consequence. [\[FN 432\]](#)

XVIII. The ORACLE Authority-Provenance Detection Method

ORACLE's value depends on whether the method can be used during an active incident. The detection method is designed to prevent investigators from stopping at official appearance. It begins with the ordinary state, moves through identity and authority, and ends with the institutional and public consequences that must be contained. [\[FN 433\]](#)

A. Establish the Ordinary State and the Event-Level Authority

First define what should ordinarily exist. Identify the case, complaint, account, role, committee, service list, public profile, and current procedural state before examining the disputed event. Without that baseline, an investigator cannot distinguish a malicious transition from an authorized change, ordinary template reuse, or administrative correction. [\[FN 434\]](#)

Then identify the represented actor and event-specific authority. Confirm the natural person through independent records, but do not stop there. Determine which account, device, number, profile, or domain performed the act; which role was claimed; what appointment, retainer, roster, delegation, or representation record established the role; and whether the natural person confirmed the event through a known-clean path. [\[FN 435\]](#)

Identify the credential or authorization object accepted by the system: password, session, OAuth grant, API key, certificate, device registration, mailbox permission, service principal, or delegated role. Review issuance, recovery, privileged changes, registered devices, and revocation. The objective is to separate 'the account acted' from 'the intended human and authorized role acted.' [\[FN 436\]](#)

B. Preserve and Compare the Communication and Source Object

Preserve the native message, headers, message ID, attachment hashes, sender and recipient copies, provider copy, mailbox and tenant logs, call records, voicemail, and the visible rendering. For a filing, preserve the local file, upload receipt, filing number, PageID, service notice, docket copy, public copy, and any restricted or chambers copy that can be lawfully obtained. Screenshots preserve appearance but do not replace native evidence. [\[FN 437\]](#)

Compare versions before assigning authorship. A changed display, reformatted body, replaced attachment, different recipient population, or different file hash identifies the point at which the rail may have changed. When an institutional participant states that a message was not the one sent or was changed, preserve both versions and request provider-side evidence before the logs age out. [\[FN 438\]](#)

For source propositions, reproduce the actual source language and the derivative language. Classify the change: allegation to finding, draft to

completed conduct, one-case criticism to generalized scheme, changed actor, altered timing, or omitted procedural posture. The method prevents institutional prestige from substituting for source fidelity. [\[FN 439\]](#)

C. Reconstruct the State Transition and Downstream Reliance

Document the before state, transition instrument, notice, deadline, authority, after state, and first downstream actor that relied on it. Ask what the affected party could know and answer at the time. A later state is not self-authenticating merely because it appears on a real docket or official profile. [\[FN 440\]](#)

Map derivative propagation. Determine whether the disputed state reached another court, regulator, client, insurer, provider, media organization, professional directory, repository, or search index. Identify which later sources are independent and which merely repeat the same upstream proposition. [\[FN 441\]](#)

Assign confidence separately to the event, mechanism, and attribution. The record may conclusively establish that a message version changed while leaving the operator unresolved. It may establish that a role assignment lacks a source instrument while leaving open whether the cause was error, account compromise, or document substitution. Clear separation allows the institution to correct the state without waiting for perfect attribution. [\[FN 442\]](#)

D. Verify Through a Known-Clean Channel and Correct the Authority State

Out-of-band verification must use contact information obtained independently of the disputed message. Calling a number supplied inside the suspicious communication does not leave the rail. High-consequence confirmations should be memorialized: who confirmed, through which channel, at what time, and against which source object. [\[FN 443\]](#)

Containment must address the accepted institutional state. Changing a password does not correct a docket; revoking a token does not restore a missed deadline; removing a mailbox rule does not change a public professional profile; and reimaging a device does not retract a derivative article. Technical remediation and legal-state correction must proceed together. [\[FN 444\]](#)

The detection method now leads directly to meaningfully timed response. The next Part explains what the legal and technical team must produce in the first hours and days to preserve business, representation, evidence, deadlines, and professional identity while attribution continues. [\[FN 445\]](#)

XIX. Meaningfully Timed Response: Preserving Business and Legal Capacity While the Incident Is Active

The governing operational principle is containment before autopsy. A complete forensic explanation may require provider process, cloud logs, discovery, or months of correlation. Legal and professional consequences can occur in hours. The response must preserve evidence and protect authority while the incident is still capable of being contained. [\[FN 446\]](#)

A. The First Six Hours: Preserve Source State and Establish Clean Contact

The first six hours determine whether authority evidence survives. The team should preserve native email files and headers, text exports, call logs, voicemail, portal receipts, docket captures, local copies, attachment hashes, sign-in logs, token and device state, DNS and MX records, and the current public profile or article. Screenshots alone are insufficient where native objects exist. [\[FN 447\]](#)

The organization must establish a clean contact path not dependent on the disputed account. The path can include an independently obtained telephone number, in-person verification, a known-clean device, a separate tenant, or a prearranged incident contact. [\[FN 448\]](#)

The legal team must identify clocks immediately: hearings, filing deadlines, service periods, client emergencies, regulatory obligations, insurance notice, preservation duties, and publication windows. A technically small delay can create default or reputational propagation. [\[FN 449\]](#)

The authority inventory should begin at once. Which people and accounts can file, sign, publish, change DNS, alter a service list, recover a mailbox, speak for the institution, or update a professional profile? The answer defines the initial containment perimeter. [\[FN 450\]](#)

The first deliverable is a native evidence package, not a screenshot folder. Preserve messages and headers, text exports, call logs, voicemail, portal receipts, filing confirmations, docket captures, attachment hashes, sign-in

history, token and device state, mailbox rules, DNS and MX records, cloud roles, and the current public profile or article. Record the collection method and time zone. [\[FN 451\]](#)

The second deliverable is a clean-contact roster. Identify independently obtained numbers, in-person contacts, known-clean devices, alternative tenants, and prearranged incident contacts for clients, courts, regulators, insurers, providers, and counterparties. The organization must know how to communicate if the ordinary domain and telephone path cannot be trusted. [\[FN 452\]](#)

The legal team must simultaneously create a critical-clock sheet. Hearings, filing deadlines, service periods, client emergencies, insurance notice, preservation duties, regulatory demands, and publication windows can convert a short technical interruption into default or irreversible reputational propagation. [\[FN 453\]](#)

B. Six to Twenty-Four Hours: Build the Authority Map and Preserve Institutional Evidence

By twenty-four hours, the response team should produce an authority map. It identifies the represented actor, natural person, account, credential, role, institution, channel, source object, before state, after state, recipient, and consequence for each material event. [\[FN 454\]](#)

The map should distinguish confirmed, disputed, and unauthenticated relationships. A real employee with a disputed email is different from an unknown person using a lookalike domain. A valid portal login with no device attribution is different from a failed authentication attempt. [\[FN 455\]](#)

The team should notify affected institutions through known-clean channels and request preservation before logs expire. The notice should identify the exact account, message ID, filing number, or record object rather than send a broad narrative difficult to operationalize. [\[FN 456\]](#)

Out-of-band verification must use contact information obtained independently of the disputed message. Calling the number provided inside the suspicious email does not leave the rail. [\[FN 457\]](#)

High-consequence verification should create a new record: who confirmed, through what channel, at what time, and which source object was compared. A verbal confirmation should be memorialized. An in-person review should identify the documents examined and custody path. [\[FN 458\]](#)

Where a court or regulator is involved, the organization should request a controlled intake method proportionate to the risk. The request should be narrow, identify the challenged channel, preserve judicial control, and propose reconciliation back into the ordinary record after authentication.

[\[FN 459\]](#)

The authority map identifies the represented actor, natural person, account, credential, role, institution, channel, source object, before state, after state, recipient, and consequence for each material event. It distinguishes confirmed, disputed, and unauthenticated relationships rather than using one global 'compromised' label. [\[FN 460\]](#)

Preservation notices should identify exact objects: account, message ID, filing number, date range, hosted zone, profile record, CMS article ID, or portal event. Broad narrative requests are difficult to operationalize and can allow short-lived logs to expire while recipients determine what the requester means. [\[FN 461\]](#)

Affected institutions should receive a concise integrity notice through a known-clean path. The notice should state the challenged channel, identify the exact event, request preservation, and propose a controlled verification process without asking the recipient to accept the entire attribution theory.

[\[FN 462\]](#)

C. Twenty-Four to Seventy-Two Hours: Reconstruct State and Contain Consequence

By seventy-two hours, the team should reconstruct each outcome-determinative transition. What was the state before the event? What instrument changed it? Who had authority to issue that instrument? What credential was used? Who received it? What later system adopted it? [\[FN 463\]](#)

The reconstruction must compare copies. The sender copy, provider copy, recipient copy, filed object, docket object, public copy, archive copy, and printed or hand-delivered copy may differ. [\[FN 464\]](#)

The team should identify derivative propagation. Has the disputed state reached a regulator profile, court order, opposing filing, client communication, media article, repository, or search index? Correction strategy depends on how far the authority rail has carried the state. [\[FN 465\]](#)

Continuity requires more than restoring email. Clients need a verified contact path. Courts need accurate service information. Staff need to know

which instructions are authentic. Providers need preservation requests. Insurers need timely notice. Public-facing records may require qualification or correction. [\[FN 466\]](#)

The response team should assign one authority coordinator tracking institutional state and one technical coordinator tracking accounts, infrastructure, and evidence. The functions must remain synchronized because technical remediation can fail if the docket or profile remains corrupted, and legal correction can fail if the account remains controlled. [\[FN 467\]](#)

Meaningfully timed relief is the governing principle. The objective is to preserve the business, representation, evidence, and access to decisionmakers while the incident is active—not to produce a perfect cyber autopsy after the target has lost everything. [\[FN 468\]](#)

By seventy-two hours, the team should have a source-state ledger showing the last authenticated state, the purported transition, the authority claimed, the copies compared, the downstream reliance, and the confidence assigned to event, mechanism, and attribution. That ledger becomes the common operating picture for counsel, forensic responders, executives, and affected institutions. [\[FN 469\]](#)

The continuity plan must preserve representation and operations. Clients need a verified path to counsel; courts need accurate service information and deadline protection; staff need verified instructions; providers need preservation and access-revocation requests; insurers need timely notice; and public records may need qualification before the disputed state becomes canonical. [\[FN 470\]](#)

The correction strategy should begin at the authoritative source. Correcting a derivative article while the official profile remains wrong will not restore professional identity. Correcting a mailbox while a docket state remains unchallenged will not restore legal capacity. The team must identify which source object controls each downstream dependency. [\[FN 471\]](#)

D. Three to Seven Days and Ongoing: Reconcile, Publish, and Monitor

During the following days, the team should reconcile provider and portal records, communicate the authenticated state to clients and institutions, seek controlled correction of public and adjudicative records, and document

unresolved questions. Versioned findings allow the organization to correct a determination without erasing the evidence state that existed earlier. [\[FN 472\]](#)

Ongoing monitoring should focus on re-entry and authority recurrence: new tokens, delegated roles, forwarding rules, recovery changes, profile updates, service-list changes, derivative publications, and repeated source propositions. Technical and publication monitoring must remain synchronized because the operation can persist through institutional state after access is revoked. [\[FN 473\]](#)

Meaningfully timed relief is achieved when the business, representation, evidence, deadlines, and professional identity remain functional while the investigation matures. The next Part assigns the corresponding responsibilities to courts, regulators, law firms, cybersecurity providers, media organizations, and identity systems. [\[FN 474\]](#)

XX. Institutional and Industry Recommendations

The Authority-Rail problem cannot be solved by the targeted professional alone. The rail is distributed across institutions, providers, accounts, records, and publication systems. Each participant therefore needs controls matched to the authority it contributes. [\[FN 475\]](#)

A. Courts, Clerks, Bars, and Regulators

Courts should maintain a narrowly defined integrity-escalation protocol for credible claims involving filing identity, service, sealed documents, docket-object divergence, or compromised credentials. The protocol should preserve judicial control while allowing known-clean intake and technical review. [\[FN 476\]](#)

High-consequence changes should produce visible provenance: corrected orders, changed service lists, consolidation, reassignment, sealed-to-public transitions, and docket replacement should identify the authorizing event and preserve the prior state. [\[FN 477\]](#)

Courts should distinguish account authentication from human authorship. Where a filing's authorship is contested and outcome-determinative, provider logs, portal audit, device evidence, and native objects should be preserved before attribution is made. [\[FN 478\]](#)

Regulators should authenticate complaint origin, response receipt, committee assignment, role, conflict, and file transfer as separate states. An acknowledged response should not become nonresponse without a file-specific transition record. [\[FN 479\]](#)

Role assignments should be verifiable through current rosters and source instruments. Form libraries and signature images should be access-controlled, logged, and monitored for reuse outside ordinary workflows. [\[FN 480\]](#)

Public profile pages should link the terminal instrument supporting the reported status and preserve corrected or superseded objects through transparent versioning. [\[FN 481\]](#)

Courts and clerks should maintain a narrow integrity-escalation protocol for credible claims involving filing identity, service, sealed materials, docket-object divergence, or compromised credentials. The protocol should preserve judicial control while allowing known-clean intake, technical preservation, and reconciliation back into the ordinary record. [\[FN 482\]](#)

Outcome-determinative state changes should preserve provenance. Corrected orders, changed service lists, consolidation, reassignment, sealed-to-public transitions, and docket replacement should identify the authorizing act and preserve the prior state. Version transparency is both a due-process control and a cybersecurity control. [\[FN 483\]](#)

Bars and regulators should authenticate complaint origin, response receipt, committee assignment, role, conflict, file transfer, probable-cause action, and public-status publication as separate states. Once receipt is acknowledged, later nonresponse should require a file-specific deficiency or transition record. Public profiles should link the terminal instrument supporting the status displayed. [\[FN 484\]](#)

B. Law Firms, Legal Departments, and Cybersecurity Providers

Law firms should maintain an authority inventory: filing accounts, Bar profiles, domain and DNS administrators, mailbox delegates, cloud roles, signature repositories, service addresses, social and media accounts, and emergency contacts. [\[FN 485\]](#)

Incident plans should include legal-workflow continuity. The firm must know how to notify clients, courts, opposing counsel, regulators, insurers,

and vendors through known-clean channels while preserving privilege and evidence. [\[FN 486\]](#)

Firms should train personnel to recognize authority anomalies rather than only malicious attachments. A message can be dangerous because the role is impossible, recipient set is wrong, source proposition changed, or timing does not permit the represented state. [\[FN 487\]](#)

Security providers should add legal control-plane analysis to incident response. Endpoint telemetry alone will not reveal that a response became nonresponse, a profile linked the wrong order, or a court cited a derivative media proposition. [\[FN 488\]](#)

The provider should work with counsel to identify authority-bearing events and preserve logs necessary to attribute them. Identity, token, mailbox, DNS, portal, and publication evidence should be correlated with hearings, filings, deadlines, and institutional decisions. [\[FN 489\]](#)

This is a complementary specialty. Traditional DFIR determines how the account or system was accessed. ORACLE determines what legal, procedural, and reputational authority the access changed and how to contain that consequence before it becomes accepted history. [\[FN 490\]](#)

Law firms should maintain an authority inventory covering filing accounts, professional profiles, domain and DNS administrators, mailbox delegates, cloud roles, signature repositories, service addresses, social and media accounts, client portals, and emergency contacts. Incident plans should describe how verified communication and filing will continue when the ordinary domain, phone, or portal path is not trusted. [\[FN 491\]](#)

Training should include authority anomalies, not only malicious attachments. A message can be dangerous because the role is impossible, the recipient population is wrong, the source proposition changed, the timing does not permit the represented state, or the request attempts to move the recipient away from an established verification channel. [\[FN 492\]](#)

Cybersecurity providers should add legal-control-plane analysis to incident response. Endpoint telemetry will not reveal that a response became nonresponse, that a committee role lacked appointment, that a derivative report expanded an order, or that a public profile linked the wrong terminal instrument. Identity, token, mailbox, DNS, portal, and publication evidence must be correlated with hearings, deadlines, filings, orders, and institutional decisions. [\[FN 493\]](#)

C. Media, Public-Record Publishers, and Professional Identity Systems

Publishers should preserve article version history, author assignment, modification time, image provenance, syndication state, and CMS access records. A byline is an authority credential and should be auditable accordingly. [\[FN 494\]](#)

Derivative sites should clearly distinguish copied reporting from added commentary, graphics, or headlines. Search platforms should provide correction paths for identity-image and author-page misbinding. [\[FN 495\]](#)

When a court or regulator cites reporting, publication and legal systems should preserve source date and version so later readers can determine what the cited article contained at the time of reliance. [\[FN 496\]](#)

Professional directories and licensing systems should log profile changes, recovery events, delegated access, and source documents. High-risk changes should trigger out-of-band confirmation through previously established contact information. [\[FN 497\]](#)

A professional number should not be treated as proof of current role, employment, representation, or federal admission. Systems should separate stable identity attributes from event-specific authority. [\[FN 498\]](#)

Cross-platform verification should detect synchronized profile creation, reused contact routes, inconsistent admission claims, and changes occurring around consequential legal events. The control should identify relationships, not merely field validity. [\[FN 499\]](#)

Media organizations should preserve author assignment, article versions, modification timestamps, image provenance, syndication state, and CMS access records. A byline is an authority credential. When a court later cites reporting, the cited version and publication date should remain recoverable. [\[FN 500\]](#)

Derivative publishers should clearly separate copied reporting from added headlines, graphics, or commentary. Search and directory platforms should provide correction paths for author-image misbinding, stale roles, and profile states that no longer match the source institution. [\[FN 501\]](#)

Professional identity systems should separate stable identity from event-specific authority. A valid Bar number, employee identity, or professional profile does not establish current representation, committee assignment, federal admission, or authorship of a particular act. High-risk profile

changes and recovery events should be logged and confirmed through previously established contact information. [\[FN 502\]](#)

These recommendations are not premised on treating institutions as adversaries. They are designed to protect honest actors from being used as the final execution layer of a corrupted upstream state. The next Part consolidates the report's determinations and defines authority manipulation as a distinctive cAPTURE-to-Kill capability. [\[FN 503\]](#)

XXI. Integrated Determinations

The preceding Parts moved from general threat capability to ordinary legal process, then through a complete field sequence and into operational response. The findings can now be stated together without reducing them to disconnected anomalies. [\[FN 504\]](#)

A. Authority Is an Operational Control Layer

Identity is not background metadata. It is the control determining who may file, direct, authenticate, receive, publish, and enforce. The cAPTURE operator controlling identity can use genuine infrastructure to perform apparently authorized acts. [\[FN 505\]](#)

We find that the mature threat is not limited to synthetic people. It includes stolen identities, co-opted accounts, false professional relationships, unauthorized roles, changed communications, and record states detached from their source transitions. [\[FN 506\]](#)

A real person's existence does not authenticate every act attributed to that person. A real court order does not authenticate every proposition later attributed to it. A real profile does not authenticate the supporting document link. A real account does not authenticate the human operator. [\[FN 507\]](#)

We determine that counterfeit authority is most effective when carried by genuine components. The recipient's verification checks succeed because each visible element is familiar. The false element is the relationship: this person authorized this message; this role belonged to this actor; this source made this finding; this state followed from this event. [\[FN 508\]](#)

We find that authority is cyber infrastructure. It can be mapped, captured, represented, transferred, and amplified through people, accounts,

credentials, roles, documents, portals, records, and publications. The relevant question is not only whether a visible object is genuine. It is whether the object authenticates the human, relationship, source proposition, and procedural state asserted through it. [\[FN 509\]](#)

We find that the most durable counterfeit authority is often carried by genuine components. The person can exist; the account can be valid; the institution can be real; the order can be authentic; and the recipient can act honestly. The false element can be the relationship among those components. [\[FN 510\]](#)

B. The Accepted State Is the Operational Objective

The operational objective is not the malware binary. It is the state the institution accepts. Once a response is treated as absent, a role as valid, a message as fabricated, a case as defaulted, or a sanction as canonical, the operation can continue through ordinary institutional behavior. [\[FN 511\]](#)

The accepted state persists after technical access ends. A corrected docket, public profile, search result, or adverse order can remain active for years. Containment must therefore include institutional correction and reputational recovery. [\[FN 512\]](#)

The field record does not require a theory that every institutional actor acted knowingly. Honest reliance is sufficient. A decisionmaker receiving a sworn affidavit, official letter, or prior order is entitled to presume regularity unless the integrity problem is presented and examined. [\[FN 513\]](#)

The threat actor exploits that presumption by shaping upstream inputs. The downstream output may be lawfully entered in form while counterfeit in provenance. [\[FN 514\]](#)

We find that the decisive objective is the state accepted by the institution. Once a response is treated as absent, a role as valid, a message as fabricated, a case as defaulted, a source proposition as established, or a sanction as canonical, the operation can continue through ordinary process after the original access has ended. [\[FN 515\]](#)

We find that time is part of authority. The date on which a source existed, notice issued, a deadline expired, an order entered, a hearing occurred, and a public record changed determines whether the resulting state was knowable, answerable, and reviewable. [\[FN 516\]](#)

We find that repeated institutional publication is not necessarily independent corroboration. A later authority must be traced to its evidence origin. Where several public objects depend on one earlier proposition or derivative paraphrase, the appearance of a mountain of evidence can be the product of recursive amplification. [\[FN 517\]](#)

C. Authority-Rail Manipulation Is a Distinctive cAPTure-to-Kill Capability

We determine that authority-rail manipulation is a distinctive capability within cAPTure-to-Kill. It combines identity, credentials, communications, roles, portals, procedural states, timing, and publication to neutralize legal capacity. [\[FN 518\]](#)

The capability explains how a targeted professional can lose clients, communications, access to evidence, access to courts, reputation, and professional status without one visible ransomware event. Systems continue to appear functional while trusted state is shaped. [\[FN 519\]](#)

We determine that authority-rail manipulation is a distinctive capability within the cAPTure-to-Kill APT. It combines identity, credentials, communications, roles, portals, procedural states, timing, publication, and institutional reliance to degrade or neutralize legal capacity without requiring a visible ransomware event or an openly announced attack. [\[FN 520\]](#)

The novelty is not the claim that attackers can impersonate people or steal credentials. Those capabilities are well documented. ORACLE's contribution is the integration of those capabilities into a templated model directed at judicial and quasi-judicial ecosystems, where the threat actor controls or corrupts the authority chain through which law, professional status, and public reputation are produced. [\[FN 521\]](#)

We further determine that response must be meaningfully timed. The organization must preserve source state, establish clean communication, map authority, protect deadlines, compare record copies, prevent further state transitions, and correct institutional and public records while attribution continues. [\[FN 522\]](#)

Finally, we determine that a legal system cannot fully evaluate a credible integrity challenge when the only permitted route for presenting it is the same route placed in dispute. A Clean Adjudicative Environment is the

controlled mechanism by which the institution protects its own source integrity and returns the authenticated result to ordinary adversarial process. [\[FN 523\]](#)

The Conclusion now retraces the complete journey in one continuous narrative so that a reader who begins there can still understand what ORACLE investigated, how the findings were reached, why the Florida record matters, and what institutions must do differently. [\[FN 524\]](#)

XXII. Conclusion

The report began with a deceptively simple question: how can a professional identity that appears legitimate become the vehicle through which another operator influences a legal or institutional outcome? The January 2026 ORACLE work approached that question through apparent avatar personas—identities whose biographies, credentials, communication paths, or professional histories did not reconcile with the acts performed under their names. The larger record showed that the question had to expand. The most effective operation does not need to fabricate every visible component. It can use a real person, real credential, real account, real law firm, real court, real regulator, real publication, and real public database while substituting the relationship that gives those components authority. [\[FN 525\]](#)

That expansion produced the central finding of ORACLE: authority itself is an attack surface. Legal and quasi-judicial systems are designed to convert trusted representations into consequence. A lawyer files; a clerk accepts; a service system gives notice; a decisionmaker acts; a regulator publishes; employers, clients, insurers, banks, journalists, and later courts rely on the result. The same architecture that makes the system efficient gives an operator leverage if identity, credentials, role, communication, source proposition, timing, or procedural state can be corrupted upstream. [\[FN 526\]](#)

A. What the Reader Has Learned About Counterfeit Authority

The report did not ask the reader to treat every unusual email, order, profile, or procedural event as fraudulent. It established a more disciplined rule: official appearance is evidence of presentation, not the end of provenance analysis. A valid account proves that a system accepted a credential. It does not prove which human operated the account, whether the represented legal role existed, whether the attachment was the approved version, or whether the act corresponded to a valid procedural state. A real court order proves that the order exists. It does not prove every broader proposition later attributed to it. A real licensing profile proves what the public is told. It does not prove that the linked instrument supports the status displayed. [\[FN 527\]](#)

The most durable counterfeit can therefore be carried by genuine components. The message may travel through the correct server. The professional may exist. The signature image may have been copied from an

authentic form library. The portal can be real. The recipient can act honestly. The counterfeit lies in the proposition that this person authorized this act, this title belonged to this actor, this source made this finding, this document created this state, or this public status followed from the record represented beneath it. [\[FN 528\]](#)

That distinction separates the natural person from the authority-bearing event. ORACLE does not require a finding that a named lawyer, investigator, journalist, clerk, judicial assistant, regulator, or institutional employee personally participated in the operation. A person's identity can be used as an alias; a mailbox can be operated through captured credentials or tokens; a professional biography can be attached to an unauthorized communication; and a real institution can process a corrupted input without anyone inside the institution recognizing the source failure. [\[FN 529\]](#)

The report defined eight authority rails because the operation becomes clearer when trust is decomposed. Identity answers who appears to act. Credentials determine what the system accepts. Communications carry the representation. Role explains why the recipient is expected to obey. Procedural state records what changed. Intake and routing determine what reaches the decisionmaker. Publication and reputation determine what becomes canonical. Time determines whether each transition was possible, knowable, answerable, and reviewable. [\[FN 530\]](#)

The rails are not abstract categories imposed after the fact. They are the ordinary infrastructure of law. They explain how a filing becomes a docket event, how a committee assignment becomes investigative authority, how an affidavit becomes emergency evidence, how default changes the scope of trial, how a referee report becomes the principal record before a supreme court, and how a public profile becomes the professional identity seen by the outside world. [\[FN 531\]](#)

B. How the Report Reached Its Findings

ORACLE reached its determinations through a source-first method. It began with the object that existed at the relevant time: native messages and headers, filed documents, portal receipts, docket entries, service notices, affidavits, rosters, public profiles, preserved publications, and independent technical reports. Sender copies, recipient copies, filed copies, docket copies, public copies, and hand-delivered copies were not assumed to be identical merely because they shared a title or visible text. [\[FN 532\]](#)

The method then reconstructed chronology. For each consequential event, the report identified the last authenticated state, the event that purported to change it, the authority carried by that event, the system or person that relied on the changed state, and the resulting consequence. That sequence is essential because time limits what an event can prove. A later order cannot support an earlier petition. A committee cannot evaluate a response before the response period expires. A party cannot answer an evidentiary use that was not disclosed through a meaningful notice path. [\[FN 533\]](#)

Event, mechanism, and attribution were kept separate. The record can conclusively establish that two message versions differ without establishing who changed them. It can establish that a role assignment lacks a source instrument while leaving open whether the cause was administrative error, account compromise, or document substitution. It can establish that an order entered one day before a hearing later became material without resolving the identity of the operator who benefited. That separation allows firm findings at the level the evidence supports while avoiding the substitution of analogy for proof. [\[FN 534\]](#)

Independent sources were used to test capability, not replace the field evidence. Government false-worker cases demonstrate that stolen or synthetic identity can be converted into genuine enterprise credentials. FBI warnings show how BEC, spoofed contact paths, and AI-generated voice exploit trusted relationships. NIST distinguishes identity proofing, authentication, federation, and zero-trust authorization. Microsoft, CISA, MITRE, AWS, Sysdig, Infoblox, and other technical sources describe tokens, cloud roles, DNS changes, mailbox persistence, and valid-account abuse. The federal Judiciary's own publications recognize sophisticated attacks on case-management systems and the need for stronger identity and sensitive-document controls. [\[FN 535\]](#)

Those sources did not prove the Florida events by similarity. The Florida record supplied its own evidence. The independent record established that the mechanisms identified by ORACLE are operational, documented, and consistent with modern attacker tradecraft. The force of the report comes from the convergence of source-native field events, independent technical capability, completed legal and public-record comparisons, and later publication states. [\[FN 536\]](#)

The report also disclosed the lead author's relationship to the field record. Farrow's first-person account was not treated as independent corroboration. It was used only for what it could establish directly—what he reported, requested, understood, or did. Material findings were anchored to acknowledged communications, filings, affidavits, dockets, source orders, public records, FBI communications, expert reports, portal datasets, and independently verifiable sources. [\[FN 537\]](#)

C. What the Florida Field Record Demonstrated

The field case began with a control state. In 2023, independent counsel responded to Florida Bar File No. 2024-70,126 carrying an uL designation associated with the Eleventh Circuit. That event fixed the original file identity and demonstrated conventional participation before the later communications and disciplinary crisis. [\[FN 538\]](#)

By September 2024, the law practice had already documented communications interference, account problems, court-themed messages, and the need for a controlled evidentiary setting in federal filings. FBI meetings, evidence intake, Teleporter uploads, and contemplated device review also predated the terminal disciplinary outcome. The cyber-integrity theory therefore existed before the later suspension, default, referee report, and permanent public status. [\[FN 539\]](#)

The September 17 communication attributed to John Derek Womack listed matters by base file number, stated that no further response was then required in the earlier matter, and represented that other complaint packages would be supplied. The consolidated response was transmitted on October 14, and Christine Mitchell acknowledged receipt on October 15. That acknowledgment created an institutional response-received state. [\[FN 540\]](#)

Within the same period, letters routed matters to Grievance Committee 17F, identified Richard Jay Weiss as chair, and used varying language to place Womack in the investigating-member role. Archived governance evidence placed another lawyer in the 17F chair position. The documents also shifted among formulations stating that Womack appointed himself, would serve, or was assigned. The ordinary process permits Bar counsel to investigate when properly assigned, but the defined record did not supply one consistent source instrument establishing the chair and assignment authority represented by the documents. [\[FN 541\]](#)

The response state then moved through additional deadlines and committee timing. October 31 letters gave November 12 as the response deadline and represented that referral would follow nonresponse. Committee material identified a November 12 meeting, while the November 25 petition later stated November 13. The affected attorney also traveled to Tallahassee on November 4 and made physical deliveries in an attempt to create a redundant channel. The later petition nevertheless presented an aggregated thirteen-file nonresponse theory without integrating the October acknowledgment, physical deliveries, or cyber-integrity context. [\[FN 542\]](#)

The Authority-Rail conversion was therefore visible: response received became response omitted; response omitted became nonresponse alleged; nonresponse became a Supreme Court petition; and the petition became the official source through which later actors understood participation. ORACLE did not decide that every response was substantively sufficient. It found that the record lacked the authenticated file-specific bridge from receipt to nonresponse. [\[FN 543\]](#)

The communications-authorship crisis in March 2025 then changed the evidentiary environment. A message attributed to Randall Berman proposed dismissal without prejudice on defined conditions. The affected attorney accepted and placed the proposal before the Court. When the Bar disputed authorship, he disclosed the dispute and sought an in-person, source-traceable reconciliation rather than concealing the uncertainty or insisting on the purported benefit. [\[FN 544\]](#)

Berrena then wrote that another email was not the email he sent and had been changed. That statement established a provenance failure inside the same institutional stream later used to support a fabrication finding. The disclosed sanctions record did not identify native-header attribution, provider-side mailbox audit, server logs, endpoint artifacts, or an email-authorship expert connecting creation or alteration to the affected attorney. Berman's denial proved disputed authorship; it did not identify the creator. Berrena's statement proved changed content; it did not identify the operator. [\[FN 545\]](#)

The June 18 Berrena affidavit then converted disputed communications, file summaries, collateral orders, and attributed oral statements into sworn support for emergency suspension. The affidavit stated that FBI agents told

Berrena the attorney had no case and that no investigation was conducted. Direct FBI communications documented meetings, evidence intake, Teleporter uploads, contemplated computer-analysis review, and continuing examination. Those communications did not establish that a numbered criminal case remained open in May 2025, but they contradicted the categorical historical statement that no investigative activity occurred. [\[FN 546\]](#)

The affidavit also used the Berman-message episode without disclosing Berrena's own changed-email statement. That omission affected how a decisionmaker would understand the authorship dispute. A record containing only the repudiation invites an inference of recipient fabrication; a record also containing an institutional statement that another email changed requires consideration of account misuse, message alteration, or version divergence. [\[FN 547\]](#)

The adjudicative rail then changed quickly. The Supreme Court entered emergency suspension on August 4. The supplied dockets contain no separately docketed notice setting an August 8 case-management conference in the emergency matter. The August 11 order nevertheless recited that the conference occurred, recorded absence, created the answer/default structure, and treated consolidation as operative. The written Motion to Consolidate appeared on August 12. Default entered on September 3, and the omitted emergency file identifier was corrected after default-related events had already occurred. [\[FN 548\]](#)

On September 30 the Middle District entered the Strenger dismissal/default order. The disciplinary sanctions hearing occurred the next day. That order did not exist when the June emergency petition was filed and did not exist when the September 3 default established guilt. The November 4 referee report later invoked the order through judicial notice. The timing therefore affected notice, opportunity to answer, and the evidentiary basis of the sanction narrative. [\[FN 549\]](#)

Source meaning also changed as authority moved. The Seminole judgment described a draft complaint attached to a demand; the referee report stated that frivolous lawsuits were filed against spouses, parents, and a pastor. The Middle District orders contained strong case-specific criticism but did not state the generalized settlement-pressure scheme later attributed to the federal court. Those changes demonstrate how a later

authoritative report can enlarge a source proposition and then carry the enlarged proposition forward under a new institutional signature. [\[FN 550\]](#)

The public profile completed the sequence. It reports permanent disbarment effective May 21, 2026, while the linked discipline-document page omits the May 21 terminal instrument and presents the corrected August 4 emergency-suspension order as the Supreme Court order. The comparator study found that the other inspected permanent-disbarment reference pages supplied the terminal instrument. The divergence matters because the profile is the public professional identity consumed by courts, employers, clients, insurers, banks, licensing bodies, media, and search engines. [\[FN 551\]](#)

D. Why the Findings Extend Beyond One Proceeding

The report's broader significance does not depend on proving that one actor controlled every field event. Government investigations, provider research, peer-reviewed studies, court publications, and technical reporting independently establish the component capabilities: synthetic and stolen identity, false-worker access, valid-account abuse, token persistence, mailbox delegation, DNS and cloud control, AI-assisted impersonation, mercenary hacking, law-firm targeting, and attacks on judicial case-management systems. [\[FN 552\]](#)

The Department of Justice and FBI false-worker record demonstrates the institutional conversion at the heart of ORACLE. The device and credentials are real because the victim organization issued them. The system logs correctly record the assigned account. The false state lies in the human principal and relationship. Business email compromise demonstrates the same structure in communications: the account or thread appears familiar, the request fits context, and the recipient acts because the relationship supplies authority. [\[FN 553\]](#)

Cloud and token research explains why visible remediation can fail. Password rotation can leave refresh tokens, service principals, mailbox permissions, recovery methods, and registered devices active. DNS and cloud APIs can process hostile instructions through the same interfaces used by legitimate administrators. The provider's record that a valid credential acted is accurate but incomplete; it does not identify whether the intended human controlled the credential. [\[FN 554\]](#)

The legal sector magnifies those risks because authority is densely interconnected. A lawyer's mailbox touches clients, courts, insurers, providers, and opposing counsel. A filing credential creates docket and service states. A byline can shape public understanding. A licensing profile can determine employability and professional status. A short upstream manipulation can therefore propagate into many institutions without requiring continued access. [\[FN 555\]](#)

ORACLE calls the resulting repetition authority stacking. Search engines, court records, profiles, media articles, and derivative pages can repeat one proposition through different institutional forms. The reader experiences the stack as independent corroboration even when the nodes depend on the same source or derivative paraphrase. Dependency mapping is therefore essential to both forensic analysis and reputational recovery. [\[FN 556\]](#)

E. Containment Before Autopsy

The operational lesson is that response cannot wait for perfect attribution. A complete cyber autopsy may take months; the legal consequence can occur before the end of the day. A filing deadline can expire, a client can lose representation, a default can enter, a regulator can accept a false state, a news article can propagate, and a public profile can become canonical while the technical team is still collecting logs. [\[FN 557\]](#)

Containment before autopsy does not lower the evidentiary standard. It preserves the evidence and legal capacity needed to reach a reliable attribution later. In the first hours, the team must preserve native messages, headers, logs, portal receipts, docket states, token and device records, DNS and MX records, cloud roles, call evidence, and current public pages. It must establish a known-clean contact path and identify every critical legal and publication clock. [\[FN 558\]](#)

Within twenty-four hours, the team should map the represented actor, natural person, account, credential, role, institution, channel, source object, before state, after state, recipient, and consequence. Preservation requests should identify exact objects. Institutions should receive a narrow integrity notice that asks them to preserve and authenticate a defined event rather than accept the entire attribution theory. [\[FN 559\]](#)

Within seventy-two hours, the team should reconstruct outcome-determinative transitions, compare sender, provider, recipient, filing, docket, and public copies, identify downstream propagation, and

implement a continuity and correction plan. Technical remediation and legal-state correction must proceed together because changing a password does not correct a docket, revoking a token does not restore a missed deadline, and reimaging a device does not retract a public professional status. [\[FN 560\]](#)

The success measure is meaningfully timed relief. The business must remain capable of communicating; clients must retain verified access to counsel; evidence must survive; deadlines must be protected; courts and regulators must receive authenticated information; and public records must not harden an unsupported state before the investigation can mature. [\[FN 561\]](#)

F. Clean Adjudication and Institutional Responsibility

The field tests across the Southern District of Florida, Eastern District of New York, District of Columbia, and Florida Supreme Court revealed a repeated circularity: the claimant alleged that identity, filing, service, routing, communications, or record custody were compromised and then had to use those same systems to prove it. A failed filing can be treated as noncompliance. A successful filing processed as ordinary advocacy can be denied without controlled technical examination. A change of channel can be treated as irregular. [\[FN 562\]](#)

A Clean Adjudicative Environment is the narrow bridge that breaks that circularity. It preserves judicial control while allowing known-clean intake, independent identity verification, source-object preservation, controlled technical review, dual-channel confirmation, provider authentication, and reconciliation back into the ordinary public record. It is not a private forum and does not bypass adversarial process. It protects the source integrity on which adversarial process depends. [\[FN 563\]](#)

Courts and clerks should preserve provenance for corrected orders, service-list changes, consolidation, reassignment, sealed-to-public transitions, and docket replacement. Bars and regulators should authenticate complaint origin, response receipt, committee authority, role, transfer, and publication as distinct states. Law firms should maintain authority inventories and clean-contact plans. Cybersecurity providers should correlate identity, token, mailbox, DNS, portal, and publication evidence with hearings, deadlines, filings, and orders. Media and identity

systems should preserve version history and event-specific authority. [\[FN 564\]](#)

These controls do not presume that institutions are malicious. They protect honest actors from becoming the execution layer of corrupted upstream authority. The institution's credibility is preserved when it can reconstruct who acted, through what credential, under what role, on what source object, at what time, and through which transition. [\[FN 565\]](#)

G. Final Determination

We find that modern legal cybersecurity cannot be limited to malware detection, endpoint protection, passwords, and perimeter defense. Those controls are necessary, but they do not authenticate the human operator, the event-specific role, the source proposition, the procedural transition, or the public state produced after the technical event. [\[FN 566\]](#)

We find that the mature avatar threat extends beyond synthetic persons. It includes stolen or co-opted identities, valid accounts, false professional relationships, unauthorized roles, changed communications, counterfeit indicia of authority, record states detached from their source transitions, and genuine institutions processing corrupted inputs. [\[FN 567\]](#)

We find that the accepted institutional state—not the malware binary—is the decisive operational objective. Once a response is treated as absent, a role as valid, a communication as fabricated, a case as defaulted, a finding as established, or a sanction as canonical, the operation can persist through ordinary institutional behavior after the original technical access ends. [\[FN 568\]](#)

We find that time is an independent authority rail and that source propositions must be traced through every derivative authority that repeats them. Repetition by different institutions is not independent proof when the later objects depend on one upstream source or expanded paraphrase. [\[FN 569\]](#)

We determine that authority-rail manipulation is a distinctive cAPTure-to-Kill capability. It integrates impersonation, valid accounts, tokens, trusted relationships, data manipulation, portal and publication control, procedural state, timing, and honest institutional reliance inside a templated operation directed at judicial and quasi-judicial ecosystems. [\[FN 570\]](#)

We determine that the appropriate response is meaningfully timed containment: preserve source state, establish clean communication, map authority, protect deadlines, compare record copies, prevent further transitions, and correct institutional and public states while attribution continues. [\[FN 571\]](#)

We determine that legal institutions require a controlled integrity path when the ordinary rail is credibly implicated. A system cannot fully evaluate a challenge to filing, service, identity, notice, routing, or record custody when the only permitted route for the challenge is the same disputed system. [\[FN 572\]](#)

ORACLE began by asking whether an apparent professional persona could be false. It concludes with a more consequential finding. The person may be real. The credential may be real. The institution may be real. The form, portal, article, profile, or order may also be real. What must still be authenticated is the chain connecting those genuine components to the act performed, the role asserted, the proposition adopted, and the state imposed. [\[FN 573\]](#)

That chain is the authority rail. Before an authority-bearing state is accepted, repeated, enforced, or published as history, the source that created it must be reconstructed. [\[FN 574\]](#)

FULL ENDNOTES

The report contains 574 distinct numbered endnotes. Each inline marker links to its corresponding note; each note returns to the point of citation. Public-source URLs are presented as active hyperlinks.

[FN 1] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* This publication comprehensively reconstructs the September 2026 v.41 working draft while preserving the January 20, 2026 ORACLE Word report as the report-lineage baseline.  [return](#)

[FN 2] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application:* Jay Lewis Farrow served as Lead Author and Senior Editor.  [return](#)

[FN 3] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* The Florida record is not included as a request to re-adjudicate every disciplinary or civil allegation.  [return](#)

[FN 4] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* The report is intended for publication through CyberLawLibrary.org and related research channels.  [return](#)

[FN 5] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted

Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: definition and framing of the authority-rail problem inside cAPTure-to-Kill. [↩ return](#)

[FN 6] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices.

<https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>.

Application: cAPTure-to-Kill strategic model and authority manipulation as a distinct capability. [↩ return](#)

[FN 7] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline..

Application: source support for the discussion under A. From Avatar Personas to Authority-Rail Exploitation. [↩ return](#)

[FN 8] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under A. From Avatar Personas to Authority-Rail Exploitation. [↩ return](#)

[FN 9] MITRE ATT&CK, T1656, Impersonation.

<https://attack.mitre.org/techniques/T1656/>. *Application:* source support for the discussion under A. From Avatar Personas to Authority-Rail Exploitation. [↩ return](#)

[FN 10] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under A. From Avatar Personas to Authority-Rail Exploitation. [↩ return](#)

[FN 11] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under B. Why Legal and Quasi-Judicial Systems Are High-Value Trust Environments. [↩ return](#)

[FN 12] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under B. Why Legal and Quasi-Judicial Systems Are High-Value Trust Environments. [↩ return](#)

[FN 13] Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023). <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>. *Application:* source support for the discussion under B. Why Legal and Quasi-Judicial Systems Are High-Value Trust Environments. [↩ return](#)

[FN 14] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under B. Why Legal and Quasi-Judicial Systems Are High-Value Trust Environments.  [return](#)

[FN 15] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application:* legal systems as trust-conversion systems and the downstream effect of corrupted upstream authority.  [return](#)

[FN 16] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* executive finding and source support.  [return](#)

[FN 17] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* executive finding and source support.  [return](#)

[FN 18] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* executive finding and source support.  [return](#)

[FN 19] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* executive finding and source support.  [return](#)

[FN 20] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* executive finding and source support.  [return](#)

[FN 21] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=. *Application:* executive finding and source support.  [return](#)

- [FN 22] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* executive finding and source support. [↩ return](#)
- [FN 23] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* executive finding and source support. [↩ return](#)
- [FN 24] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying 'J. Derek Womack, Senior Litigation Attorney.'. *Application:* executive finding and source support. [↩ return](#)
- [FN 25] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* executive finding and source support. [↩ return](#)
- [FN 26] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* executive finding and source support. [↩ return](#)
- [FN 27] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* executive finding and source support. [↩ return](#)
- [FN 28] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* executive finding and source support. [↩ return](#)

- [FN 29] A Novel Deep Synthesis-Based Insider Intrusion Detection Model for Malicious Insiders and AI-Generated Threats, *Scientific Reports* (2025). <https://www.nature.com/articles/s41598-025-85352-4>; Kely Gonzaga et al., AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies, *Computers* 15, no. 2 (2026). <https://doi.org/10.3390/computers15020128>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: reader-centered structure and use of the field case after general mechanism explanation.  [return](#)
- [FN 30] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: source-state transition method and cross-disciplinary accessibility.  [return](#)
- [FN 31] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application*: transition from avatar-persona research to authority-rail analysis.  [return](#)
- [FN 32] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: ORACLE lineage and the insufficiency of a binary real-or-fake inquiry.  [return](#)
- [FN 33] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.. *Application*: source support for the discussion under A. The ORACLE First Draft as the Preserved Baseline.  [return](#)
- [FN 34] MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>. *Application*: source support for the discussion under A. The ORACLE First Draft as the Preserved Baseline.  [return](#)
- [FN 35] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.. *Application*: source support for the discussion under A. The ORACLE First Draft as the Preserved Baseline.  [return](#)
- [FN 36] MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>. *Application*: source support for the discussion under A. Fully Synthetic Personas.  [return](#)

- [FN 37] Federal Bureau of Investigation, warning concerning criminals' use of generative AI, voice cloning, and video to impersonate trusted people and organizations. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>. *Application:* source support for the discussion under A. Fully Synthetic Personas.  [return](#)
- [FN 38] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>. *Application:* source support for the discussion under A. Fully Synthetic Personas.  [return](#)
- [FN 39] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* source support for the discussion under B. Stolen-Identity and Credential-Backed Avatars.  [return](#)
- [FN 40] MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under B. Stolen-Identity and Credential-Backed Avatars.  [return](#)
- [FN 41] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under B. Stolen-Identity and Credential-Backed Avatars.  [return](#)
- [FN 42] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.. *Application:* source support for the discussion under C. Blended Personas.  [return](#)
- [FN 43] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* source support for the discussion under C. Blended Personas.  [return](#)
- [FN 44] Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application:* source support for the discussion under C. Blended Personas.  [return](#)
- [FN 45] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* event-specific identity classification and blended persona operations.  [return](#)

- [FN 46] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.. *Application:* source support for the discussion under D. Communications Avatars. [↩ return](#)
- [FN 47] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under D. Communications Avatars. [↩ return](#)
- [FN 48] Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under D. Communications Avatars. [↩ return](#)
- [FN 49] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. Role-and-Authority Avatars. [↩ return](#)
- [FN 50] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under E. Role-and-Authority Avatars. [↩ return](#)
- [FN 51] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under E. Role-and-Authority Avatars. [↩ return](#)
- [FN 52] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under F. Record-State Avatars. [↩ return](#)
- [FN 53] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under F. Record-State Avatars. [↩ return](#)
- [FN 54] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under F. Record-State Avatars. [↩ return](#)
- [FN 55] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, McClatchyDC.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler

Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under G. Media and Reputation Avatars. [!\[\]\(da3dd1d44378ef625513225eb3da25fc_img.jpg\) return](#)

[FN 56] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under G. Media and Reputation Avatars. [!\[\]\(3969144645fd70df7eab65919ae2ddc9_img.jpg\) return](#)

[FN 57] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv. *Application:* source support for the discussion under G. Media and Reputation Avatars. [!\[\]\(dc15fe4119de1a7701c2eadd3b759d89_img.jpg\) return](#)

[FN 58] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under H. Institutional Avatars. [!\[\]\(fd3078a0028b703bf47b1e666b23155b_img.jpg\) return](#)

[FN 59] The Florida Bar, Scam Alert: Fake Emails Claim to Be from the Bar's Executive Director (Nov. 5, 2019). <https://www.floridabar.org/the-florida-bar-news/scam-alert-fake-emails-claim-to-be-from-the-bars-executive-director/>. *Application:* source support for the discussion under H. Institutional Avatars. [!\[\]\(cc4676f7fb2a17fd25df7d1bb92c73ef_img.jpg\) return](#)

[FN 60] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>. *Application:* source support for the discussion under H. Institutional Avatars. [!\[\]\(7f3b3f55cc6dde7544d78cda0664abcb_img.jpg\) return](#)

[FN 61] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>. *Application:* authority avatar as the larger category encompassing people, roles, communications, and records. [!\[\]\(aebe38265dd2d080f597681237d84283_img.jpg\) return](#)

[FN 62] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* separation of natural person from account operator or authority-bearing event. [!\[\]\(e54e870b808ff195da9f2fae56c9e9af_img.jpg\) return](#)

[FN 63] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* transition to source-first methodology. [!\[\]\(7a6366957a78d522e7a652add6f64ea7_img.jpg\) return](#)

[FN 64] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8,

21-29, 40-48.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* source-first method and separation of account activity from human authority. [↩ return](#)

[FN 65] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>. *Application:* source support for the discussion under B. Relationship to the CNF, CCDG, RAPS, and Civil Cyber-Infrastructure Research. [↩ return](#)

[FN 66] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.. *Application:* source support for the discussion under B. Relationship to the CNF, CCDG, RAPS, and Civil Cyber-Infrastructure Research. [↩ return](#)

[FN 67] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* source support for the discussion under B. Relationship to the CNF, CCDG, RAPS, and Civil Cyber-Infrastructure Research. [↩ return](#)

[FN 68] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under B. Relationship to the CNF, CCDG, RAPS, and Civil Cyber-Infrastructure Research. [↩ return](#)

[FN 69] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.. *Application:* source support for the discussion under B. Relationship to the CNF, CCDG, RAPS, and Civil Cyber-Infrastructure Research. [↩ return](#)

[FN 70] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under C. Source Hierarchy and Sentence-Level Citation Method. [↩ return](#)

[FN 71] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under C. Source Hierarchy and Sentence-Level Citation Method. [↩ return](#)

[FN 72] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under C. Source Hierarchy and Sentence-Level Citation Method. [↩ return](#)

- [FN 73] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* source support for the discussion under C. Source Hierarchy and Sentence-Level Citation Method. [↩ return](#)
- [FN 74] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under C. Source Hierarchy and Sentence-Level Citation Method. [↩ return](#)
- [FN 75] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* source support for the discussion under D. Evidence Preservation, Visual Artifacts, and Reproducibility. [↩ return](#)
- [FN 76] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under D. Evidence Preservation, Visual Artifacts, and Reproducibility. [↩ return](#)
- [FN 77] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under D. Evidence Preservation, Visual Artifacts, and Reproducibility. [↩ return](#)
- [FN 78] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* native-object preservation and copy comparison. [↩ return](#)
- [FN 79] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* limits of institutional records and source-layer separation. [↩ return](#)

[FN 80] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>.

Application: role of independent open sources in mechanism corroboration.  [return](#)

[FN 81] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-. *Application:* temporal analysis as an authority control.  [return](#)

[FN 82] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>; MITRE ATT&CK, T1565, Data Manipulation. <https://attack.mitre.org/techniques/T1565/>.

Application: event-state-mechanism-attribution separation.  [return](#)

[FN 83] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Instructions to View Discipline Documents.

<https://www.floridabar.org/public/acap/instructions/>. *Application:* bounded comparator method.  [return](#)

[FN 84] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* dependency mapping and recursive repetition.  [return](#)

[FN 85] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* citation architecture and reproducibility.  [return](#)

- [FN 86] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: versioning, peer review, and disciplined correction.  [return](#)
- [FN 87] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: transition from methodology to ordinary legal authority flow.  [return](#)
- [FN 88] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: ordinary legal and quasi-judicial trust architecture.  [return](#)
- [FN 89] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application*: ordinary relationship among identity, credential, and legal authority.  [return](#)
- [FN 90] Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>; Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>. *Application*: ordinary electronic filing and service workflow.  [return](#)
- [FN 91] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application*: service and recipient population as legal-control-plane elements.  [return](#)
- [FN 92] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: ordinary evidentiary source distinctions.  [return](#)

[FN 93] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: rule-governed legal state transitions.  [return](#)

[FN 94] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, ‘Swindler Barbie’ graphic, and article-distribution screenshots.; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application*: publication layer as canonical professional identity.  [return](#)

[FN 95] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>. *Application*: transitive trust and upstream leverage.  [return](#)

[FN 96] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application*: proportionate verification rather than universal suspicion.  [return](#)

[FN 97] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application*: transition to the Authority-Rail Model.  [return](#)

- [FN 98] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* Authority-Rail Model and multi-rail convergence.  [return](#)
- [FN 99] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* source support for the discussion under A. Identity Rail.  [return](#)
- [FN 100] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue>. *Application:* source support for the discussion under A. Identity Rail.  [return](#)
- [FN 101] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under A. Identity Rail.  [return](#)
- [FN 102] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>. *Application:* source support for the discussion under B. Credential Rail.  [return](#)
- [FN 103] Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023). <https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>; BleepingComputer, Russian Hackers Exploit Exchange OWA Zero-Day for Long-Term Mailbox Access (July 29, 2026). <https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/>. *Application:* source support for the discussion under B. Credential Rail.  [return](#)

- [FN 104] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application*: source support for the discussion under B. Credential Rail.  [return](#)
- [FN 105] David Temoshok et al., National Institute of Standards and Technology, Digital Identity Guidelines: Identity Proofing and Enrollment, NIST SP 800-63A-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63A-4>; David Temoshok et al., National Institute of Standards and Technology, Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63B-4>; Justin Richer et al., National Institute of Standards and Technology, Digital Identity Guidelines: Federation and Assertions, NIST SP 800-63C-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63C-4>. *Application*: NIST identity proofing, authentication, federation, and the remaining role-authority question.  [return](#)
- [FN 106] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue>; KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us (July 23, 2024). <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>. *Application*: false-worker conversion of synthetic identity into genuine enterprise authority.  [return](#)
- [FN 107] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; MITRE ATT&CK, Detection Strategy DET0560, Detection of Valid Account Abuse Across Platforms (created Oct. 21, 2025; modified May 12, 2026). <https://attack.mitre.org/detectionstrategies/DET0560/>. *Application*: detection of valid-account abuse beyond password validity.  [return](#)
- [FN 108] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>. *Application*: source support for the discussion under C. Communications Rail.  [return](#)
- [FN 109] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023).

<https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>. *Application:* source

support for the discussion under C. Communications Rail.  [return](#)

[FN 110] Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>; Federal Bureau of Investigation, warning concerning criminals' use of generative AI, voice cloning, and video to impersonate trusted people and organizations. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>. *Application:* source support for the

discussion under C. Communications Rail.  [return](#)

[FN 111] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source support for the discussion under D. Role-and-Authority Rail.

 [return](#)

[FN 112] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under D. Role-and-Authority Rail.

 [return](#)

[FN 113] Respondent's Motion for Order to Show Cause, SC2024-1681 (Feb. 27, 2025), including embedded Feb. 26 Weiss Serota communication directing future communications to Patricia Ann Toro Savitz at psavitz@floridabar.org.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>. *Application:* source support for the discussion under D. Role-and-Authority Rail.

 [return](#)

[FN 114] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023).

<https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>. *Application:* technical

email authentication and its inability to prove human intent or legal authority.  [return](#)

[FN 115] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>.

Application: event-specific role authentication through governance records.  [return](#)

[FN 116] Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>; Federal Bureau of Investigation, warning concerning criminals' use of generative AI, voice cloning, and video to impersonate trusted people and organizations. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>; Federal Bureau of Investigation, Spoofing and Phishing. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/spoofing-and-phishing>. *Application:* limits of voice, video, telephone number, and familiar presentation.  [return](#)

[FN 117] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source support for the discussion under E. Procedural-State Rail.  [return](#)

[FN 118] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; MITRE ATT&CK, T1565, Data Manipulation. <https://attack.mitre.org/techniques/T1565/>. *Application:* source support for the discussion under E. Procedural-State Rail.  [return](#)

[FN 119] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under E. Procedural-State Rail.  [return](#)

[FN 120] Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap->

[to-floridas-lawyer-regulation-system/](#). *Application:* source support for the discussion under F. Adjudicative Intake-and-Routing Rail.  [return](#)

[FN 121] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* source support for the discussion under F. Adjudicative Intake-and-Routing Rail.  [return](#)

[FN 122] Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; Administrative Office of the U.S. Courts, Judges Outline Accelerated Modernization of Case Management System (Mar. 10, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system>. *Application:* source support for the discussion under F. Adjudicative Intake-and-Routing Rail.  [return](#)

[FN 123] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* conversion of technical interference into legal state.  [return](#)

[FN 124] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application:* separation of portal transaction states.  [return](#)

[FN 125] Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; Administrative Office of the U.S. Courts, Judges Outline Accelerated Modernization of Case Management System (Mar. 10, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system>; Administrative Office of the U.S. Courts, Judiciary Approves Funding for Case Management and Public Access Modernization (June 26, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization>; Administrative Office of the U.S. Courts, Court Operations—Annual Report 2025. <https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2025/court-operations-annual-report-2025>. *Application:* official recognition of attacks and modernization of judicial case-management systems.  [return](#)

- [FN 126]** The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.
<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under G. Publication-and-Reputation Rail.  [return](#)
- [FN 127]** The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.
<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under G. Publication-and-Reputation Rail.  [return](#)
- [FN 128]** Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.. *Application:* source support for the discussion under H. Temporal Rail.  [return](#)
- [FN 129]** Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025.
[https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=.](https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=)
Application: source support for the discussion under H. Temporal Rail.  [return](#)
- [FN 130]** Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.; Wieder research package, including Wieder Dossier v.10, National Press Foundation profile research, McClatchy/Miami Herald author materials, telephone and email artifacts, and preserved screenshots.. *Application:* source support for the discussion under H. Temporal Rail.  [return](#)
- [FN 131]** The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.
<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-

distribution screenshots.. *Application:* publication as a terminal authority rail. [↩ return](#)

[FN 132] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-. *Application:* temporal authority and event-availability analysis. [↩ return](#)

[FN 133] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* transition to the templated cAPTure authority sequence. [↩ return](#)

[FN 134] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>. *Application:* templated cAPTure authority-avatar sequence. [↩ return](#)

[FN 135] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>. *Application:* source support for the discussion under A. Reconnaissance and Target Mapping. [↩ return](#)

[FN 136] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under A. Reconnaissance and Target Mapping. [↩ return](#)

[FN 137] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under A. Reconnaissance and Target Mapping. [↩ return](#)

[FN 138] MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>. *Application:* source support for the discussion under B. Persona or Role Seeding. [↩ return](#)

[FN 139] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under B. Persona or Role Seeding. [↩ return](#)

- [FN 140] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline. *Application:* source support for the discussion under B. Persona or Role Seeding.  [return](#)
- [FN 141] MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under C. Credential Acquisition or Relationship Substitution.  [return](#)
- [FN 142] Respondent's Motion for Order to Show Cause, SC2024-1681 (Feb. 27, 2025), including embedded Feb. 26 Weiss Serota communication directing future communications to Patricia Ann Toro Savitz at psavitz@floridabar.org.. *Application:* source support for the discussion under C. Credential Acquisition or Relationship Substitution.  [return](#)
- [FN 143] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.. *Application:* source support for the discussion under D. Trusted-Channel Insertion.  [return](#)
- [FN 144] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under D. Trusted-Channel Insertion.  [return](#)
- [FN 145] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPtUre-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; MITRE ATT&CK, T1114, Email Collection. <https://attack.mitre.org/techniques/T1114/>. *Application:* relationship-centered reconnaissance.  [return](#)
- [FN 146] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.; Respondent's Motion for Order to Show Cause, SC2024-1681 (Feb. 27, 2025), including embedded Feb. 26 Weiss Serota communication directing future communications to Patricia Ann Toro Savitz at psavitz@floridabar.org.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>. *Application:* documentary and relational role seeding.  [return](#)
- [FN 147] MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>; Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>. *Application:* credential acquisition and relationship substitution.  [return](#)

- [FN 148] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. State Transition. [↩ return](#)
- [FN 149] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. State Transition. [↩ return](#)
- [FN 150] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under F. Institutional Reliance. [↩ return](#)
- [FN 151] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under F. Institutional Reliance. [↩ return](#)
- [FN 152] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under G. Recursive Amplification. [↩ return](#)
- [FN 153] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under G. Recursive Amplification. [↩ return](#)
- [FN 154] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under H. Adaptation and Persistence. [↩ return](#)
- [FN 155] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* source support for the discussion under H. Adaptation and Persistence. [↩ return](#)
- [FN 156] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* accepted state as the operational objective. [↩ return](#)
- [FN 157] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* honest institutional reliance as an attack surface. [↩ return](#)

[FN 158] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; *Strenger v. RMC Consulting, Inc.*, No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application*: recursive institutional authority amplification.  [return](#)

[FN 159] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: institutional persistence after technical access ends.  [return](#)

[FN 160] MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>; Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>. *Application*: transition to the external comparator record.  [return](#)

[FN 161] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: purpose and boundaries of the external comparator record.  [return](#)

[FN 162] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue>. *Application*: source support for the discussion under A. Government-Documented False-Worker and Stolen-Identity Operations.  [return](#)

[FN 163] KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us (July 23, 2024). <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to->

[infiltrate-us](#). *Application:* source support for the discussion under A. Government-Documented False-Worker and Stolen-Identity Operations. [↩ return](#)

[FN 164] Federal Bureau of Investigation, North Korean IT Workers Conducting Data Extortion (Jan. 23, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-workers-conducting-data-extortion>. *Application:* source support for the discussion under A. Government-Documented False-Worker and Stolen-Identity Operations. [↩ return](#)

[FN 165] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under A. Government-Documented False-Worker and Stolen-Identity Operations. [↩ return](#)

[FN 166] Federal Bureau of Investigation, warning concerning criminals' use of generative AI, voice cloning, and video to impersonate trusted people and organizations. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>; Matthew Edwards et al., DeepPhish: Measuring Users' Vulnerability to Artificially Generated Social Media Profiles, USENIX Security Symposium (2022). <https://www.usenix.org/conference/usenixsecurity22/presentation/edwards>. *Application:* source support for the discussion under E. AI-Assisted Impersonation, Deepfakes, and Scalable Persona Maintenance. [↩ return](#)

[FN 167] Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>; Kely Gonzaga et al., AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies, *Computers* 15, no. 2 (2026). <https://doi.org/10.3390/computers15020128>. *Application:* source support for the discussion under E. AI-Assisted Impersonation, Deepfakes, and Scalable Persona Maintenance. [↩ return](#)

[FN 168] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us (July 23, 2024). <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>. *Application:* source support for the discussion under E. AI-Assisted Impersonation, Deepfakes, and Scalable Persona Maintenance. [↩ return](#)

[FN 169] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:*

source support for the discussion under E. AI-Assisted Impersonation, Deepfakes, and Scalable Persona Maintenance.  [return](#)

[FN 170] U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue>; CISA, FBI, and partners, Guidance on the North Korean IT Worker Threat (May 16, 2022, updated). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>. *Application:* government-documented remote IT worker schemes.  [return](#)

[FN 171] KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us (July 23, 2024). <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>. *Application:* enterprise false-worker case.  [return](#)

[FN 172] Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* synthetic identities converted into enterprise footholds.  [return](#)

[FN 173] Matthew Edwards et al., DeepPhish: Measuring Users' Vulnerability to Artificially Generated Social Media Profiles, USENIX Security Symposium (2022). <https://www.usenix.org/conference/usenixsecurity22/presentation/edwards>; A Novel Deep Synthesis-Based Insider Intrusion Detection Model for Malicious Insiders and AI-Generated Threats, Scientific Reports (2025). <https://www.nature.com/articles/s41598-025-85352-4>; Kely Gonzaga et al., AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies, Computers 15, no. 2 (2026). <https://doi.org/10.3390/computers15020128>. *Application:* peer-reviewed evidence on synthetic profiles and AI-enabled social engineering.  [return](#)

[FN 174] Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>; Federal Bureau of Investigation, warning concerning criminals' use of generative AI, voice cloning, and video to impersonate trusted people and organizations. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>. *Application:* AI-assisted impersonation of trusted officials.  [return](#)

[FN 175] MITRE ATT&CK, T1078, Valid Accounts.

<https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under A. Credential Theft and Valid Accounts.  [return](#)

[FN 176] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Microsoft Threat Intelligence, Microsoft Digital Defense Report 2025 and related identity-threat research. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2025>. *Application:* source support for the discussion under A. Credential Theft and Valid Accounts.  [return](#)

[FN 177] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* source support for the discussion under A. Credential Theft and Valid Accounts.  [return](#)

[FN 178] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under A. Credential Theft and Valid Accounts.  [return](#)

[FN 179] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>. *Application:* source support for the discussion under B. Session, OAuth, Token, and Mailbox Persistence.  [return](#)

[FN 180] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; BleepingComputer, Russian Hackers Exploit Exchange OWA Zero-Day for Long-Term Mailbox Access (July 29, 2026). <https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/>. *Application:* source support for the discussion under B. Session, OAuth, Token, and Mailbox Persistence.  [return](#)

[FN 181] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023).

<https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>. *Application:* source support for the discussion under B. Session, OAuth, Token, and Mailbox Persistence.  [return](#)

[FN 182] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under B. Session, OAuth, Token, and Mailbox Persistence.  [return](#)

[FN 183] Amazon Web Services, Route 53 API: ChangeResourceRecordSets and IAM service-authorization documentation. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html. *Application:* source support for the discussion under C. DNS, MX, Cloud, and Trusted Relay Control.  [return](#)

[FN 184] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Amazon Web Services, Route 53 API: ChangeResourceRecordSets and IAM service-authorization documentation. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html. *Application:* source support for the discussion under C. DNS, MX, Cloud, and Trusted Relay Control.  [return](#)

[FN 185] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; MITRE ATT&CK, T1557, Adversary-in-the-Middle. <https://attack.mitre.org/techniques/T1557/>. *Application:* source support for the discussion under C. DNS, MX, Cloud, and Trusted Relay Control.  [return](#)

[FN 186] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under C. DNS, MX, Cloud, and Trusted Relay Control.  [return](#)

[FN 187] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Administrative Office of the U.S. Courts, CM/ECF and

PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application:* source support for the discussion under D. Portal Identity and Restricted Workflow Access.  [return](#)

[FN 188] Team B, Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess e-Filing Portal datasets (2024-2025), Project artifacts.. *Application:* source support for the discussion under D. Portal Identity and Restricted Workflow Access.  [return](#)

[FN 189] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* source support for the discussion under D. Portal Identity and Restricted Workflow Access.  [return](#)

[FN 190] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under D. Portal Identity and Restricted Workflow Access.  [return](#)

[FN 191] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under D. Cloud, Token, and Valid-Account Abuse.  [return](#)

[FN 192] Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023). <https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>. *Application:* source support for the discussion under D. Cloud, Token, and Valid-Account Abuse.  [return](#)

[FN 193] Microsoft Security, Storm-0501: Ransomware Attacks Expanding to Hybrid Cloud Environments (Sept. 26, 2024). <https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/>; Sysdig Threat Research Team, SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft (Feb. 28, 2023). <https://www.sysdig.com/blog/cloud-breach-terraform-data-theft>. *Application:* source support for the discussion under D. Cloud, Token, and Valid-Account Abuse.  [return](#)

[FN 194] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; BleepingComputer, Russian Hackers Exploit Exchange OWA Zero-Day for Long-Term Mailbox Access (July 29, 2026). <https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/>. *Application:* source support for the discussion under D. Cloud, Token, and Valid-Account Abuse. [↩ return](#)

[FN 195] MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>; MITRE ATT&CK, T1565, Data Manipulation. <https://attack.mitre.org/techniques/T1565/>; MITRE ATT&CK, T1557, Adversary-in-the-Middle. <https://attack.mitre.org/techniques/T1557/>; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>; MITRE ATT&CK, T1114, Email Collection. <https://attack.mitre.org/techniques/T1114/>; MITRE ATT&CK, T1583, Acquire Infrastructure. <https://attack.mitre.org/techniques/T1583/>. *Application:* MITRE techniques relevant to authority-rail operations. [↩ return](#)

[FN 196] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Microsoft Threat Intelligence, Microsoft Digital Defense Report 2025 and related identity-threat research. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2025>; Microsoft Security, Storm-0501: Ransomware Attacks Expanding to Hybrid Cloud Environments (Sept. 26, 2024). <https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/>. *Application:* modern identity and hybrid-cloud persistence. [↩ return](#)

[FN 197] Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023). <https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>. *Application:* forged tokens accepted through trusted signing infrastructure. [↩ return](#)

[FN 198] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* cloud identity controls and event logging. [↩ return](#)

[FN 199] Amazon Web Services, Route 53 API: ChangeResourceRecordSets and IAM service-authorization documentation.

https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html; Sysdig Threat Research Team, SCARLETEEL: Operation Leveraging Terraform, Kubernetes, and AWS for Data Theft (Feb. 28, 2023). <https://www.sysdig.com/blog/cloud-breach-terraform-data-theft>; Infoblox Threat Intelligence, Vacant Viper: Sitting Ducks, Cobalt Strike and Malspam (July 30, 2024). <https://www.infoblox.com/blog/threat-intelligence/vacant-viper-sitting-ducks-cobalt-strike-and-malspam/>. *Application:* cloud and DNS control through legitimate administrative interfaces.  [return](#)

[FN 200] BleepingComputer, Russian Hackers Exploit Exchange OWA Zero-Day for Long-Term Mailbox Access (July 29, 2026). <https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/>. *Application:* server-side mailbox persistence surviving endpoint remediation.  [return](#)

[FN 201] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* source support for the discussion under B. Business Email Compromise and Account Impersonation.  [return](#)

[FN 202] Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>. *Application:* source support for the discussion under B. Business Email Compromise and Account Impersonation.  [return](#)

[FN 203] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48; Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* source support for the discussion under B. Business Email Compromise and Account Impersonation.  [return](#)

[FN 204] Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023). <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>; United Kingdom National Cyber Security Centre, Cyber Threat Report: UK Legal Sector. <https://www.ncsc.gov.uk/report/cyber-threat-report-uk-legal-sector>. *Application:* source support for the discussion under C. Hackers-for-Hire Targeting Legal Professionals.  [return](#)

[FN 205] U.S. Department of Justice, Justice Department Charges 12 Chinese Contract Hackers and Law-Enforcement Officers in Global Computer Intrusion Campaigns (Mar. 5, 2025). <https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global>. *Application:* source support for the discussion under C. Hackers-for-Hire Targeting Legal Professionals.  [return](#)

[FN 206] Reuters, Dechert Resolves Claims Concerning Hired Hackers in Litigation-Related Operations (2025). <https://www.reuters.com/legal/litigation/dechert->

[resolves-claims-over-hired-hackers-2025-04-28/](#). *Application:* source support for the discussion under C. Hackers-for-Hire Targeting Legal Professionals.  [return](#)

[FN 207] Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; Administrative Office of the U.S. Courts, Judges Outline Accelerated Modernization of Case Management System (Mar. 10, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system>. *Application:* source support for the discussion under E. Court and Case-Management Infrastructure Attacks.  [return](#)

[FN 208] Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>. *Application:* source support for the discussion under E. Court and Case-Management Infrastructure Attacks.  [return](#)

[FN 209] Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf>. *Application:* source support for the discussion under E. Court and Case-Management Infrastructure Attacks.  [return](#)

[FN 210] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* source support for the discussion under E. Court and Case-Management Infrastructure Attacks.  [return](#)

[FN 211] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Federal Bureau of Investigation, Spoofing and Phishing. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/spoofing-and-phishing>. *Application:* BEC and spoofing as relationship exploitation.  [return](#)

[FN 212] Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023). <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>; United Kingdom National Cyber Security Centre, Cyber Threat Report: UK Legal Sector. <https://www.ncsc.gov.uk/report/cyber-threat-report-uk-legal-sector>; Microsoft, Expanding Cybersecurity Services for Attorneys Targeted by Nation-State Actors (June 12, 2024). <https://blogs.microsoft.com/on-the-issues/2024/06/12/cybersecurity-services-for-attorneys/>. *Application:*

independent reporting and government/provider recognition of legal-sector targeting. [↩ return](#)

[FN 213] U.S. Department of Justice, Justice Department Charges 12 Chinese Contract Hackers and Law-Enforcement Officers in Global Computer Intrusion Campaigns (Mar. 5, 2025). <https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global>; Reuters, Dechert Resolves Claims Concerning Hired Hackers in Litigation-Related Operations (2025). <https://www.reuters.com/legal/litigation/dechert-resolves-claims-over-hired-hackers-2025-04-28/>. *Application:* hackers-for-hire and litigation-related cyber operations. [↩ return](#)

[FN 214] Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; Administrative Office of the U.S. Courts, Judges Outline Accelerated Modernization of Case Management System (Mar. 10, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/03/10/judges-outline-accelerated-modernization-case-management-system>; Administrative Office of the U.S. Courts, Judiciary Approves Funding for Case Management and Public Access Modernization (June 26, 2026). <https://www.uscourts.gov/data-news/judiciary-news/2026/06/26/judiciary-approves-funding-case-management-and-public-access-modernization>; PACER / Administrative Office of the U.S. Courts, Multifactor Authentication Coming Soon (May 2, 2025), and subsequent NextGen CM/ECF implementation notices. <https://pacer.uscourts.gov/announcements/multifactor-authentication-coming-soon>; PACER, Additional Security Enhancements Coming Soon (June 27, 2025). <https://pacer.uscourts.gov/announcements/2025/06/27/additional-security-enhancements-coming-soon>; Administrative Office of the U.S. Courts, Court Operations—Annual Report 2025. <https://www.uscourts.gov/data-news/reports/annual-reports/directors-annual-report/annual-report-2025/court-operations-annual-report-2025>. *Application:* official acknowledgment and remediation of judicial case-management risk. [↩ return](#)

[FN 215] Microsoft Digital Crimes Unit, Fortra, Health-ISAC, and sworn declarations in Microsoft Corp. et al. v. John Does 1-2, No. 1:23-cv-02447 (E.D.N.Y.), together with the Sept. 8, 2025 permanent injunction. <https://blogs.microsoft.com/on-the-issues/2023/04/06/fortra-microsoft-health-isac-cobalt-strike-cracked-copies/>; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* controlled filing and court-authorized technical containment. [↩ return](#)

[FN 216] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal,

Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: transition from external mechanisms to field validation. [↩ return](#)

[FN 217] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application*: reason the Florida record functions as a longitudinal field case. [↩ return](#)

[FN 218] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Marlin Technologies, Expert Network and Endpoint Report (Dec. 5, 2024).; Team B, Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess e-Filing Portal datasets (2024-2025), Project artifacts.. *Application*: field-case selection based on complete source-to-consequence sequence. [↩ return](#)

[FN 219] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Marlin Technologies, Expert Network and Endpoint Report (Dec. 5, 2024).; Team B, Florida Bar Employee Portal, Florida Bar Membership Portal, and MyFLCourtAccess e-Filing Portal datasets (2024-2025), Project artifacts.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application*: contemporaneous documentation preceding terminal consequences. [↩ return](#)

[FN 220] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: mapping the field case to all authority rails. [↩ return](#)

[FN 221] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: plain-language authorship and participant disclosure. [↩ return](#)

[FN 222] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application*: evidentiary treatment of author-participant statements. [↩ return](#)

[FN 223] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: scope boundary for field validation. [↩ return](#)

[FN 224] The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: transition to the Florida discipline process primer. [↩ return](#)

[FN 225] Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: purpose of the Florida discipline primer. [↩ return](#)

[FN 226] The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: institutional allocation of authority in Florida lawyer discipline. [↩ return](#)

[FN 227] The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: ACAP intake and branch investigation. [↩ return](#)

[FN 228] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Grievance Committees (current public roster and committee overview, accessed

Sept. 16, 2026). <https://www.floridabar.org/about/cmtes/cmtes-gr/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: file identity and committee suffix as authority-bearing information.

 [return](#)

[FN 229] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: response notice, receipt, deficiency, and nonresponse states.  [return](#)

[FN 230] The Florida Bar, Grievance Committees (current public roster and committee overview, accessed Sept. 16, 2026). <https://www.floridabar.org/about/cmtes/cmtes-gr/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: grievance committee composition and function.  [return](#)

[FN 231] The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; The Florida Bar, Grievance Committees (current public roster and committee overview, accessed Sept. 16, 2026). <https://www.floridabar.org/about/cmtes/cmtes-gr/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: chair and investigating-member authority.  [return](#)

[FN 232] Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: designated reviewer and Board oversight.  [return](#)

[FN 233] The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: formal complaint and referee appointment.  [return](#)

[FN 234] The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar.

<https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: referee function and Supreme Court final authority.  [return](#)

[FN 235] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: case management, notice, and consolidation.  [return](#)

[FN 236] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: disciplinary evidence and source-layer distinctions.  [return](#)

[FN 237] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application*: default and its antecedent authority requirements.  [return](#)

[FN 238] Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: aggravation, mitigation, and sanction recommendation.  [return](#)

[FN 239] Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>; The Florida Bar, Count Amends Rules Concerning Emergency Suspensions When Lawyers Are Charged with a Felony (Sept. 5, 2023), reproducing Rule 3-5.2 procedures then governing petitions, formal-complaint status, answers, referee appointment, and expedited proceedings. <https://www.floridabar.org/the-florida-bar-news/count-amends-rules-concerning-emergency-suspensions-when-lawyers->

[are-charged-with-a-felony/](#). *Application:* historical Rule 3-5.2 emergency-suspension standard and authority.  [return](#)

[FN 240] Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>; The Florida Bar, Count Amends Rules Concerning Emergency Suspensions When Lawyers Are Charged with a Felony (Sept. 5, 2023), reproducing Rule 3-5.2 procedures then governing petitions, formal-complaint status, answers, referee appointment, and expedited proceedings. <https://www.floridabar.org/the-florida-bar-news/count-amends-rules-concerning-emergency-suspensions-when-lawyers-are-charged-with-a-felony/>. *Application:* petition as formal complaint, answer period, and prompt referee appointment.  [return](#)

[FN 241] Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>; The Florida Bar, Count Amends Rules Concerning Emergency Suspensions When Lawyers Are Charged with a Felony (Sept. 5, 2023), reproducing Rule 3-5.2 procedures then governing petitions, formal-complaint status, answers, referee appointment, and expedited proceedings. <https://www.floridabar.org/the-florida-bar-news/count-amends-rules-concerning-emergency-suspensions-when-lawyers-are-charged-with-a-felony/>. *Application:* motion to dissolve and expedited referee procedure.  [return](#)

[FN 242] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source provenance inside emergency-suspension affidavits.  [return](#)

[FN 243] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>. *Application:* Supreme Court review and contested/uncontested posture.  [return](#)

[FN 244] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Supreme Court of Florida, May 21, 2026 disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.; Brian D. Burgoon, Lawyer

Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: final disciplinary authority and permanent disbarment.  [return](#)

[FN 245] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application*: terminal order, costs, and publication as professional identity.  [return](#)

[FN 246] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida’s Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application*: transition from ordinary process to field deviations.  [return](#)

[FN 247] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: purpose of Field Validation One.  [return](#)

[FN 248] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: source support for the discussion under A. The 11L Control Baseline.  [return](#)

[FN 249] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: source support for the discussion under A. The 11L Control Baseline.  [return](#)

[FN 250] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: source support for the discussion under A. The 11L Control Baseline.  [return](#)

[FN 251] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’. *Application*: source support for the discussion under B. The September 17 Base-File Communication.  [return](#)

[FN 252] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’. *Application*: source support for the discussion under B. The September 17 Base-File Communication.  [return](#)

- [FN 253] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’. *Application:* source support for the discussion under B. The September 17 Base-File Communication. [↩ return](#)
- [FN 254] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* 11L matter as pre-incident control. [↩ return](#)
- [FN 255] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’. *Application:* September 17 represented file and response state. [↩ return](#)
- [FN 256] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’. *Application:* source-state checkpoint and required transition records. [↩ return](#)
- [FN 257] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under D. The 17F Referral and Womack Role Variants. [↩ return](#)
- [FN 258] The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source support for the discussion under D. The 17F Referral and Womack Role Variants. [↩ return](#)
- [FN 259] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under D. The 17F Referral and Womack Role Variants. [↩ return](#)
- [FN 260] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 (‘We have received the email that you sent last night at 7:20pm. Thank you.’).. *Application:* source support for the discussion under D. The 17F Referral and Womack Role Variants. [↩ return](#)
- [FN 261] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cyber=N.E.T.

Forensics, Second Supplemental Expert Avatar Report (Jan. 15, 2026), treated as a source reservoir only where supported by primary evidence.. *Application:* source support for the discussion under E. Weiss Chair Provenance. [!\[\]\(05ed99f561fd6053ce777c32283aee3d_img.jpg\) return](#)

[FN 262] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. Weiss Chair Provenance. [!\[\]\(8ce929a099a0fd2d5bbf036577b726a5_img.jpg\) return](#)

[FN 263] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Respondent's Motion for Order to Show Cause, SC2024-1681 (Feb. 27, 2025), including embedded Feb. 26 Weiss Serota communication directing future communications to Patricia Ann Toro Savitz at psavitz@floridabar.org.. *Application:* source support for the discussion under E. Weiss Chair Provenance. [!\[\]\(d7554398931fcb5834d8aea939ea59f0_img.jpg\) return](#)

[FN 264] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* source support for the discussion under E. Weiss Chair Provenance. [!\[\]\(5dea6a19c3c32a12a1f074e6fce1ec99_img.jpg\) return](#)

[FN 265] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* source support for the discussion under G. The 17F-to-17A Transition. [!\[\]\(4b294d924559403807fa5a60fb9fc1b3_img.jpg\) return](#)

[FN 266] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under G. The 17F-to-17A Transition. [!\[\]\(fbc0cdd52cb75d882c5fddc19e649478_img.jpg\) return](#)

[FN 267] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source support for the discussion under G. The 17F-to-17A Transition. [!\[\]\(b8830c021588891e9990d03ceb9bb5e3_img.jpg\) return](#)

[FN 268] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation,

and signature placement.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* committee identity and role as authority-bearing state. [↩ return](#)

[FN 269] Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* different role-assignment narratives within the same document series. [↩ return](#)

[FN 270] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Respondent's Motion for Order to Show Cause, SC2024-1681 (Feb. 27, 2025), including embedded Feb. 26 Weiss Serota communication directing future communications to Patricia Ann Toro Savitz at psavitz@floridabar.org.; Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report (Jan. 15, 2026), treated as a source reservoir only where supported by primary evidence.. *Application:* chair-roster conflict and overlapping adverse law-firm activity. [↩ return](#)

[FN 271] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* 17F-to-17A transition and missing transfer bridge. [↩ return](#)

[FN 272] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.. *Application:* synthesis and transition to response/nonresponse. [↩ return](#)

[FN 273] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.'). *Application:* purpose of Field Validation Two. [↩ return](#)

- [FN 274] Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.'). *Application*: source support for the discussion under C. October 14 Response and October 15 Receipt. [!\[\]\(dd267770bb8d478489478484c242cb1b_img.jpg\) return](#)
- [FN 275] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.'). *Application*: source support for the discussion under C. October 14 Response and October 15 Receipt. [!\[\]\(694273bf1c663f5a489038cdeb572b9e_img.jpg\) return](#)
- [FN 276] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application*: source support for the discussion under C. October 14 Response and October 15 Receipt. [!\[\]\(2975ef8dfee0fb93ee0afd2f82de00ea_img.jpg\) return](#)
- [FN 277] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: source support for the discussion under C. October 14 Response and October 15 Receipt. [!\[\]\(324a184ccdd5a90789881819b24814f0_img.jpg\) return](#)
- [FN 278] Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.'). *Application*: institutional receipt as controlling source state. [!\[\]\(fac41854343236de7f729adb96be06d0_img.jpg\) return](#)
- [FN 279] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.'). *Application*: separation of response receipt from sufficiency. [!\[\]\(36f42b07bf6cddfb548f7f0b840da38f_img.jpg\) return](#)
- [FN 280] Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application*: source support for the discussion under F. November 12 Deadline and Meeting Collision. [!\[\]\(1ba2de2b8c8e197396ddc055a3f3ef75_img.jpg\) return](#)
- [FN 281] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in

Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.. *Application:* source support for the discussion under F. November 12 Deadline and Meeting Collision.

 [return](#)

[FN 282] Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.');

Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.. *Application:* source support for the discussion under F. November 12 Deadline and Meeting Collision.

 [return](#)

[FN 283] Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* deadline and committee-date collision.

 [return](#)

[FN 284] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application:* physical delivery as attempted out-of-band verification.

 [return](#)

[FN 285] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* evidentiary function of out-of-band delivery.

 [return](#)

[FN 286] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* aggregated nonresponse petition and omitted response state.

 [return](#)

[FN 287] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 ('We have received the email that you sent last night at 7:20pm. Thank you.').; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application*: response-to-nonresponse authority conversion. [!\[\]\(ee28bce606e2d37171120e83682c1db9_img.jpg\) return](#)

[FN 288] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: bounded finding on missing response-state transition. [!\[\]\(4f97e81895879c5a84ed037660a7e593_img.jpg\) return](#)

[FN 289] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application*: transition to communications-authorship failure. [!\[\]\(90ed8598d63f63715c3c411e1ff296ae_img.jpg\) return](#)

[FN 290] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application*: purpose of Field Validation Three. [!\[\]\(a4e24a0f320eacbc3cf32e390ccc309c_img.jpg\) return](#)

[FN 291] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application*: source support for the discussion under A. The Berman Message and Repudiation. [!\[\]\(755e44246b0990e78b26fd36f13642ec_img.jpg\) return](#)

[FN 292] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application*: source support for the discussion under A. The Berman Message and Repudiation. [!\[\]\(4ab7bc89770c21ed7f7805ba532f8381_img.jpg\) return](#)

[FN 293] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application*: source support for the discussion under A. The Berman Message and Repudiation. [!\[\]\(b15a52694309ea4c274a394158422056_img.jpg\) return](#)

[FN 294] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical

source reconciliation.. *Application:* source support for the discussion under C.

March 18-20 Candor and Physical Reconciliation Request. [!\[\]\(748dc8d87d0f32ea3bb207b6d62ddceb_img.jpg\) return](#)

[FN 295] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under C. March 18-20 Candor and Physical Reconciliation Request. [!\[\]\(97b985f10292d65284476b0e77871f13_img.jpg\) return](#)

[FN 296] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under C. March 18-20 Candor and Physical Reconciliation Request. [!\[\]\(d687f41ee7eed47b6d58529359066db2_img.jpg\) return](#)

[FN 297] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* chronology and candor following repudiation. [!\[\]\(2febc8fd29307bcd54fa8da7cde7d167_img.jpg\) return](#)

[FN 298] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* intent and mitigation significance of seeking reconciliation. [!\[\]\(eb78d55b2f8ba643a351dd750205025d_img.jpg\) return](#)

[FN 299] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under B. Berrena's "Has Been Changed" Statement. [!\[\]\(1cc400d82f149188d6392e1d21bafad2_img.jpg\) return](#)

[FN 300] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under B. Berrena's "Has Been Changed" Statement. [!\[\]\(252401321ba480309c9ccf6d0e6447ec_img.jpg\) return](#)

[FN 301] Federal Bureau of Investigation, Business Email Compromise.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; The Florida Bar, Scam Alert: Fake Emails Claim to Be from the Bar's Executive Director (Nov. 5, 2019), <https://www.floridabar.org/the-florida-bar-news/scam-alert-fake-emails-claim-to-be-from-the-bars-executive-director/>.

Application: source support for the discussion under B. Berrena's "Has Been Changed" Statement. [↩ return](#)

[FN 302] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under D. Missing Forensic Attribution Bridge. [↩ return](#)

[FN 303] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under D. Missing Forensic Attribution Bridge. [↩ return](#)

[FN 304] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under D. Missing Forensic Attribution Bridge. [↩ return](#)

[FN 305] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* institutional acknowledgment of changed email content. [↩ return](#)

[FN 306] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* missing forensic evidence for authorship attribution. [↩ return](#)

[FN 307] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4,

2025), pp. 1-7, 13-24.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* bounded determination on the fabrication finding. [↩ return](#)

[FN 308] Federal Bureau of Investigation, Business Email Compromise.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>.

Application: containment obligation after institutional communication integrity failure. [↩ return](#)

[FN 309] Affidavit of John Berrena supporting the June 18, 2025 Petition for

Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11..

Application: transition to affidavit authority amplification. [↩ return](#)

[FN 310] Affidavit of John Berrena supporting the June 18, 2025 Petition for

Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.;

The Florida Bar, Count Amends Rules Concerning Emergency Suspensions When Lawyers Are Charged with a Felony (Sept. 5, 2023), reproducing Rule 3-5.2

procedures then governing petitions, formal-complaint status, answers, referee appointment, and expedited proceedings. <https://www.floridabar.org/the-florida-bar-news/count-amends-rules-concerning-emergency-suspensions-when-lawyers-are-charged-with-a-felony/>.

Application: purpose of Field Validation Four. [↩ return](#)

[FN 311] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency

Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; The Florida

Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>.

Application: source support for the discussion under A. Berrena Affidavit Source Layers. [↩ return](#)

[FN 312] Affidavit of John Berrena supporting the June 18, 2025 Petition for

Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11..

Application: source support for the discussion under A. Berrena Affidavit Source Layers. [↩ return](#)

[FN 313] Historical Impossibility of the Purported Permanent-Disbarment Path: A

Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John

Berrena supporting the June 18, 2025 Petition for Emergency Suspension,

paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under A. Berrena Affidavit Source Layers. [↩ return](#)

- [FN 314] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source-layer separation within the affidavit. [↩ return](#)
- [FN 315] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* method for evaluating affidavit propositions. [↩ return](#)
- [FN 316] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under B. Direct FBI Communications. [↩ return](#)
- [FN 317] Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* source support for the discussion under B. Direct FBI Communications. [↩ return](#)
- [FN 318] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under B. Direct FBI Communications. [↩ return](#)
- [FN 319] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* source support for the discussion under B. Direct FBI Communications. [↩ return](#)
- [FN 320] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under C. Omitted Qualifying Evidence. [↩ return](#)
- [FN 321] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under C. Omitted Qualifying Evidence. [↩ return](#)

[FN 322] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* source support for the discussion under C. Omitted Qualifying Evidence. [↩ return](#)

[FN 323] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* direct comparison between affidavit summary and FBI communications. [↩ return](#)

[FN 324] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* bounded FBI finding and rejection of categorical no-investigation summary. [↩ return](#)

[FN 325] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* omitted qualifying evidence affecting interpretation. [↩ return](#)

[FN 326] The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Florida Rules of General Practice and Judicial Administration, Florida Courts E-Filing Portal standards, and Rules Regulating The Florida Bar, operative historical and current versions. <https://www.floridabar.org/rules/rtrfb/>. *Application:* source support for the discussion under D. Emergency Petition as Authority Amplifier. [↩ return](#)

[FN 327] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under D. Emergency Petition as Authority Amplifier. [↩ return](#)

[FN 328] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and

SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under D. Emergency Petition as Authority Amplifier. [↩ return](#)

[FN 329] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; The Florida Bar, Count Amends Rules Concerning Emergency Suspensions When Lawyers Are Charged with a Felony (Sept. 5, 2023), reproducing Rule 3-5.2 procedures then governing petitions, formal-complaint status, answers, referee appointment, and expedited proceedings. <https://www.floridabar.org/the-florida-bar-news/count-amends-rules-concerning-emergency-suspensions-when-lawyers-are-charged-with-a-felony/>. *Application:* emergency affidavit to complaint, default, and sanction sequence. [↩ return](#)

[FN 330] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* bounded finding on affidavit provenance and authority amplification. [↩ return](#)

[FN 331] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* transition to adjudicative-state changes. [↩ return](#)

[FN 332] The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* purpose and role of the referee proceeding. [↩ return](#)

[FN 333] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>. *Application:* source

support for the discussion under A. August 8 Conference Without a Located Notice. [!\[\]\(b45e3730c89dd2ef339bd39434a0e45d_img.jpg\) return](#)

[FN 334] Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.. *Application:* source support for the discussion under A. August 8 Conference Without a Located Notice. [!\[\]\(679e73932001537df8fed751180004e8_img.jpg\) return](#)

[FN 335] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>. *Application:* source support for the discussion under A. August 8 Conference Without a Located Notice. [!\[\]\(b0bf7851bfd7de2284d5b04cb54a31a6_img.jpg\) return](#)

[FN 336] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.. *Application:* source support for the discussion under B. August 11 Order and August 12 Motion Sequence. [!\[\]\(98a45a4015fdcee784d8fa756361d6cc_img.jpg\) return](#)

[FN 337] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under B. August 11 Order and August 12 Motion Sequence. [!\[\]\(3eaabb1cc67b25848e6bfb3258d47a71_img.jpg\) return](#)

[FN 338] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.. *Application:* source support for the discussion under B. August 11 Order and August 12 Motion Sequence. [!\[\]\(76a7624be0fc480beb765315b5ac8389_img.jpg\) return](#)

[FN 339] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>. *Application:* source support for the discussion under B. August 11 Order and August 12 Motion Sequence. [!\[\]\(ae4f541fc0aca70dcac694110c448905_img.jpg\) return](#)

[FN 340] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under C. Default and Case-Identity Correction. [!\[\]\(9888f02200c020a2fabd750dc7194e9d_img.jpg\) return](#)

[FN 341] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Supreme Court of Florida, Aug. 4, 2025

Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.. *Application:* source support for the discussion under C. Default and Case-Identity Correction.  [return](#)

[FN 342] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under C. Default and Case-Identity Correction.  [return](#)

[FN 343] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.. *Application:* August 8-12 docket and order sequence.  [return](#)

[FN 344] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.. *Application:* notice as antecedent to default.  [return](#)

[FN 345] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.. *Application:* legal consequences of consolidation timing.  [return](#)

[FN 346] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.. *Application:* default and later case-identity correction.  [return](#)

[FN 347] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=. *Application:* source support for the discussion under D. September 30 / October 1 Temporal Insertion.  [return](#)

[FN 348] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025.

https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=.

Application: source support for the discussion under D. September 30 / October 1 Temporal Insertion. [↩ return](#)

[FN 349] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under D. September 30 / October 1 Temporal Insertion. [↩ return](#)

[FN 350] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under D. September 30 / October 1 Temporal Insertion. [↩ return](#)

[FN 351] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; *Strenger v. RMC Consulting, Inc.*, No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=. *Application:* temporal placement of the September 30 collateral order. [↩ return](#)

[FN 352] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* admitted-exhibit list and judicial-notice use. [↩ return](#)

[FN 353] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; *Strenger v. RMC Consulting, Inc.*, No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=. *Application:* notice and opportunity consequences of one-day temporal insertion. [↩ return](#)

[FN 354] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* transition to source-to-derivative amplification. [↩ return](#)

[FN 355] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* purpose of source-to-derivative analysis. [↩ return](#)

[FN 356] Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Final Judgment for Plaintiffs, *Insurance Office of America, Inc. et al. v. Farrow et al.*, No. 2020-CA-000725 (Fla. 18th Jud. Cir. Dec. 26, 2024), pp. 3-16.. *Application:* source support for the discussion under E. Source-Order Expansion in the November 4 Report. [↩ return](#)

- [FN 357] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application*: source support for the discussion under E. Source-Order Expansion in the November 4 Report. [↩ return](#)
- [FN 358] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application*: source support for the discussion under E. Source-Order Expansion in the November 4 Report. [↩ return](#)
- [FN 359] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application*: source support for the discussion under E. Source-Order Expansion in the November 4 Report. [↩ return](#)
- [FN 360] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Final Judgment for Plaintiffs, Insurance Office of America, Inc. et al. v. Farrow et al., No. 2020-CA-000725 (Fla. 18th Jud. Cir. Dec. 26, 2024), pp. 3-16.. *Application*: exact source-to-derivative comparison in the Seminole sequence. [↩ return](#)
- [FN 361] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Final Judgment for Plaintiffs, Insurance Office of America, Inc. et al. v. Farrow et al., No. 2020-CA-000725 (Fla. 18th Jud. Cir. Dec. 26, 2024), pp. 3-16.. *Application*: downstream effect of expanding draft conduct into filed conduct. [↩ return](#)
- [FN 362] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=. *Application*: Middle District source-order comparison. [↩ return](#)
- [FN 363] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025.

https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=.

Application: judicial authority transferred to an expanded proposition. [↩ return](#)

[FN 364] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under A. Source Proposition to Derivative Finding. [↩ return](#)

[FN 365] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.. *Application:* source support for the discussion under A. Source Proposition to Derivative Finding. [↩ return](#)

[FN 366] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under A. Source Proposition to Derivative Finding. [↩ return](#)

[FN 367] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under A. Source Proposition to Derivative Finding. [↩ return](#)

[FN 368] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application:* source support for the discussion under B. Derivative Finding to Official Public Record. [↩ return](#)

[FN 369] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Supreme Court of Florida, May 21, 2026 disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.. *Application:* source support for the discussion under B. Derivative Finding to Official Public Record. [↩ return](#)

[FN 370] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source

support for the discussion under B. Derivative Finding to Official Public Record.

 [return](#)

[FN 371] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.

<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>.

Application: source support for the discussion under B. Derivative Finding to Official Public Record.  [return](#)

[FN 372] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.

<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under C.

Public Record to Media and Search.  [return](#)

[FN 373] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv;

Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under C.

Public Record to Media and Search.  [return](#)

[FN 374] MITRE ATT&CK, T1565, Data Manipulation.

<https://attack.mitre.org/techniques/T1565/>; Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023).

<https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>.

Application: source support for the discussion under C. Public Record to Media and Search.  [return](#)

[FN 375] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source

support for the discussion under C. Public Record to Media and Search.  [return](#)

[FN 376] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv;

The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026.

<https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication

artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile

captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* multi-institution recursive amplification. [↩ return](#)

[FN 377] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* independence and dependency in authority stacks. [↩ return](#)

[FN 378] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source fidelity as protection of institutional authority. [↩ return](#)

[FN 379] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* transition to publication and media rails. [↩ return](#)

[FN 380] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* publication and media systems as authority rails. [↩ return](#)

[FN 381] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under D. The Terminal-Order Publication Anomaly. [↩ return](#)

[FN 382] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Supreme Court of Florida, May 21, 2026

disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.. *Application:* source support for the discussion under D. The Terminal-Order Publication Anomaly. [↩ return](#)

[FN 383] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under D. The Terminal-Order Publication Anomaly. [↩ return](#)

[FN 384] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Supreme Court of Florida, May 21, 2026 disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application:* terminal public status and wrong supporting-document path. [↩ return](#)

[FN 385] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application:* public document path as professional identity infrastructure. [↩ return](#)

[FN 386] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Supreme Court of Florida, May 21, 2026 disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.. *Application:* downstream significance of a terminal-document mismatch. [↩ return](#)

[FN 387] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler

Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under A. Byline and Publication Identity. [!\[\]\(b031865b899559cc68af31669ff7ece9_img.jpg\) return](#)

[FN 388] Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.; Wieder research package, including Wieder Dossier v.10, National Press Foundation profile research, McClatchy/Miami Herald author materials, telephone and email artifacts, and preserved screenshots.. *Application:* source support for the discussion under A. Byline and Publication Identity. [!\[\]\(16cb39f2c5dde85d43bc59355ae6ebae_img.jpg\) return](#)

[FN 389] Wieder research package, including Wieder Dossier v.10, National Press Foundation profile research, McClatchy/Miami Herald author materials, telephone and email artifacts, and preserved screenshots.; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under A. Byline and Publication Identity. [!\[\]\(edec62eaa4e19cb25faa1eb2c022ca3a_img.jpg\) return](#)

[FN 390] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under A. Byline and Publication Identity. [!\[\]\(792c157b08ca4b312ec2327e36d7a846_img.jpg\) return](#)

[FN 391] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under B. CMS, Syndication, and Republished Authority. [!\[\]\(2316339b7fcc7ac31f2aaab1990b3fd6_img.jpg\) return](#)

[FN 392] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under B. CMS, Syndication, and Republished Authority. [!\[\]\(7fa5ab4f7792cf387eb55b82e2fe60bb_img.jpg\) return](#)

[FN 393] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under B. CMS, Syndication, and Republished Authority. [!\[\]\(e7e47211fe1e5996134cb5995bcf5712_img.jpg\) return](#)

[FN 394] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support

for the discussion under B. CMS, Syndication, and Republished Authority.  [return](#)

[FN 395] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* source support for the discussion under C. Professional Profiles and Credential Laundering.  [return](#)

[FN 396] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application:* source support for the discussion under C. Professional Profiles and Credential Laundering.  [return](#)

[FN 397] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under C. Professional Profiles and Credential Laundering.  [return](#)

[FN 398] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, moclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under D. Search-Index Authority Stacking.  [return](#)

[FN 399] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under D. Search-Index Authority Stacking.  [return](#)

[FN 400] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under D. Search-Index Authority Stacking.  [return](#)

[FN 401] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development,

Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under D. Search-Index Authority Stacking.  [return](#)

[FN 402] Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.; Wieder research package, including Wieder Dossier v.10, National Press Foundation profile research, McClatchy/Miami Herald author materials, telephone and email artifacts, and preserved screenshots.; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* event-specific media authority analysis.  [return](#)

[FN 403] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>. *Application:* CMS compromise and derivative-wrapper mechanisms.  [return](#)

[FN 404] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* authority transclusion through derivative republication.  [return](#)

[FN 405] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv=; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* media authority converted into judicial authority.  [return](#)

[FN 406] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* search-index authority stacking and correction strategy.  [return](#)

[FN 407] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* transition to the Clean Adjudicative Environment. [!\[\]\(59aab71b78f6976850ef9b998f61c7a9_img.jpg\) return](#)

[FN 408] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* circularity of proving compromise through the disputed channel. [!\[\]\(61adf492115e5370cefe707cbff8d382_img.jpg\) return](#)

[FN 409] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Microsoft Digital Crimes Unit, Fortra, Health-ISAC, and sworn declarations in Microsoft Corp. et al. v. John Does 1-2, No. 1:23-cv-02447 (E.D.N.Y.), together with the Sept. 8, 2025 permanent injunction. <https://blogs.microsoft.com/on-the-issues/2023/04/06/fortra-microsoft-health-isac-cobalt-strike-cracked-copies/>. *Application:* source support for the discussion under A. The Civil Cyber-Infrastructure Model. [!\[\]\(2a6ecdb9b259debd98ee67d4c1e8f1fc_img.jpg\) return](#)

[FN 410] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under A. The Civil Cyber-Infrastructure Model. [!\[\]\(a7f0ce2e7629ec5079603dcc53d91068_img.jpg\) return](#)

[FN 411] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* source support for the discussion under A. The Civil Cyber-Infrastructure Model. [!\[\]\(67e138e2cc53b6b871748d43f446569a_img.jpg\) return](#)

[FN 412] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under A. The Civil Cyber-Infrastructure Model. [!\[\]\(cd672dea2713c38ec97aeac6ab3a4f6c_img.jpg\) return](#)

[FN 413] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance

and post-2025 sensitive-document handling materials.

<https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* definition and limits of a Clean Adjudicative Environment.  [return](#)

[FN 414] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Microsoft Digital Crimes Unit, Fortra, Health-ISAC, and sworn declarations in Microsoft Corp. et al. v. John Does 1-2, No. 1:23-cv-02447 (E.D.N.Y.), together with the Sept. 8, 2025 permanent injunction. <https://blogs.microsoft.com/on-the-issues/2023/04/06/fortra-microsoft-health-isac-cobalt-strike-cracked-copies/>; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* analogy to civil disruption remedies and highly sensitive document procedures.  [return](#)

[FN 415] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under B. S.D. Florida Field Test.  [return](#)

[FN 416] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under B. S.D. Florida Field Test.  [return](#)

[FN 417] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under B. S.D. Florida Field Test.  [return](#)

[FN 418] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under C. E.D.N.Y. Field Test.  [return](#)

[FN 419] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under C. E.D.N.Y. Field Test.  [return](#)

[FN 420] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32,

55-96, 124-136.. *Application:* source support for the discussion under C. E.D.N.Y.

Field Test. [!\[\]\(0caf4cbec0748cfa42e6d04b8736d8f1_img.jpg\) return](#)

[FN 421] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under D. D.D.C. Field Test. [!\[\]\(996b1298432cbd4ddbe3af24648cfe7a_img.jpg\) return](#)

[FN 422] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under D. D.D.C. Field Test. [!\[\]\(a9372630ea6af351197bea8c57ddb161_img.jpg\) return](#)

[FN 423] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. Florida Supreme Court Original-Writ and

Secure-Handling Field Test. [!\[\]\(f6169b5357590c8cae88f8b0da545bad_img.jpg\) return](#)

[FN 424] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. Florida Supreme Court Original-Writ and

Secure-Handling Field Test. [!\[\]\(3139d17c58f097dfa25be2d561294d3e_img.jpg\) return](#)

[FN 425] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under E. Florida Supreme Court Original-Writ and

Secure-Handling Field Test. [!\[\]\(fbdf1951ccf99e3b94f739c8c2a25267_img.jpg\) return](#)

[FN 426] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under F. Cross-Jurisdiction

Synthesis. [!\[\]\(0f01c0e79b2bb3d9dbdec48290ce144d_img.jpg\) return](#)

[FN 427] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:*

source support for the discussion under F. Cross-Jurisdiction Synthesis. [!\[\]\(48b146703f622ab2c108f9d741cf70ae_img.jpg\) return](#)

[FN 428] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136..

Application: source support for the discussion under F. Cross-Jurisdiction

Synthesis. [!\[\]\(4d5fb7c3961ad2e2ec55b528d157a39f_img.jpg\) return](#)

[FN 429] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-

First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application*: cross-jurisdiction attempts to obtain controlled technical review. [↩ return](#)

[FN 430] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: cross-jurisdiction clean-channel failure. [↩ return](#)

[FN 431] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: institutional integrity escalation as a security control. [↩ return](#)

[FN 432] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application*: transition to operational detection method. [↩ return](#)

[FN 433] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application*: purpose of the Authority-Provenance Detection Method. [↩ return](#)

[FN 434] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application*: baseline establishment before anomaly analysis. [↩ return](#)

[FN 435] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; David Temoshok et al., National Institute of Standards and Technology, Digital Identity Guidelines: Identity Proofing and Enrollment, NIST SP 800-63A-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63A-4>. *Application*: event-specific identity and role verification. [↩ return](#)

- [FN 436] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; David Temoshok et al., National Institute of Standards and Technology, Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63B-4>; Justin Richer et al., National Institute of Standards and Technology, Digital Identity Guidelines: Federation and Assertions, NIST SP 800-63C-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63C-4>. *Application*: credential and authorization-object analysis.  [return](#)
- [FN 437] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application*: native evidence preservation and copy comparison.  [return](#)
- [FN 438] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application*: version comparison and preservation after changed-email statement.  [return](#)
- [FN 439] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Final Judgment for Plaintiffs, Insurance Office of America, Inc. et al. v. Farrow et al., No. 2020-CA-000725 (Fla. 18th Jud. Cir. Dec. 26, 2024), pp. 3-16.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv. *Application*: source-to-derivative comparison method.  [return](#)
- [FN 440] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: source-state transition ledger.  [return](#)

- [FN 441] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* dependency and propagation mapping.  [return](#)
- [FN 442] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* confidence discipline and correction before perfect attribution.  [return](#)
- [FN 443] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Federal Bureau of Investigation, Spoofing and Phishing. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/spoofing-and-phishing>. *Application:* known-clean out-of-band verification.  [return](#)
- [FN 444] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* institutional-state containment in addition to technical remediation.  [return](#)
- [FN 445] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* transition to meaningfully timed response.  [return](#)
- [FN 446] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST

SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* meaningfully timed relief and containment before complete attribution.  [return](#)

[FN 447] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under A. First Six Hours.  [return](#)

[FN 448] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* source support for the discussion under A. First Six Hours.  [return](#)

[FN 449] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* source support for the discussion under A. First Six Hours.  [return](#)

[FN 450] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under A. First Six Hours.  [return](#)

[FN 451] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* first-six-hour preservation package.  [return](#)

[FN 452] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; American Bar Association Formal Opinion 477R, Securing Communication of Protected Client Information (May 11, 2017). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477r.pdf; American Bar Association Formal Opinion

483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018).

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* clean-contact roster and continuity communications.  [return](#)

[FN 453] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018).

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* critical legal and publication clocks.  [return](#)

[FN 454] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems.

<https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under B. Six-to-Twenty-Four-Hour Authority Map.  [return](#)

[FN 455] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; MITRE ATT&CK, T1078, Valid Accounts.

<https://attack.mitre.org/techniques/T1078/>. *Application:* source support for the discussion under B. Six-to-Twenty-Four-Hour Authority Map.  [return](#)

[FN 456] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>;

Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under B. Six-to-Twenty-Four-Hour Authority Map.  [return](#)

[FN 457] Federal Bureau of Investigation, Business Email Compromise.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* source support for the discussion under D. Out-of-Band Verification and Evidence Preservation.  [return](#)

[FN 458] Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for

the discussion under D. Out-of-Band Verification and Evidence Preservation.  [return](#)

[FN 459] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32,

55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* source support for the discussion under D. Out-of-Band Verification and Evidence Preservation.  [return](#)

[FN 460] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* authority map structure.  [return](#)

[FN 461] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* specific preservation requests.  [return](#)

[FN 462] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* narrow integrity notice.  [return](#)

[FN 463] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under C. Twenty-Four-to-Seventy-Two-Hour Source-State Reconstruction.  [return](#)

[FN 464] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application:* source support for the discussion under C. Twenty-Four-to-Seventy-Two-Hour Source-State Reconstruction.  [return](#)

[FN 465] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile

captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under C. Twenty-Four-to-Seventy-Two-Hour Source-State Reconstruction.  [return](#)

[FN 466] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; American Bar Association Formal Opinion 477R, Securing Communication of Protected Client Information (May 11, 2017). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf. *Application:* source support for the discussion under E. Business, Client, Litigation, and Reputational Continuity.  [return](#)

[FN 467] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under E. Business, Client, Litigation, and Reputational Continuity.  [return](#)

[FN 468] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* source support for the discussion under E. Business, Client, Litigation, and Reputational Continuity.  [return](#)

[FN 469] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* 72-hour source-state ledger.  [return](#)

[FN 470] American Bar Association Formal Opinion 477R, Securing Communication of Protected Client Information (May 11, 2017). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_483.pdf

[ponsibility/ethics-opinions/aba-formal-op-483.pdf](#). *Application:* business, client, litigation, and reputational continuity.  [return](#)

- [FN 471] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source-first correction strategy.  [return](#)
- [FN 472] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* post-72-hour reconciliation and versioned findings.  [return](#)
- [FN 473] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* ongoing re-entry and authority-state monitoring.  [return](#)
- [FN 474] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* transition to institutional recommendations.  [return](#)
- [FN 475] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* distributed institutional responsibility.  [return](#)
- [FN 476] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly->

[sensitive-documents](#). *Application:* source support for the discussion under A. Courts and Clerks.  [return](#)

[FN 477] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under A. Courts and Clerks.  [return](#)

[FN 478] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; PACER / Administrative Office of the U.S. Courts, Multifactor Authentication Coming Soon (May 2, 2025), and subsequent NextGen CM/ECF implementation notices. <https://pacer.uscourts.gov/announcements/multifactor-authentication-coming-soon>. *Application:* source support for the discussion under A. Courts and Clerks.  [return](#)

[FN 479] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>. *Application:* source support for the discussion under B. Bar and Regulatory Bodies.  [return](#)

[FN 480] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under B. Bar and Regulatory Bodies.  [return](#)

[FN 481] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application:* source support for the discussion under B. Bar and Regulatory Bodies.  [return](#)

[FN 482] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance

and post-2025 sensitive-document handling materials.

<https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* court integrity-escalation protocol.  [return](#)

[FN 483] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* provenance for corrected and superseded court states.  [return](#)

[FN 484] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application:* regulatory state authentication and publication integrity.  [return](#)

[FN 485] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under C. Law Firms and Legal Departments.  [return](#)

[FN 486] American Bar Association Formal Opinion 477R, Securing Communication of Protected Client Information (May 11, 2017). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* source support for the discussion under C. Law Firms and Legal Departments.  [return](#)

[FN 487] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. *Application:* source support for the discussion under C. Law Firms and Legal Departments.  [return](#)

- [FN 488] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* source support for the discussion under D. Cybersecurity and MDR/IR Providers.  [return](#)
- [FN 489] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under D. Cybersecurity and MDR/IR Providers.  [return](#)
- [FN 490] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under D. Cybersecurity and MDR/IR Providers.  [return](#)
- [FN 491] Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; American Bar Association Formal Opinion 477R, Securing Communication of Protected Client Information (May 11, 2017). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* law-firm authority inventory and continuity planning.  [return](#)
- [FN 492] Federal Bureau of Investigation, Business Email Compromise. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; Federal Bureau of Investigation, Spoofing and Phishing. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/spoofing-and-phishing>. *Application:* authority-anomaly training.  [return](#)
- [FN 493] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business

Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* legal control-plane incident response as a complementary specialty.  [return](#)

[FN 494] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* source support for the discussion under E. Media and Public-Record Publishers.  [return](#)

[FN 495] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under E. Media and Public-Record Publishers.  [return](#)

[FN 496] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* source support for the discussion under E. Media and Public-Record Publishers.  [return](#)

[FN 497] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* source support for the discussion under F. Professional Identity and Credential Systems.  [return](#)

[FN 498] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under F. Professional Identity and Credential Systems.  [return](#)

[FN 499] Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:*

source support for the discussion under F. Professional Identity and Credential Systems. [↩ return](#)

[FN 500] Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* media versioning and byline provenance. [↩ return](#)

[FN 501] Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* derivative publication transparency and correction. [↩ return](#)

[FN 502] National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>. *Application:* separation of stable identity from event-specific authority. [↩ return](#)

[FN 503] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.. *Application:* transition to integrated determinations. [↩ return](#)

[FN 504] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* synthesis orientation. [↩ return](#)

[FN 505] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under A. Identity Is an Operational Control Layer. [↩ return](#)

[FN 506] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.. *Application:* source support for the discussion under A. Identity Is an Operational Control Layer. [↩ return](#)

- [FN 507] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* source support for the discussion under B. Real People and Real Systems Can Carry Counterfeit Authority. [↩ return](#)
- [FN 508] MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>. *Application:* source support for the discussion under B. Real People and Real Systems Can Carry Counterfeit Authority. [↩ return](#)
- [FN 509] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* authority as cyber infrastructure. [↩ return](#)
- [FN 510] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>. *Application:* genuine components carrying a false relationship. [↩ return](#)
- [FN 511] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under C. The Accepted State Is the Operational Objective. [↩ return](#)
- [FN 512] The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>. *Application:* source support for the discussion under C. The Accepted State Is the Operational Objective. [↩ return](#)
- [FN 513] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.. *Application:* source support for the discussion under D. Honest Institutional Reliance Can Be Weaponized. [↩ return](#)
- [FN 514] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under D. Honest Institutional Reliance Can Be Weaponized. [↩ return](#)
- [FN 515] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal,

Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* accepted state as the decisive operational objective. [↩ return](#)

[FN 516] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; *Strenger v. RMC Consulting, Inc.*, No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-. *Application:* time as an authority rail. [↩ return](#)

[FN 517] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, *The Florida Bar v. Farrow*, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mcclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application:* recursive amplification and dependency. [↩ return](#)

[FN 518] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under E. Authority-Rail Manipulation Is a Distinctive cAPTure-to-Kill Capability. [↩ return](#)

[FN 519] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application:* source support for the discussion under E. Authority-Rail Manipulation Is a Distinctive cAPTure-to-Kill Capability. [↩ return](#)

[FN 520] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>. *Application:* integrated Authority-Rail capability within cAPTure-to-Kill. [↩ return](#)

[FN 521] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat->

[enterprises](#); Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023), <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>. *Application*: bounded statement of the report's contribution.  [return](#)

[FN 522] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025), <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems, <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application*: operational determination on containment.  [return](#)

[FN 523] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials, <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application*: final institutional determination.  [return](#)

[FN 524] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.. *Application*: transition to conclusion.  [return](#)

[FN 525] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6, <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>. *Application*: conclusion: evolution from avatar-persona inquiry to authority-rail inquiry.  [return](#)

[FN 526] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, CM/ECF and PACER historical and technical materials, <https://www.uscourts.gov/court-records/electronic-filing->

[cm-ecf](#). *Application*: conclusion: authority as attack surface and trust-conversion chain. [↩ return](#)

[FN 527] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>.

Application: conclusion: official appearance and limits of authentication. [↩ return](#)

[FN 528] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>. *Application*: conclusion: genuine components and false relationships. [↩ return](#)

[FN 529] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; Federal Bureau of Investigation / Internet Crime Complaint Center, Senior U.S. Officials Impersonated in Malicious Messaging Campaign (May 15, 2025). <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>. *Application*: conclusion: natural person versus operator and event. [↩ return](#)

[FN 530] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.. *Application*: conclusion: recap of eight authority rails. [↩ return](#)

[FN 531] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida's Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Brian D. Burgoon, Lawyer Discipline—A Roadmap to Florida's Lawyer Regulation System, 98 Fla. B.J. 8 (May/June 2024). <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>

[journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/](#).

Application: conclusion: rails mapped to legal process. [↩ return](#)

[FN 532] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>.

Application: conclusion: source-first method and separate evidence states. [↩ return](#)

[FN 533] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-.

Application: conclusion: chronology and state-transition method. [↩ return](#)

[FN 534] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* conclusion: event-mechanism-attribution discipline.

[↩ return](#)

[FN 535] Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025). <https://doi.org/10.6028/NIST.SP.800-63-4>; U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic->

[of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue](#); Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>. *Application*: conclusion: independent capability corroboration. [↩ return](#)

[FN 536] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: conclusion: separation and convergence of field and external sources. [↩ return](#)

[FN 537] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application*: conclusion: author-participant disclosure and source controls. [↩ return](#)

[FN 538] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: conclusion: uL baseline. [↩ return](#)

[FN 539] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.; Farrow et al. v. IOA Group, LLC et al., No. 1:25-cv-20544 (S.D. Fla.), Verified Complaint filed Feb. 5, 2025, related filings, and Feb. 8 affidavit of Dr. Jane Doe.. *Application*: conclusion: preexisting cyber-integrity record. [↩ return](#)

[FN 540] Email attributed to John Derek Womack to Jay Lewis Farrow (Sept. 17, 2024), with chain and signature block identifying ‘J. Derek Womack, Senior Litigation Attorney.’; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 (‘We have received the email that you sent last night at 7:20pm. Thank you.’). *Application:* conclusion: September communication and October receipt control. [!\[\]\(97381344c44b7425ced73466b6343f89_img.jpg\) return](#)

[FN 541] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Florida Bar letters and Notices of Assignment attributed to John D. Womack and transmitted Oct. 15-18, 2024, identifying Richard Jay Weiss as 17F Chair and using varying investigating-member language, typography, name presentation, and signature placement.; The Florida Bar, Lawyer Discipline: A Roadmap to Florida’s Lawyer Regulation System, and Rules Regulating The Florida Bar. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>; Cyber-N.E.T. Forensics, Second Supplemental Expert Avatar Report (Jan. 15, 2026), treated as a source reservoir only where supported by primary evidence..

Application: conclusion: committee and role provenance. [!\[\]\(7a42230c24529ce5bb7ba161abd16906_img.jpg\) return](#)

[FN 542] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* conclusion: deadline collision, physical delivery, and aggregated nonresponse. [!\[\]\(c2db7765b8edc602be58f8149cec0ee2_img.jpg\) return](#)

[FN 543] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Jay Lewis Farrow consolidated response transmitted Oct. 14, 2024, and Christine Mitchell acknowledgment dated Oct. 15, 2024 (‘We have received the email that you sent last night at 7:20pm. Thank you.’); The Florida Bar, Petition for Contempt and Order to Show Cause and Possible Venue filing, Filing No. 211689379 (Nov. 25, 2024), SC2024-1681.. *Application:* conclusion: response-to-nonresponse conversion. [!\[\]\(88c679da45f3ab495bdcc1d85f6bf1ad_img.jpg\) return](#)

[FN 544] March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena’s statement that an email ‘was not the email I sent you’ and ‘has been changed,’ and the request for physical source reconciliation.. *Application:* conclusion: Berman message, repudiation, and candor. [!\[\]\(f358a2bd23d913e35d2ba2871225e8e9_img.jpg\) return](#)

[FN 545] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4,

2025), pp. 1-7, 13-24.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* conclusion: changed-email statement and missing attribution bridge. [↩ return](#)

[FN 546] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; Direct FBI communications and Teleporter records, Sept. 2024, concerning meetings, evidence uploads, contemplated computer-analysis response-team review of telephones, and continuing review of submitted material.. *Application:* conclusion: affidavit-FBI comparison. [↩ return](#)

[FN 547] Affidavit of John Berrena supporting the June 18, 2025 Petition for Emergency Suspension, paragraphs 4-19 and Composite Exhibits A-1 through A-11.; March 12-20, 2025 Berman/Berrena/Farrow communications and filings, including proposed dismissal terms, repudiation, Berrena's statement that an email 'was not the email I sent you' and 'has been changed,' and the request for physical source reconciliation.. *Application:* conclusion: omitted qualifying evidence. [↩ return](#)

[FN 548] Florida Appellate Case Information System docket exports for SC2024-1681 and SC2025-0863, captured Sept. 2026. <https://acis.flcourts.gov/>; Referee Case Management Order entered Aug. 11, 2025; written Motion to Consolidate and consolidation orders entered Aug. 12, 2025.; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.. *Application:* conclusion: notice, consolidation, default, and correction. [↩ return](#)

[FN 549] Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-. *Application:* conclusion: September 30/October 1 temporal insertion. [↩ return](#)

[FN 550] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Final Judgment for Plaintiffs, Insurance Office of America, Inc. et al. v. Farrow et al., No. 2020-CA-000725 (Fla. 18th Jud. Cir. Dec. 26, 2024), pp. 3-16.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv-. *Application:* conclusion: source-to-derivative expansion. [↩ return](#)

[FN 551] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar,

Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Supreme Court of Florida, May 21, 2026 disposition in SC2024-1681 / SC2025-0863 approving the referee report and imposing permanent disbarment and costs.; Supreme Court of Florida, Aug. 4, 2025 Emergency Suspension Order as later presented in a 'CORRECTED ORDER' version with a Sept. 30 footnote adding 2025-70,622(17A)(FES), together with the Bar's Aug. 7 correction motion and Sept. 30 clerk order.; The Florida Bar, Instructions to View Discipline Documents. <https://www.floridabar.org/public/acap/instructions/>. *Application*: conclusion: terminal public profile and supporting-document mismatch.  [return](#)

[FN 552] MITRE ATT&CK, T1656, Impersonation.

<https://attack.mitre.org/techniques/T1656/>; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>; U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Recorded Future Insikt Group, Synthetic Identities: A Dual Threat to Enterprises (Oct. 1, 2025), pp. 1-6. <https://www.recordedfuture.com/research/synthetic-identities-dual-threat-enterprises>; Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Administrative Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025). <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023). <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>. *Application*: conclusion: independent component capabilities.  [return](#)

[FN 553] Federal Bureau of Investigation, Business Email Compromise.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>; U.S. Department of Justice, Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote IT Worker Schemes (June 30, 2025). <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>; Federal Bureau of Investigation, DPRK Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue (May 16, 2024). <https://www.fbi.gov/investigate/cyber/alerts/2024/democratic-peoples-republic-of-korea-leverages-us-based-individuals-to-defraud-us-businesses-and-generate-revenue>; KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us (July 23, 2024). <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>. *Application*: conclusion: genuine enterprise authority issued to wrong operator.  [return](#)

[FN 554] Microsoft Threat Intelligence, Defending Against Evolving Identity Attack Techniques (May 29, 2025). <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>; Microsoft Security Response Center, Results of Major Technical Investigations for Storm-0558 Key Acquisition (Sept. 6, 2023). <https://www.microsoft.com/en-us/security/blog/2023/09/06/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Amazon Web Services, Route 53 API: ChangeResourceRecordSets and IAM service-authorization documentation. https://docs.aws.amazon.com/Route53/latest/APIReference/API_ChangeResourceRecordSets.html. *Application*: conclusion: persistence beyond password and endpoint.  [return](#)

[FN 555] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Raphael Satter, Hackers-for-Hire Targeted Lawyers and Law Firms, Reuters (June 29, 2023). <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>; Microsoft, Expanding Cybersecurity Services for Attorneys Targeted by Nation-State Actors (June 12, 2024). <https://blogs.microsoft.com/on-the-issues/2024/06/12/cybersecurity-services-for-attorneys/>. *Application*: conclusion: legal-sector amplification.  [return](#)

[FN 556] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Preserved media and derivative-publication artifacts, including April 2, 2024 @benbwieder post, Miami Herald author/profile captures, mclatchydc.com email presentation, Proton tips address, PPPFraudChronicle republishing, 'Swindler Barbie' graphic, and article-distribution screenshots.. *Application*: conclusion: authority stacking and dependency mapping.  [return](#)

[FN 557] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST

SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* conclusion: urgency and containment before complete attribution.  [return](#)

[FN 558] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* conclusion: first-hours preservation and continuity.  [return](#)

[FN 559] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* conclusion: authority map and narrow preservation requests.  [return](#)

[FN 560] Cyber-N.E.T. Forensics / Bridge-Gate E.S.S., Restricted Access Portal Solutions materials, as integrated in the September 2026 cAPTure and Civil Cyber-Infrastructure reports.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>. *Application:* conclusion: state reconstruction and dual-track correction.  [return](#)

[FN 561] Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data

Breach or Cyberattack (Oct. 17, 2018).

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application:* conclusion: meaningfully timed relief.  [return](#)

[FN 562] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* conclusion: cross-jurisdiction circularity.  [return](#)

[FN 563] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application:* conclusion: Clean Adjudicative Environment.  [return](#)

[FN 564] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; The Florida Bar, Member Profile and Discipline Documents for Jay Lewis Farrow, Bar No. 625213, captured Sept. 2026. <https://www.floridabar.org/public/acap/disc-docs/?icn=202570622&member=625213>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. *Application:* conclusion: institutional responsibilities.  [return](#)

[FN 565] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>. *Application:* conclusion: protecting institutions and honest actors.  [return](#)

[FN 566] Cyber-N.E.T. Forensics, Cryptographic-Counterfeit Defense Group Report (Feb. 25, 2026), pp. 2-8, 21-29, 40-48.; Scott Rose et al., National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207 (Aug. 2020). <https://doi.org/10.6028/NIST.SP.800-207>; National Institute of Standards and

Technology, Digital Identity Guidelines, NIST SP 800-63-4 (July 2025).
<https://doi.org/10.6028/NIST.SP.800-63-4>. *Application:* conclusion: limits of conventional security controls.  [return](#)

[FN 567] O.R.A.C.L.E. Logistics Team, Online Reputation and Credential Laundering Exposure Expert Report, Version 30 (Jan. 20, 2026), controlling first-draft baseline.; Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>; MITRE ATT&CK, T1565, Data Manipulation. <https://attack.mitre.org/techniques/T1565/>. *Application:* conclusion: mature avatar threat.  [return](#)

[FN 568] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application:* conclusion: accepted state as objective.  [return](#)

[FN 569] Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.; Oct. 31, 2024 letters in Florida Bar File Nos. 2025-70,132(17F) and 2025-70,140(17F), each setting Nov. 12, 2024 as the deadline before forwarding to the grievance committee; compared with committee-meeting materials and the Nov. 25 petition.; Report of Referee, The Florida Bar v. Farrow, SC2024-1681 / SC2025-0863, Filing No. 235057778 (Nov. 4, 2025), pp. 1-7, 13-24.; Strenger v. RMC Consulting, Inc., No. 2:23-cv-01226 (M.D. Fla.), orders dated Feb. 18, Mar. 19, May 23, and Sept. 30, 2025. https://ecf.flmd.uscourts.gov/cgi-bin/show_public_doc?2023-01226-49-2-cv. *Application:* conclusion: time and derivative authority.  [return](#)

[FN 570] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Cyber-N.E.T. Forensics, Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report (Oct. 22, 2025), pp. 1-24, 69-203, 238-267, and appendices. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>; MITRE ATT&CK, T1585, Establish Accounts. <https://attack.mitre.org/techniques/T1585/>; MITRE ATT&CK, T1656, Impersonation. <https://attack.mitre.org/techniques/T1656/>; MITRE ATT&CK, T1078, Valid Accounts. <https://attack.mitre.org/techniques/T1078/>; MITRE ATT&CK, T1565, Data Manipulation. <https://attack.mitre.org/techniques/T1565/>; MITRE ATT&CK, T1199, Trusted Relationship. <https://attack.mitre.org/techniques/T1199/>. *Application:* conclusion: distinctive capability.  [return](#)

[FN 571] National Institute of Standards and Technology, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST SP 800-61 Rev. 3 (Apr. 2025). <https://doi.org/10.6028/NIST.SP.800-61r3>; Cybersecurity and Infrastructure Security Agency, Cloud Identity and Access Management: Recommended Best Practices for Administrators (May 2025). <https://www.cisa.gov/resources-tools/resources/cloud-identity-and-access-management-recommended-best-practices-administrators>; Cybersecurity and Infrastructure Security Agency, Use Logging on Business Systems. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>; American Bar Association Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf. *Application*: conclusion: response determination.  [return](#)

[FN 572] Jay Lewis Farrow, Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes (Sept. 10, 2026), pp. 6-12, 23-32, 55-96, 124-136.; Administrative Office of the U.S. Courts, Highly Sensitive Documents guidance and post-2025 sensitive-document handling materials. <https://www.uscourts.gov/court-records/electronic-filing-cm-ecf/highly-sensitive-documents>. *Application*: conclusion: need for controlled integrity path.  [return](#)

[FN 573] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: conclusion: final synthesis.  [return](#)

[FN 574] Cyber-N.E.T. Forensics, cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat (Sept. 2026), pp. 4-18, 22-46, 68-106.; Historical Impossibility of the Purported Permanent-Disbarment Path: A Source-First Legal, Public-Record, and Forensic Reconstruction of SC2024-1681 and SC2025-0863 (Sept. 14, 2026), pp. 2-10, 18-31, 43-74, 82-92, 102-116.. *Application*: conclusion: governing final principle.  [return](#)