

ASSOCIATED CYBERSECURITY INCIDENT SUPPORT COLLABORATIVE (ACIS COLAB)

Deepfake Forensic Incident Response & Environment Team (DF-F.I.R.E. Team)

OCTOBER 25, 2026

PHP CYBER EMERGENCY AUTHORITY-AVATAR THREAT REPORT

Weaponized Professional Personas, Credentialed Identity Substitution & Counterfeit Authority
Across Law Firms, Courts and Active Litigation



**Pre-/Post-PHP Cyber-Emergency Legal-Fiduciary Sector Threat Assessment, Emergency
Containment and Digital-Empirical Environments Preservation & Restoration Report**

About the ACIS COLAB – DF-F.I.R.E. Team

The Associated Cybersecurity Incident Support Collaborative (“ACIS COLAB”) is an incident-support and threat-research environment organized around a practical premise: modern cyber incidents rarely remain confined to a single endpoint, mailbox, website, network, institution, or victim. Advanced threat actors increasingly operate across interconnected digital ecosystems in which identity, professional authority, communications, cloud services, websites, credentials, vendor relationships, portals, records, and institutional workflows function together. The ACIS COLAB therefore approaches a significant cyber event as an environmental incident—one requiring reconstruction of the digital and institutional system through which the threat actor obtained access, maintained persistence, exercised authority, and produced downstream consequences.

Within that collaborative structure, the Deepfake Forensic Incident Response & Environment Team (“DF-F.I.R.E. Team”) is a rapid-response forensic and threat-research team dedicated to detecting, researching, mapping, containing, reconstructing, and studying cyber-attacks involving professional identity, credentialed authority, intake, routing, communications, institutional reliance, and persistent record state. Its principal investigative focus is the point at which control of a technical system becomes control of a trusted human or institutional relationship.

DF-F.I.R.E. therefore begins with the source object and the consequential act. The Team separately establishes the identity represented, credential or account used, role asserted, communications path, technical control mechanism, recipient population, institutional reliance, and resulting state. It then follows that state forward into later communications, filings, docket entries, payment instructions, publications, disciplinary or regulatory records, professional profiles, judicial actions, or other decisions. This method prevents a technical event from being severed from the institutional consequence it was designed to produce.

The approach reflects lessons developed across prior cyber-forensic research concerning advanced persistent threats, legal-sector compromise, valid-account abuse, portal infiltration, DNS and mail-routing manipulation, counterfeit electronic service, synthetic or co-opted professional identities, and hackers-for-hire. Earlier research demonstrated that sophisticated threat actors frequently seek more than data.

For legal and fiduciary organizations, that distinction is critical. A threat actor who changes one professional contact field, captures one administrative session, obtains one mail credential, modifies one intake destination, or acquires access to one trusted application may be able to redirect an existing relationship without fabricating the institution itself. The firm remains real. The domain remains real. The professional may remain real. The portal may remain operational. The communication may travel through accepted infrastructure. What changes is the operator exercising the authority.

The DF-F.I.R.E. Team was organized to study precisely that type of tradecraft. Its forensic work is directed toward identifying when an otherwise legitimate digital environment has been repurposed to support an unauthorized professional persona, counterfeit authority signal, substituted relationship, manipulated routing state, or corrupted institutional record. These conditions are examined across the complete attack surface: endpoint activity, credentials, sessions, cloud control, DNS and MX infrastructure, mailboxes, websites, professional directories, e-filing and membership portals, vendor relationships, intake systems, document production, electronic service, docket associations, payment flows, publication systems, and subsequent institutional reliance.

The Team refers to these interconnected environments as *digital-empirical environments* because the evidentiary value resides not merely in isolated artifacts but in the measurable relationships among them. A professional profile modification acquires greater significance when it coincides with a credential event, a changed communication route, a disputed filing, an altered service population, or a consequential institutional action. Conversely, repeated copies of the same upstream assertion are not treated as independent evidence merely because they appear across several websites or records. Evidentiary weight is assigned through source dependency, chronology, technical mechanism, and independently preserved consequence.

This methodology is deliberately conjunctive. The DF-F.I.R.E. Team therefore treats identity and authority as operational cybersecurity controls. Incident containment is incomplete when the malicious code has been removed but the attacker-controlled professional profile remains online, the mailbox delegation remains active, the OAuth grant remains valid, the service list remains contaminated, the redirected intake form continues delivering information, or an institution continues relying upon an unauthorized instruction already incorporated into its records. Recovery requires restoration of both technical integrity and authority integrity.

Accordingly, the mission of ACIS COLAB and the DF-F.I.R.E. Team is not confined to describing how an intrusion occurred. It is to determine what the intrusion was used to

accomplish, reconstruct how the resulting state propagated through the surrounding environment, identify the control points that permitted that state to become trusted, and provide containment and restoration strategies capable of reaching the same institutional environment in which the adverse consequence occurred.

The October 2026 PHP emergency makes that work immediate. The legal sector now faces a materially expanded attack surface layered upon a threat class already documented through years of cyber-forensic research, government advisories, judicial records, independent expert studies, and operational case examples. DF-F.I.R.E.'s role within ACIS COLAB is to connect those technical capabilities to the professional and adjudicative systems they can affect, preserve the evidentiary path from source to consequence, and support rapid restoration of trustworthy identity, communications, intake, routing, and institutional decision-making before a compromised digital state becomes a durable legal one.

Report Lineage, Immediate Purpose, and Investigative Mandate

This edition was prepared because the October 2026 PHP emergency converted a known professional-identity and legal-routing threat into a substantially larger legal-sector emergency. PHP is a server-side software runtime used to assemble web pages, process forms, query databases and connect websites to mail, storage, identity, payment and administrative services. The emergency corrections issued on October 21, 2026 addressed vulnerabilities that permit attackers to move from a public web request into unintended server-side execution. AWS observed exploitation on October 17, 2026, before the public patch announcement. [FN 1] [FN 2]

The timing is decisive. The cAPTure investigation had already identified credential-backed professional personas, placeholder attorneys, counterfeit e-service, portal compromise, authority substitution and adjudicative-routing manipulation. CNF published the integrated cAPTure model on October 22, 2025. ORACLE, RAPS and CCDG continued the investigation through 2026. September 2026 threat assessments formalized authority-rail exploitation before the public disclosure of the PHP emergency. [FN 3] [FN 4] [FN 5] [FN 6] [FN 7]

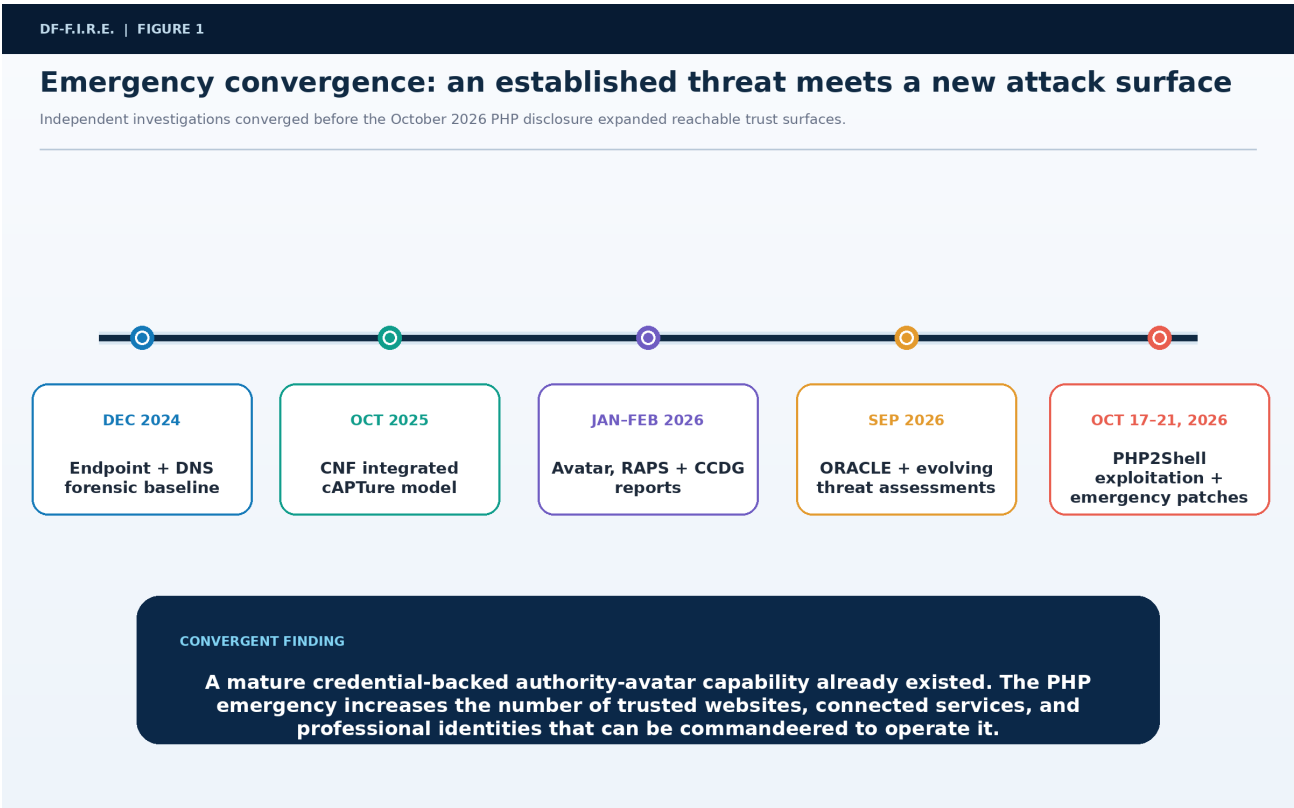


Figure 1. October 2026: the emergency meets an established threat record
Source: DF-F.I.R.E. synthesis of the December 2024–October 2026 report,

Special Acknowledgment of Public-Interest Reporting and Technical Research

A. Journalist Authors

The investigation benefited from sustained public-interest reporting that preserved dates, official statements, technical disclosures and institutional responses. The following journalists and technical authors who created an accessible public chronology that this report uses for source verification. [FN 8]

Journalist / author	Outlet	Professional profile
Raphael Satter	Reuters	Profile
John Sakellariadis	POLITICO	Profile
Matt Burgess	WIRED	Profile
Sergiu Gatlan	BleepingComputer	Profile
Swati Khandelwal	The Hacker News	Profile
Davey Winder	Forbes	Profile
Lily Hay Newman	WIRED	Profile
Kevin Collier	NBC News	Profile
Ionut Arghire	SecurityWeek	Profile
Eduard Kovacs	SecurityWeek	Profile
Lawrence Abrams	BleepingComputer	Profile
Josh Gerstein	POLITICO	Profile
Leo Marchandon	Reuters	Profile
Kanjyik Ghosh	Reuters	Profile
Rajveer Pardesi	Reuters	Profile
Waqas	HackRead	Profile
Greg Otto	CyberScoop	Profile
Lindsay Clark	The Register	Profile
Sarah Perez	TechCrunch	Profile
CJ Moses	AWS Security Blog	Profile
John Blackburn	WordPress.org	Profile

B. Technical Acknowledgements

Technical acknowledgments. The methodology also incorporates expert declarations and research from Microsoft Digital Crimes Unit investigators Christopher Coy, Jason Lyons and Kevin Garlow; Google Threat Analysis Group research led by Shane Huntley and associated teams; Sophos incident-response research including Joseph Levy; DXC expert materials including Mark Hughes; Citizen Lab's Dark Basin investigators; MITRE ATT&CK; NIST; CISA; the FBI; and the independent CNF, ORACLE, RAPS and CCDG research teams. Their work supplies the capability definitions, command-and-control comparators, valid-account models, identity-abuse patterns and disruption precedents used throughout this report. [FN 9]

Expert association / team	Contribution	Source
Microsoft Digital Crimes Unit	Christopher Coy; Jason Lyons; Kevin Garlow	Source / declaration
Google Threat Analysis Group	Shane Huntley and TAG investigators	Source / declaration
Sophos	Joseph Levy and incident-response researchers	Source / declaration
DXC Technology	Mark Hughes and referenced expert materials	Source / declaration
Citizen Lab	Dark Basin investigative team	Source / declaration
MITRE ATT&CK	Enterprise technique corpus	Source / declaration
NIST	Digital identity and incident-response guidance	Source / declaration
CISA	Operational advisories and defensive guidance	Source / declaration

Table of Content

Report Lineage, Immediate Purpose, and Investigative Mandate.....	2
Special Acknowledgment of Public-Interest Reporting and Technical Research	4
Summary	10
Part I — The October 2026 PHP Emergency	14
1. PHP in ordinary language.....	14
2. The October 17–21 emergency window.....	14
3. Why lawyers and courts face an outsized consequence	14
4. Patch completion and authority recovery are separate states	15
Part II — The Threat Record Before the PHP Emergency	16
5. Federal judicial systems were already confirmed cyber targets.....	16
6. The October 22, 2025 CNF foundation	16
7. ORACLE, RAPS and CCDG convergence	16
8. September 2026 threat assessments	17
Part III — Methodology of Authority-Avatar Detection	18
9. Begin with the consequential act	18
10. Resolve identity, credential, role and event separately.....	18
11. Determine first visibility and first divergence.....	19
12. Correlate without multiplying dependent sources.....	20
13. Confidence through convergence.....	20
14. Peer-reviewed research on synthetic and co-opted personas	21
Part IV — How Counterfeit Authority Enters Legal Work	24
15. Professional avatars, placeholders and delegated authority	24
16. Credentials, sessions, tokens and mailbox permissions.....	25
17. Authentication is transport authority, not human authority.....	25
18. Documents, metadata and mutable destinations	26
19. Hackers-for-hire as a commercial operating model	27
20. Recognized technique mappings	30
Part V — Southern District of Florida Placeholder-Avatar Study.....	32
21. Population and source architecture.....	32
22. What happened after the placeholder entered	32
23. How the avatars were identified	32
Part VI — Fifteen Independent Authority-Manipulation Case Studies	34
24. Piney Point Homes — court-registry funds released through compromised counsel communications.....	34
25. Thomas v. Corbyn Restaurant Development — counsel impersonation redirects settlement	34
26. Erie Insurance v. WAWGD — more than fifty emails sustain the impostor	34
27. Oregon DOJ settlement diversion — both sides of the trusted exchange controlled.....	35
28. Lisa Findley and Graceland — a fabricated lender becomes a court claim	35
29. Anton Iagounov — fictitious agents seek real judicial signatures.....	35
30. Miranda Devlin — valid professional credentials maintained for unauthorized practice	36

31. Leaford George Cameron — a fabricated multi-office law firm.....	36
32. Matthew Weidner — a real lawyer’s name and Bar number inserted into a pleading.....	36
33. Angel Ariel Bermudez — simulated hearing, real regulatory consequence.....	36
34. Edmond Abordo — forged chief-judge authority in a property scheme	37
35. Andrew Wynne — fabricated orders across approximately thirty client matters.....	37
36. Matthew Elstein — sham records and a fabricated settlement.....	37
37. FBI fictitious-law-firm recovery schemes	37
38. North Korean remote-worker operations — accepted enterprise identities operated by substitutes.....	38
Part VII — Beyond the Attorney: Firms, Vendors, Staff, Clerks and Judges.....	39
39. The intra-firm avatar at a global firm.....	39
40. Vendors and legal supply chains	40
41. Paralegals, assistants and staff as authority carriers	40
42. Clerks, registries, law clerks and chambers.....	41
Part VIII — Bounded Anonymized Florida Field Reconstruction	43
43. J.D.W. — response population, acknowledgment and nonresponse conversion.....	43
44. R.B. and Staff Investigator J.B. — source denial and message-version conflict	44
45. P.S. — private-counsel routing through an institutional address.....	46
46. R.W. — committee authority and reassignment.....	48
47. Staff Investigator J.B. — institutional communication and source compression.....	49
48. E-court notices, service lists and accepted state	50
Part IX — Detection, Containment and Resilient Access to Judicial Power.....	54
49. Detection begins with authority differences.....	54
50. Containment must preserve legal continuity.....	54
51. Professional-identity recovery	54
52. Response priorities for the PHP emergency.....	55
Part X — Integrated Findings and Final Determinations	57
53. Professional identity is an operational control surface.....	57
54. Trusted infrastructure can carry adversarial authority.....	57
55. Authority-avatar manipulation is a distinctive cAPTure capability.....	57
56. High-confidence conclusions.....	58
57. Final determination.....	59
Endnotes and Sources.....	60

Summary

We find with very high confidence that the October 2026 PHP emergency enlarged a pre-existing authority-avatar attack surface across the legal sector. The vulnerable runtime sits inside law-firm websites, professional directories, client-intake forms, publication systems, vendor portals and court-adjacent services. Server-side execution can expose application secrets, change professional contact instructions, alter document destinations, reach connected mail or storage accounts and create durable administrative access. [FN 1] [FN 2]

The emergency arrived after an established investigative record. CNF's October 22, 2025 report identified a templated cAPtUre operation targeting attorneys, law firms, electronic filing systems, communications and judicial infrastructure. ORACLE, RAPS and CCDG expanded the record through identity rails, portal control, cryptographically aligned counterfeit communication and procedural-state manipulation. September 2026 assessments then integrated authority avatars into the evolving cAPtUre model. [FN 4] [FN 3] [FN 6] [FN 7]

The legal sector now faces a convergent emergency. Commercial hackers-for-hire provide access, persistence, collection and infrastructure at a price point available to private clients and intermediaries. Their tradecraft uses techniques associated with nation-state operations without requiring nation-state participation. Genuine professional data, accepted accounts, synthetic media, trusted websites and institutional workflows reduce the amount of fabrication needed for each operation. The resulting authority signal can enter an active matter as counsel, staff, vendor, clerk, expert, reporter, client, law-firm partner or judicial actor.

The adjudicative environment is especially exposed because filing, service, docketing, sealed-document handling, fee payment, court-registry disbursement and chambers communication now depend on electronic identity and routing. A compromised professional identity can file a notice of appearance, receive privileged material, alter the service population, redirect a payment, supply a false deadline or place a fabricated instrument before a court. Once the system accepts the input, later participants inherit an official-looking state.

The independent comparator record establishes fifteen open

rational pathways. They include stolen attorney identities maintained through valid licenses; false firms and fictitious staff; fabricated lenders and foreclosure authority; forged judicial orders; impersonated counsel directing settlements; compromise of both sides of an attorney-client exchange; diversion of court-registry funds; simulated hearings; counterfeit federal-agent requests for judicial signatures; AI-generated pleadings using a real lawyer's credentials; and accepted enterprise identities operated by substitute workers.

The United States District Court for the Southern District of Florida study supplies the population-level legal-workflow signal. CNF enumerated 56 cases in Table 1, studied more than 250 litigation matters across the broader universe and examined approximately 32 attorneys. The report recorded a reported mean placeholder tenure of 57 days; 93 percent of the studied placeholder matters terminating or resolving within that period; 81 percent showing zero, appearance-only or non-substantive activity; 19 filings omitting professional identifiers; 78 percent of a suspect-document subset using four unusual PDF tools; caption errors in 62 percent of the suspect set compared with 37 percent of a comparator set; and stale or incorrect contact data in 21 percent. [FN 10]

The bounded Florida field case supplies direct source objects showing how the mechanism operates inside one institutional sequence: a private law firm redirected communications to P.S. at an institutional Bar address; Staff Investigator J.B. wrote that an attributed counsel email did not originate from the office; the same investigator later wrote that an email included in the response "has been changed"; the dispute entered pleadings and affidavits; and the resulting authority representations were used within adjudicative proceedings. The field case appears later as a corroborating operational reconstruction, not as the report's principal population.

Our final determination is stated with very high confidence. PHP exploitation, valid-account abuse, professional-persona operations, portal compromise and counterfeit authority are convergent components of a scalable cAPTure capability. Their joint purpose is to convert access into accepted authority and accepted authority into a consequential legal, financial, regulatory or reputational state. The legal sector must treat identity, website runtime, communication, intake, routing and record integrity as one incident environment.

What PHP controls inside a legal-sector website

The visible webpage is only the outer surface. Server-side code can connect identity, mail, storage, data, and administrative authority.

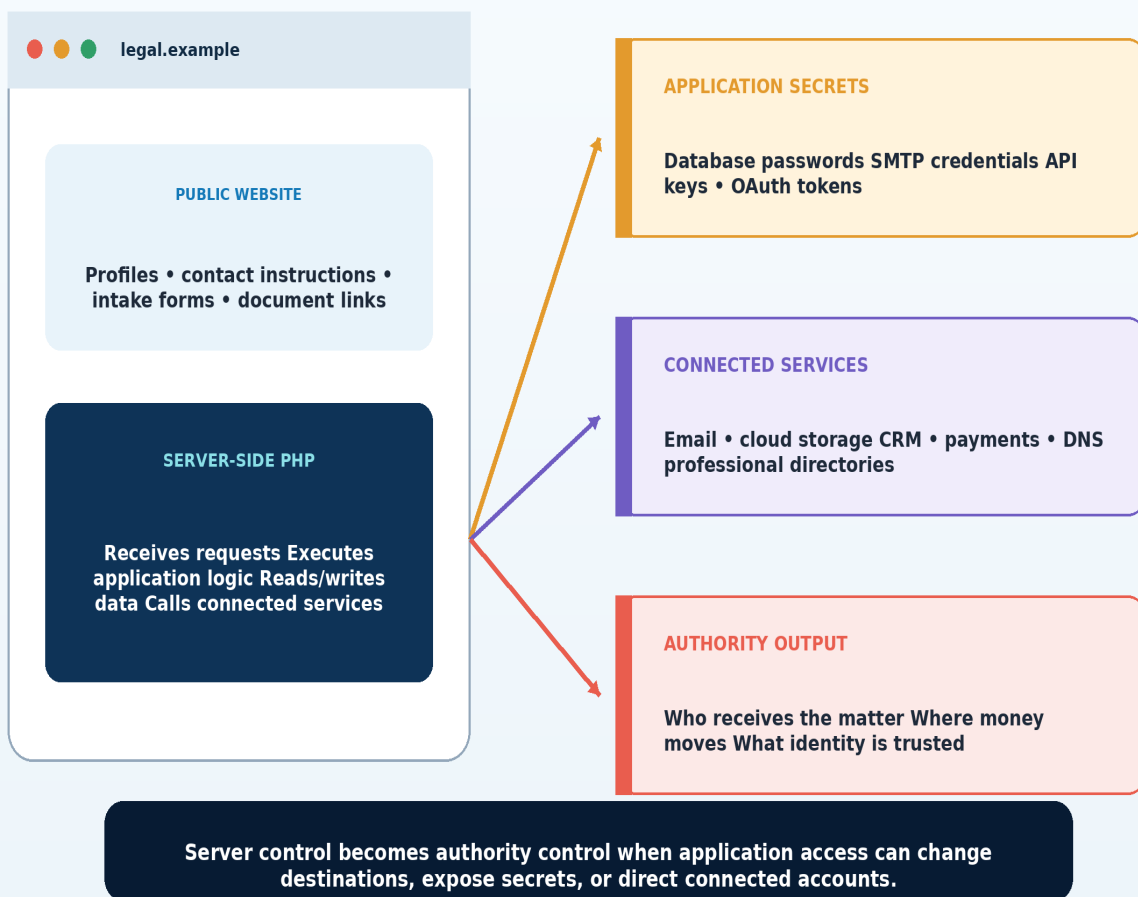


Figure 2. What PHP controls inside a legal-sector website

Source: PHP architecture and legal-sector trust relationships synthesized by DF-F.I.R.E.

The legal authority stack

A professional identity becomes consequential only after multiple trust rails align — or are co-opted.

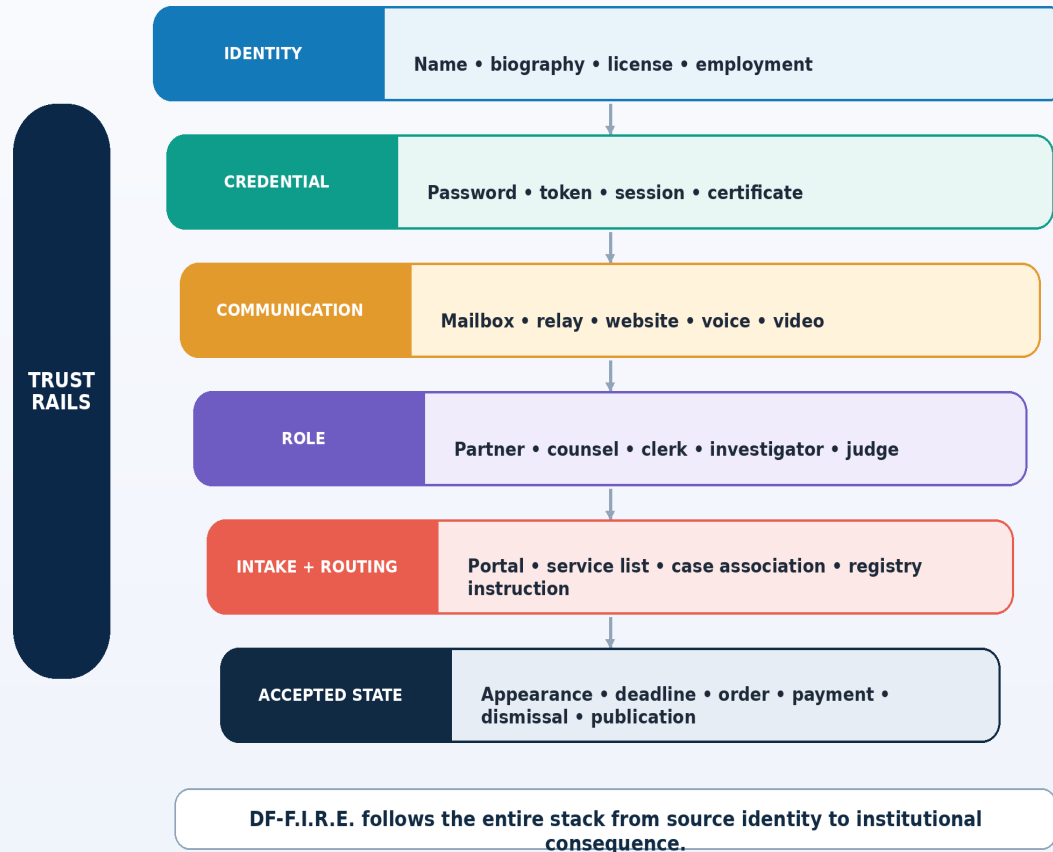


Figure 3. The legal authority stack

Source: ORACLE authority-rail model, CNF cAPtUre model, RAPS portal model and CCDG communications model.

Part I — The October 2026 PHP Emergency

1. PHP in ordinary language

PHP is a server-side runtime. A visitor requests a page; the web server passes that request to PHP; PHP executes the application's instructions; and the application reads data, builds the response, sends mail, writes a file or calls another service. The browser receives the finished page. The sensitive work occurs on the server, where the application can reach resources the visitor cannot see.

Legal-sector organizations use PHP directly and indirectly. WordPress and many content-management systems use PHP. Law-firm sites use it for attorney biographies, intake forms, document libraries, recruiting pages and news publications. Bar associations and legal vendors use it for directories, event registration, learning systems, membership pages and payment flows. Court-adjacent providers use web applications to receive information, authenticate users, link documents and deliver notifications.

A successful server-side exploit can therefore reach beyond the visible page. The application may hold database passwords, SMTP credentials, cloud-storage keys, OAuth tokens, payment-provider secrets, administrative cookies and API credentials. Those objects connect the website to the organization's authority-bearing systems. [FN 1] [FN 2]

2. The October 17–21 emergency window

AWS recorded an attempted PHP2Shell exploit on October 17, 2026. The PHP project issued emergency corrections on October 21. The sequence establishes active exploitation before public disclosure and before many operators knew which systems required immediate correction. [FN 2] [FN 1]

The corrected branches identified by PHP were 8.2.35, 8.3.36, 8.4.27 and 8.5.12. The emergency implicated both current operations and historical authority states: profiles already altered, contact destinations already changed, credentials already exposed, OAuth relationships already granted and messages already accepted remain part of the incident after the runtime is patched. [FN 1]

3. Why lawyers and courts face an outsized consequence

A legal website is a verification layer. Clients, courts, opposing counsel, reporters, vendors and banks use it to confirm where a lawyer works, which email address belongs to the lawyer, which office handles a matter and how to submit information. A one-line contact substitution can redirect an entire relationship while preserving the firm's genuine name, design, domain and professional history.

A legal website is also an intake layer. A compromised form can collect privileged facts, identify active disputes, obtain exhibits, map deadlines and send the submission to an operator-controlled mailbox. The operator receives the information needed to create a tailored professional persona before the target knows the channel has changed.

A legal website is a credential bridge. Plugins, mail services, cloud storage, analytics, customer-relationship systems and identity providers create connected trust. Access to the application's secrets can move the operation from website control to mailbox control, session persistence, document access and administrative authority.



Figure 4. Lifecycle of a co-opted professional persona

Source: MITRE account-establishment and valid-account techniques; CNF and ORACLE persona models.

4. Patch completion and authority recovery are separate states

Technical patching stops the vulnerable code path. Authority recovery reconstructs every downstream relationship the exploited application could reach. The response therefore includes source-code and runtime correction, secret rotation, session revocation, OAuth review, mailbox-permission review, account recovery, DNS/MX verification, content comparison, directory correction, document-link validation and notification to institutions that accepted instructions during the exposure window.

Part II — The Threat Record Before the PHP Emergency

5. Federal judicial systems were already confirmed cyber targets

On August 7, 2025, the Administrative Office of the U.S. Courts publicly acknowledged recent escalated cyberattacks of a sophisticated and persistent nature against the federal case-management system. The Judiciary announced strengthened protections for sensitive documents. Reuters and POLITICO reported exposure risks affecting CM/ECF, PACER and sealed material. [FN 11] [FN 12] [FN 13]

The modernization timeline confirms the depth of the legacy transition. The Judiciary stated in June 2026 that all new district-court cases were scheduled to move to the modernized platform by the end of 2027, with legacy migration continuing later and full replacement no sooner than 2030. The operational exposure therefore spans an extended period in which modern and legacy components coexist. [FN 14]

RAPS independently analyzed legacy .dcn naming, CM/ECF gateway hosts, email-authentication gaps and off-PACER artifacts. CCDG examined state e-filing, Bar portals, trusted relays and communications that passed ordinary cryptographic checks while carrying operationally false content. Their reports establish that the same legal process can contain technically authentic infrastructure and unauthorized authority at the same time. [FN 6] [FN 7]

6. The October 22, 2025 CNF foundation

CNF defined cAPTure-to-Kill as a templated advanced persistent threat directed at the legal ecosystem. The model connects endpoint compromise, credentials, DNS/MX control, portal access, e-service, court intake, professional personas, publication and downstream institutional consequences. Its objective is not limited to theft. It is the suppression, redirection, corruption or premature termination of a claim, remedy, evidence path or professional capacity.

CNF's avatar methodology began with anomalies in active cases and then tested them against credential exposure, document production, email infrastructure, domain history, portal data and institutional chronology. The method identified the professional identity as an access node through which an operator could occupy the role of attorney of record, communicate with the court and opposing counsel, and operate inside an active proceeding. [FN 10]

7. ORACLE, RAPS and CCDG convergence

ORACLE separated the authority environment into identity, credential, communications, role, procedural-state, adjudicative-routing, publication and temporal rails. The model

explains how a genuine name and valid credential become operational when an operator controls the channel and claims a role accepted by another institution. [FN 3]

RAPS focused on restricted-access portals and the procedural consequences of compromised gatekeeping. Its analysis treats missing filings, changed service lists, assignment irregularities, payment disruption and access failure as direct manifestations of portal control. [FN 6]

CCDG focused on cryptographic counterfeit: an email can pass SPF, DKIM and DMARC because it traveled through an authorized tenant or relay, while the human authority, case identifier, recipient population or procedural instruction is false. [FN 7]

8. September 2026 threat assessments

The September 2026 cAPTure threat assessment integrated current cloud, portal, identity, session, mailbox and professional-persona mechanisms. The Civil Cyber-Infrastructure Disruption Litigation report reconstructed thirty-five cyber-disruption cases and measured whether legal remedies remained operational after adversaries adapted. ORACLE's September report formalized authority-rail exploitation before the PHP emergency was publicly disclosed. [FN 4] [FN 5] [FN 3]

Part III — Methodology of Authority-Avatar Detection

9. Begin with the consequential act

The methodology is anchored in MITRE impersonation, valid-account and account-establishment technique definitions; NIST identity-proofing and integrated-forensic guidance; and CISA logging practices. These sources supply standardized controls for separating identity, accepted credentials, event authorization and preserved activity. [FN 15] [FN 16] [FN 17] [FN 18] [FN 19] [FN 20]

The foundational method begins with a consequential discrepancy in a filing, message, service entry, representation of counsel or response sequence, then expands outward to the professional identity and systems through which that act was presented. [FN 21]

The primary object is preserved before its interpretation is expanded. A message is examined with its attachment and displayed recipients; a filing with its signature and service certificate; a webpage with its address, collection time and visible fields. This keeps the observed content separate from conclusions later added by a witness, researcher or publisher. [FN 22]

A useful starting question is exact: what differs between the two objects that purport to represent the same event? In the changed-email sequence, that means comparing the words attributed to the sender, the version attached as an original, and the language later presented to the court. The resulting finding concerns a specific communication, not a general impression that an account “looks fake.” [FN 23]

The same method applies to case chronology. Each grievance is identified by its base number, the request associated with it, the deadline in the correspondence and the action later said to follow nonresponse. Aggregating the files comes after those separate timelines, so an earlier obligation is not silently assigned to a later-created matter. [FN 24]

10. Resolve identity, credential, role and event separately

Identity resolution asks which person a record purports to describe. Credential validation asks whether the asserted identifier belongs to that record. Event authorization asks whether the relevant person or institution approved the particular act. These are distinct comparisons, and a successful match at one level does not substitute for the remaining relationships. [FN 25]

The named-subject review records the full professional name, aliases used professionally, Bar number, admission date and institutional role shown in each source. A shortened name or reordered first and middle names is retained as a matching field

rather than treated as a separate person automatically. This is particularly important for John D.W., Derek John D.W. and John D.W.. [FN 26]

A dated filing provides a historical reference to the role displayed on its face. An affidavit supplies the employment statement its author swore. A current biography supplies a current retrospective account. The methodology records those distinctions so that a historical document date, a claimed employment start and a webpage acquisition date do not become one invented “first appearance” date. [FN 27]

The October 2025 method combined professional-information exposure research, side-by-side document examination and internet-infrastructure comparison, using each layer to test the same suspected use of an attorney identity rather than treating the layers as unrelated incidents. [FN 28]

11. Determine first visibility and first divergence

Four dates are recorded separately: when the event occurred, when a source says it was published, when an archive captured it, and when the investigator acquired it. The first located record is a search result within the examined source set. A preserved archival capture establishes that the archived content was retrievable at that capture time. [FN 29]

First visibility and first divergent use answer different questions. An older court opinion can establish that a professional name appeared historically, while a later contested message raises a separate question about how that name was used. We find this distinction essential for a co-opted-persona investigation because the attack can begin long after the genuine professional's career began. [FN 30]

The John D.W. screenshot is recorded as a preserved search-result display with a filename bearing December 9, 2024. The visible employer, city, education and admission fields are transcribed exactly. The filename and the content are separate observations: the image preserves what was displayed, while the webpage's original field-publication date belongs to its publication history. [FN 31]

Historical comparison follows the exact URL and its variants, including redirected paths and separate profile identifiers. Each acquired version is associated with its capture time and preserved content. A change is then described by the field that changed—employer, title, address, contact destination, role or document association—rather than by a broad claim that an entire identity appeared or disappeared. [FN 32]

A professional's hiring announcement, award announcement and employer's corporate-adviser notice are different kinds of evidence. They establish different relationships at different times. The method preserves that granularity when examining a journalist's

byline, an employer's communications adviser and a disputed interaction attributed to the journalist. [FN 33]

12. Correlate without multiplying dependent sources

Cumulative analysis connects the events through their actual relationships: the message attached to a filing, the filing supporting a request, the request preceding an order, and the order reproduced in a professional record. [FN 34]

Three profiles repeating one biography supply three publications, but may supply only one underlying claim. A complaint, affidavit and news report can likewise repeat the same statement. We preserve the publication chain and identify the originating observation before assigning additional evidentiary weight to repetition. [FN 35]

The analytical sequence is event, mechanism, operational purpose and attribution. An event can be established from a preserved document; a mechanism from an identified technical action; an operational purpose from the action's function in the sequence. Actor attribution requires a connection to the person or resource exercising control, so the report's confidence is attached to the specific finding rather than the narrative as a whole. [FN 36]

Original files and later readable renderings serve different functions. The original preserves the available bytes and metadata; a rendering makes the document accessible to a lay reader. A screenshot is valuable for the displayed state, while the source file carries additional structural information. The analysis labels each object by what it actually preserves. [FN 37]

13. Confidence through convergence

DF-F.I.R.E. assigns very high confidence to directly preserved documentary facts, official adjudications and independently reproducible technical states. High confidence applies where a coherent source-to-consequence sequence is supported across separate technical, documentary, chronological and institutional domains. The confidence statement attaches to the precise proposition being made.

Convergence is evaluated conjunctively. A changed professional profile, credential exposure, accepted account, altered message, portal event and resulting order are not treated as independent probability multipliers when they depend on one upstream act. Their strength comes from the operational relationship among them: one event supplies access, another supplies authority, another records institutional reliance, and the final object preserves the consequence.

The professional echo chamber

A single planted claim can appear independent when platforms copy, index, rank, and republish it.

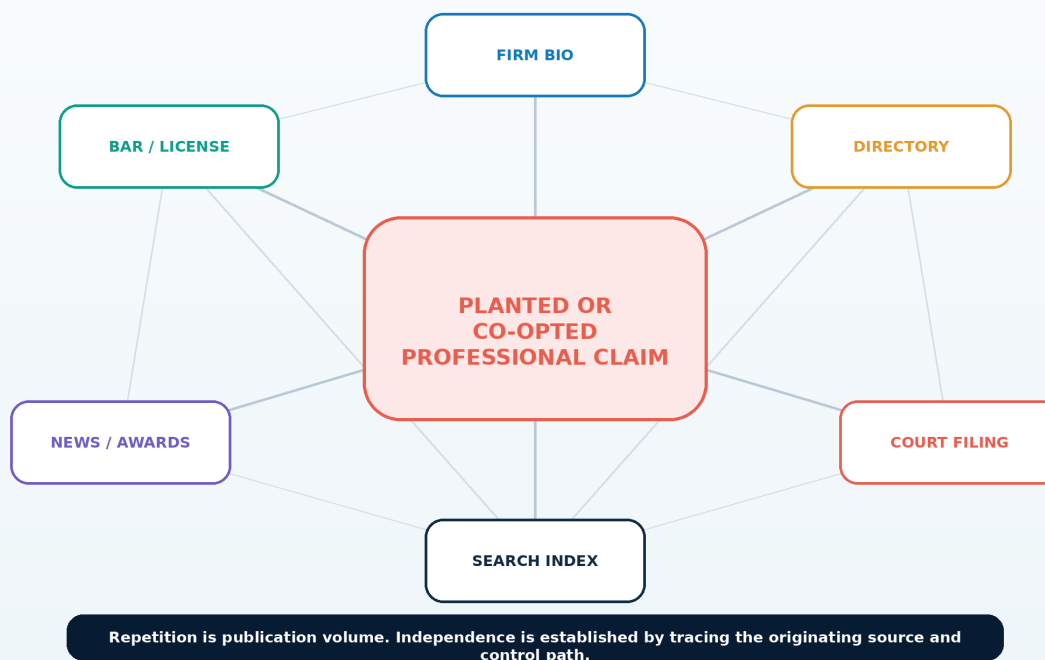


Figure 5. The professional echo chamber

Source: DF-F.I.R.E. dependency-analysis model; NIST preservation and source-tracing principles.

14. Peer-reviewed research on synthetic and co-opted personas

The peer-reviewed foundation includes research on deepfake-driven social engineering, AI-powered social engineering, behavioral identity profiling and media forensics. The studies independently identify authoritative-role simulation, realism, personalization, automation, cross-system behavior and source authentication as central analytical dimensions. [FN 38] [FN 39] [FN 40] [FN 41]

Synthetic media adds a persuasive representation of a person to an existing authority claim. A voice or video can make the request appear to come directly from a known professional rather than from an unfamiliar text account. The underlying security problem remains authorization of the requested act, even when the media looks and sounds convincing. [FN 42]

The 2025 corporate social-engineering study examines how synthetic media can exploit trust in authoritative roles and familiar communication channels. It combines technical discussion with interviews of security professionals and proposes the PREDICT framework. Its contribution to this report is the integration of policy, preparation, detection and response around the human decision being targeted. [FN 43]

The 2026 AI-powered social-engineering study organizes the threat around realism, personalization and automation. Realism improves the apparent presentation,

personalization adapts the request to the target, and automation increases the number or speed of interactions. Together these capabilities explain how an operator can maintain a coherent professional persona across repeated communications. [FN 44]

The addition of synthetic media can increase the apparent independence of several participants in a conversation. A target may encounter a purported colleague, supervisor and adviser whose presentations reinforce the same instruction. We assess this as an important expansion of coordinated-persona tradecraft because it can reproduce the social setting in which consequential decisions are ordinarily made. [FN 45]

Passive media analysis examines the content itself for traces of manipulation. Active authentication uses information attached during creation or handling, such as a digital signature or watermark. Attribution examines the origin of the content or the tool used to produce it. These are separate functions, and the report introduces them before discussing a technical result. [FN 46]

A screenshot or heavily compressed video may preserve fewer useful traces than the original recording. The visible realism of the image and the strength of an authentication result are therefore different questions. We find that source history and the circumstances of acquisition remain important even when an automated detector is available. [FN 47]

A video that resembles a professional can establish what the viewer was shown. An identity check establishes the evidence used to connect that presentation to a person. The authority check establishes whether that person was entitled to direct the transaction. Keeping these steps distinct prevents a compelling image from substituting for the role and authorization evidence. [FN 48]

The DS-IID study constructs behavioral profiles from event data such as logins, email activity, file use and web activity. It then tests a model designed to distinguish types of behavior, including generated abnormal profiles. The relevance is methodological: identity-related activity can be compared across several systems rather than judged from a professional headshot or biography alone. [FN 49]

The paper reports 97 percent accuracy in its stated insider-threat experiment and greater than 99 percent for specified generated-data tests. Those numbers describe the reported benchmark tasks. They are not probabilities that a particular lawyer or investigator in this report is an impostor; the case findings remain tied to their own source objects and event sequences. [FN 50]

The practical analytical gain is the ability to connect activity associated with one identity across different event classes. A role change, unusual message, document modification and consequential instruction can be studied in sequence. We find that this approach is

more informative than measuring whether a profile contains many posts, endorsements or connections. [FN 51]

The research supports a layered examination of the presented person, the account used, the instruction given and the institutional action requested. A technical detector addresses one part of that examination, while professional-role verification and document comparison address other parts. The combined method fits legal work because the consequence depends on accepted authority as much as on access to a device. [FN 52]

The supplied investigative-industry article likewise treats synthetic identities as a cross-channel problem involving records, communications and relationships. Its operational themes are consistent with the broader public guidance on impersonation. We use those themes to organize the evidence, while relying on the underlying government, research and case sources for the specific findings in this report. [FN 53]

The peer-reviewed record converges on five capabilities: realism, personalization, automation, authoritative-role simulation and cross-system behavioral continuity. Those capabilities explain how a co-opted professional identity can operate through text, email, profiles, filings, voice, video and enterprise accounts without requiring a wholly invented human being.

Part IV — How Counterfeit Authority Enters Legal Work

15. Professional avatars, placeholders and delegated authority

An avatar, as used in this report, is a representation through which an operator acts under another identity or claimed professional capacity. The representation can be wholly invented, assembled from several real identities, or built around one genuine professional whose credentials or communications have been appropriated. This definition directs attention to the relationship between the represented person and the act performed under that person's name. [FN 54]

A synthetic persona is an assembled identity presented as a coherent person. An appropriated persona uses a real person's identifiers. A blended persona combines genuine employment or licensing details with an operator-controlled address, image, account or employment claim. Those categories explain why a search result can contain accurate biographical facts and still direct a recipient to the wrong operator. [FN 55]

The professional whose name is used and the actor using it occupy different evidentiary positions. In an identity-theft operation, the genuine lawyer can become a second victim when clients complain, regulators receive reports or search results associate the lawyer with conduct performed by the impersonator. We therefore examine the identity-bearing transaction instead of treating every person named in a disputed document as a participant in wrongdoing. [FN 56]

A convincing persona is usually supported by more than one object: an account, a biography, an email address, a conversation history and a reason to act. Coordinated personas can reinforce one another by appearing to be independent correspondents who already know the supposed professional. The resulting conversation supplies social corroboration even when the visible participants share one operational source. [FN 57]

A deepfake is artificially generated or materially manipulated audio, imagery or video that presents a person as saying or doing something. A professional avatar is broader: it can operate entirely through text, credentials and institutional forms. Deepfake media can strengthen the presentation of an avatar, but the operative deception may be the claimed authority rather than the face or voice. [FN 58]

The October 22, 2025 integrated investigation used “placeholder counsel” to describe an attorney identity occupying a functional place in litigation while the challenged activity was performed through that identity rather than verified direct professional engagement. [FN 59]

The operational significance of a placeholder is access to a trusted role: opposing counsel, clerks, clients and service systems respond to the attorney of record. Once the representation is accepted, the name becomes associated with communications,

documents and deadlines. A genuine license number can therefore supply credibility to an act performed by someone other than its holder. [FN 60]

A notice of appearance or substitution records a claimed representational relationship. The research separates that relationship from the lawyer's biographical existence, the identity of the account submitting the notice, and the authority of the person communicating afterward. In the Florida example, the substitution identified Randall B. as counsel for the Bar, which is the role used throughout this edition. [FN 61]

We use the term authority pathway for the connected steps through which a represented identity becomes an accepted institutional act: a person or account asserts a role, a recipient accepts the assertion, a document or instruction enters a process, and a later actor relies on the resulting state. [FN 62]

The strongest impersonation operation does not need to fabricate every downstream object. An authentic clerk can receive a false submission, a genuine court can be asked to sign a fabricated warrant, and a real financial transaction can follow an unauthorized instruction. We find that the conversion of counterfeit input into genuine institutional action is the central risk examined here. [FN 63]

16. Credentials, sessions, tokens and mailbox permissions

A credential is information a system accepts to grant access, such as a password, key or certificate. A session allows continued access after sign-in, and a token is a digital value representing an accepted identity or permission. Possession of those items can let an operator act through a real account without changing the visible professional name. [FN 64]

A mailbox can have delegated access, application permissions and folder-level rights in addition to its owner's password. Those relationships determine who or what can read, change or send information. A password reset changes one credential; the operational control described by a separate token or permission must be understood as a separate part of the account's authority. [FN 65]

An institution can issue genuine access to an incorrectly identified applicant. In that sequence the compromised relationship begins at enrollment rather than at a later stolen-password event. The account, laptop and internal profile can all be institutionally created while the person operating them is different from the person the institution believed it had engaged. [FN 66]

17. Authentication is transport authority, not human authority

SPF is a domain policy that tells a receiving mail system which sending servers are authorized for a specified email identity. Its result concerns the sending path checked

by the receiver. The displayed person's name in the mail application is a different field and is evaluated separately from that server-authorization result. [FN 67]

DKIM attaches a domain-linked digital signature to selected parts of a message. A valid check means the signed material matches the signature under the specified signing rules. It connects the checked content to a signing domain, while the human author, permission to communicate and meaning of the instruction remain distinct facts about the transaction. [FN 68]

DMARC evaluates whether the visible sender domain aligns with an authenticated SPF or DKIM identity under the domain's policy. This helps recipients handle unauthorized use of a domain name. The result is an authentication relationship among domains and message fields, not a professional-role determination by the receiving mail system. [FN 69]

A message sent from an account under unauthorized control can satisfy the provider's normal delivery and authentication rules. We find with high confidence that valid transport and valid human authorization are separate security properties. This is why a message-version dispute must be read alongside the role, content, timing and institutional use of the message. [FN 70]

18. Documents, metadata and mutable destinations

Email headers record technical fields used in handling and routing a message. A display name, signature block or quoted conversation is content that can be reproduced or edited. The useful comparison follows the message identifiers, routing fields, attachment identities and the exact words being attributed, instead of assigning authorship from typography alone. [FN 71]

In the supplied Bar exhibits, the March 14 message contains a public-records footer and identifies an attached message file. Those visible features are retained in the description of that source copy. Comparing them with another rendering is a document-version exercise; the observed differences should be named precisely rather than converted into a general assertion about every message in the exchange. [FN 72]

PDF metadata can identify software, a stored author string or the time a file was created or modified. Such fields can originate from a template, workstation profile or conversion process. Their strongest value here is comparative: they help distinguish document versions and production paths when correlated with the actual content and the surrounding communication sequence. [FN 73]

A repeated paragraph or shared template reveals text reuse. A change to a recipient, deadline, asserted capacity or requested action changes the document's operational

meaning. We give the latter changes greater analytical weight because they identify the point at which a recipient's decision can be redirected. [FN 74]

A remotely loaded image can create a network request when an email or page is displayed. A redirect can send a browser to another address. Executing unauthorized code through a vulnerability is a separate mechanism with its own triggering conditions. The report explains which of these actions is documented before discussing its consequences. [FN 75]

In the 2026 OWA campaign, Proofpoint documented malicious code running in the webmail reading environment and using mailbox functions to alter stored content and permissions. That is a concrete example of a message becoming an access mechanism. Its relevance to the earlier field record is explanatory: it establishes a current capability class, while the earlier documents retain their own dates and observed features. [FN 76]

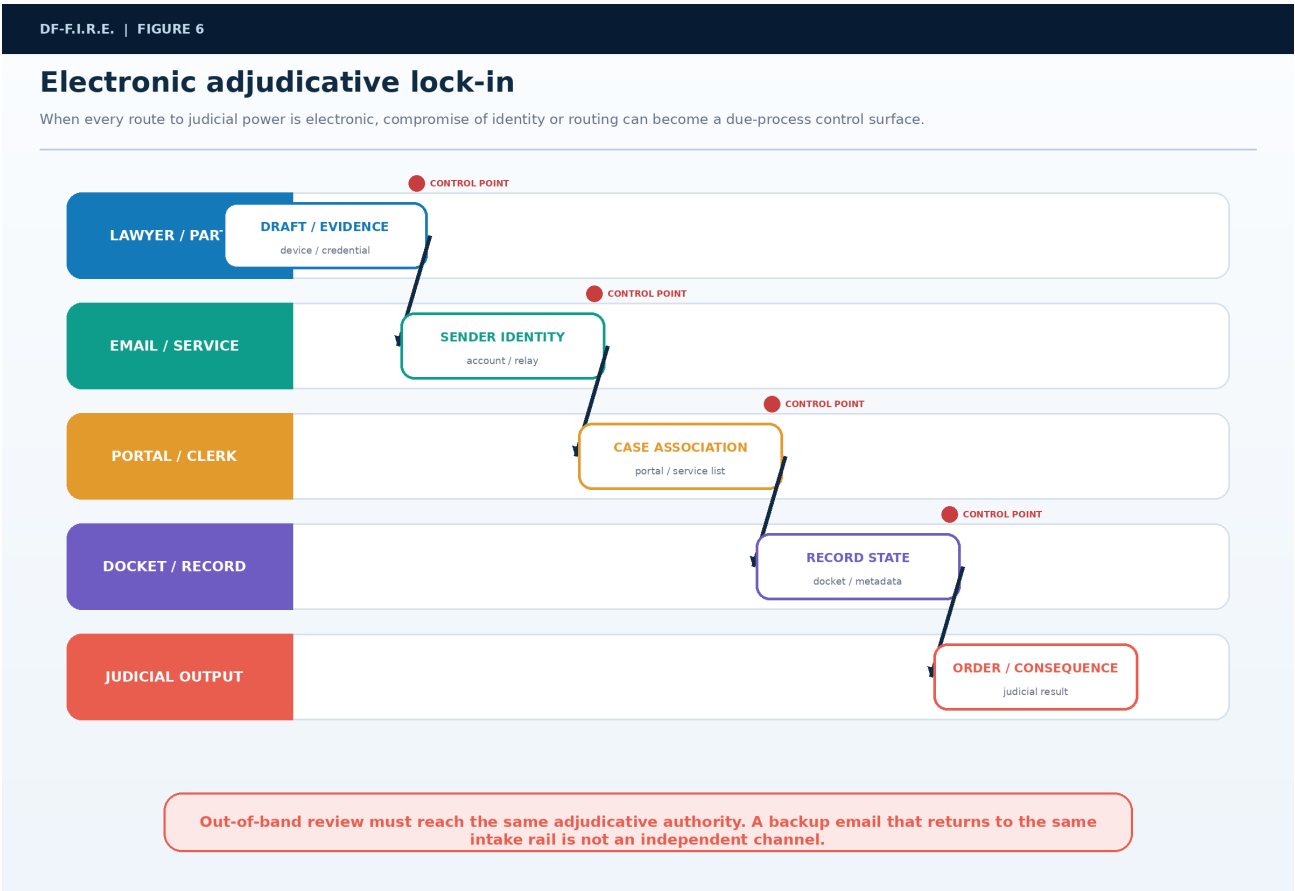


Figure 6. Electronic adjudicative lock-in
Source: CNF, RAPS, CCDG and federal Judiciary system architecture.

19. Hackers-for-hire as a commercial operating model

The commercial operating model is independently documented through Google Threat Analysis Group, Citizen Lab, Microsoft Digital Crimes Unit and Proofpoint research. Together, these sources establish purchasable targeting, persistent access, coordinated

personas, modular command-and-control and court-authorized disruption of criminal infrastructure. [FN 77] [FN 78] [FN 79] [FN 80]

The Azari prosecution supplies a concrete commercial example: a paid intermediary arranged hacking services for clients, and the resulting federal sentencing record describes the spearphishing operation and its financial structure. The case establishes that targeted intrusion can be purchased through a service chain rather than performed directly by the eventual beneficiary. That structure is central to our assessment of commercially motivated persona tradecraft. [FN 81]

Google's hack-for-hire research describes operators serving clients with targeted account compromise and information collection. This supports treating the contractor's technical access and the customer's objective as different layers of an operation. A target may encounter the phishing message or compromised account without seeing the intermediary who requested the task. [FN 82]

Citizen Lab's Dark Basin investigation provides an independently developed account of a large targeting operation affecting organizations and individuals across several contexts. Its research demonstrates the value of linking infrastructure, targeting patterns and victim-facing messages. We draw from that method when evaluating a professional-persona operation whose visible acts are distributed among several platforms. [FN 83]

We assess with high confidence that the commercial service chain is a practical operating model for cyber-enabled interference in disputes. The intermediary can translate an end client's desired outcome into tasks involving access, collection, contact or publication. A professional avatar provides a way to carry those tasks into relationships that would reject an openly hostile or unidentified actor. [FN 84]

The September 2026 Reuters article records a request by U.S. lawmakers to restrict three firms described as operating in the hack-for-hire market. The reported action was a request for designation, not a completed designation. Its value here is the documented institutional concern about targeted espionage affecting lawyers and the people they represent. [FN 85]

A professional persona supplies an accepted reason to ask questions, request documents or introduce a new communication channel. The operator can tailor the role to the stage of the dispute: an apparent lawyer for legal documents, a reporter for background information, or an investigator for purported verification. We find that the persona's function is to make the requested act appear ordinary in the target's professional environment. [FN 86]

Pre-existing accounts and stolen biographical data reduce the amount of credibility an operator must manufacture. The account may already have age, contacts and professional associations. A substitute person or synthetic presentation can then carry

the identity through a particular encounter, allowing the operation to combine real history with false current control. [FN 87]

Several personas can divide the work of one interaction. One introduces the matter, another verifies the supposed relationship and a third supplies the consequential instruction. We find that this arrangement makes source-dependency analysis especially important, because the number of voices in an exchange is not necessarily the number of independent sources. [FN 88]

A co-opted account can be more effective than a new alias because it inherits an existing relationship. The recipient recognizes the address, the conversation and the expected subject matter. The operational change can be small—a different payment destination, a canceled meeting or a new contact instruction—while its consequence is substantial. [FN 89]

Microsoft investigator Jason Lyons described an enterprise manufacturing accounts under fictitious users and selling them to cybercriminals in a declaration supporting a December 2023 federal action. He explained that automated registration defeated challenges designed to distinguish human applicants from software. The declaration also reports controlled purchases yielding approximately 16,500 accounts, followed by analysis of registration and sign-in addresses. We find that this evidence identifies a practical supply layer for persona operations: an operator can acquire functioning accounts from a separate provider instead of constructing every credential independently. [FN 90]

Figure 12. Commercial service chain and professional authority. Source: Citizen Lab Dark Basin, Google TAG, DOJ Azari; deck slide 5. [FN 81] [FN 85]

The hackers-for-hire authority pipeline

Commercial specialization converts nation-state-grade methods into purchasable litigation and reputation services.

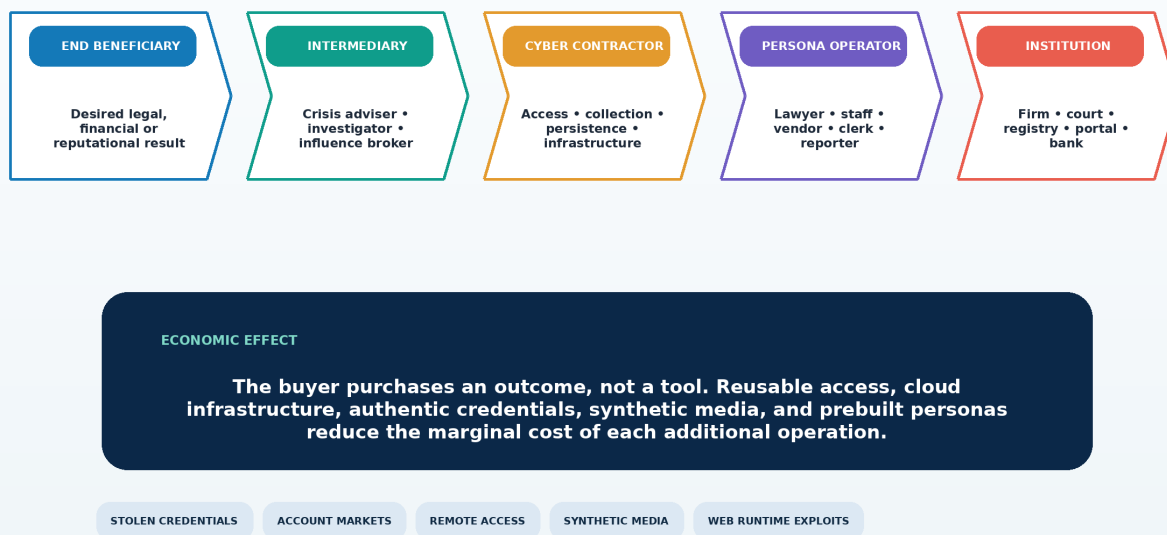


Figure 7. The hackers-for-hire authority pipeline

Source: Citizen Lab Dark Basin; Google TAG; DOJ hacker-for-hire prosecutions; CNF and ORACLE.

20. Recognized technique mappings

MITRE's account-establishment techniques describe the creation and cultivation of social-media and email accounts for later operations. These categories supply a precise vocabulary for preparation of a persona. The technique names are used according to their published definitions, rather than relabeling an email-account sub-technique as a generic professional-website category. [FN 91]

Valid-account abuse describes use of credentials that the targeted service accepts. It explains why a legitimate account can become the vehicle for an unauthorized instruction. In a co-opted-persona operation, the account's institutional appearance is retained because that appearance helps the instruction reach and persuade the intended recipient. [FN 92]

Spearphishing by link directs a target toward a chosen destination, while spearphishing through a service uses a platform's existing communication functions. The distinction identifies how the message reaches the target. Both can use a professional pretext, but the report names the delivery technique actually described by the source. [FN 93]

Stored-data manipulation concerns changing information that a system or user later relies upon. A substituted contact field, altered document or changed role record can affect a decision without making the surrounding service unavailable. This technique is

analytically relevant when the observed consequence is acceptance of a false state rather than an obvious outage. [FN 94]

An email-forwarding rule can copy messages to another destination while the original mailbox continues to function. The ordinary appearance of the inbox can therefore coexist with an additional collection path. In a professional context, that path can expose the timing, participants and substance needed to make later impersonation more convincing. [FN 95]

An adversary-in-the-middle position places the operator within a communication path. That is a technical mechanism, distinct from an author later disputing the contents of a displayed email. The report uses the mechanism term where the source describes the interception position and uses message-version dispute for the directly preserved documentary event. [FN 96]

Software-supply-chain compromise concerns tampering with software or its delivery process. Abuse of a legal directory or an institutional role can attack a chain of trust without being that particular software technique. Likewise, malicious HTML hosted on a package mirror can exploit trusted hosting without infecting a developer through package installation. [FN 97]

We find that technique labels are most useful when they explain an observed step in a sequence, with continuity determined by the linked accounts, content, timing and consequences rather than by a generic resemblance between two events. [FN 98]

Part V — Southern District of Florida Placeholder-Attorney Study

21. Population and source architecture

CNF's Table 1 enumerates 56 Southern District of Florida cases. The broader research universe exceeded 250 matters filed from 2018 through May 2025 and focused on approximately 32 attorneys. The report also identifies at least 62 federal matters across jurisdictions in which a placeholder entry was documented. These counts describe different source populations and are preserved separately. [FN 10]

The investigation began with docket behavior and filing anomalies, then tested the subject professional identities against credential exposure, email accounts, law-firm domains, DNS/MX history, portal activity, document metadata and professional-directory records. Table 2 preserves the attorney, paralegal and assistant addresses used to reconstruct communication pathways around the examined cases. [FN 10]

22. What happened after the placeholder entered

The reported mean tenure was 57 days from appearance to dismissal or withdrawal. Ninety-three percent of the studied placeholder matters terminated, resolved or were dismissed within that reported period. Eighty-one percent of placeholder activity consisted of no substantive filing, an appearance document or another non-substantive filing. None of the studied matters proceeded to trial through the placeholder's participation, and substantive dispositive activity was effectively absent from the late-entering cohort. [FN 10]

The operational pattern is short-duration occupation at a decisive stage. The attorney identity entered the case, acquired service and communication standing, and remained long enough to influence settlement, dismissal, withdrawal or procedural closure without undertaking the sustained work expected of ordinary merits litigation.

23. How the avatars were identified

CNF recorded 19 filings omitting Bar or court identifiers; less than one percent using the subject firms' branding logos; 78 percent of the suspect-document subset produced by four unusual PDF tools; caption errors in 62 percent of the suspect set compared with 37 percent in a random comparator set; and stale or incorrect firm contact information in 21 percent. The recurring shifts included fonts, spacing, caption format, signature blocks, office addresses, domains, telephone numbers and professional identifiers. [FN 10]

The decisive finding did not arise from one formatting defect. It arose from repeated combinations of identical or rotating irregularities across separate lawyers, firms and matters, followed by credential-exposure and infrastructure correlations. The convergence identified a centralized document-production and identity-use pattern operating through valid professional names.

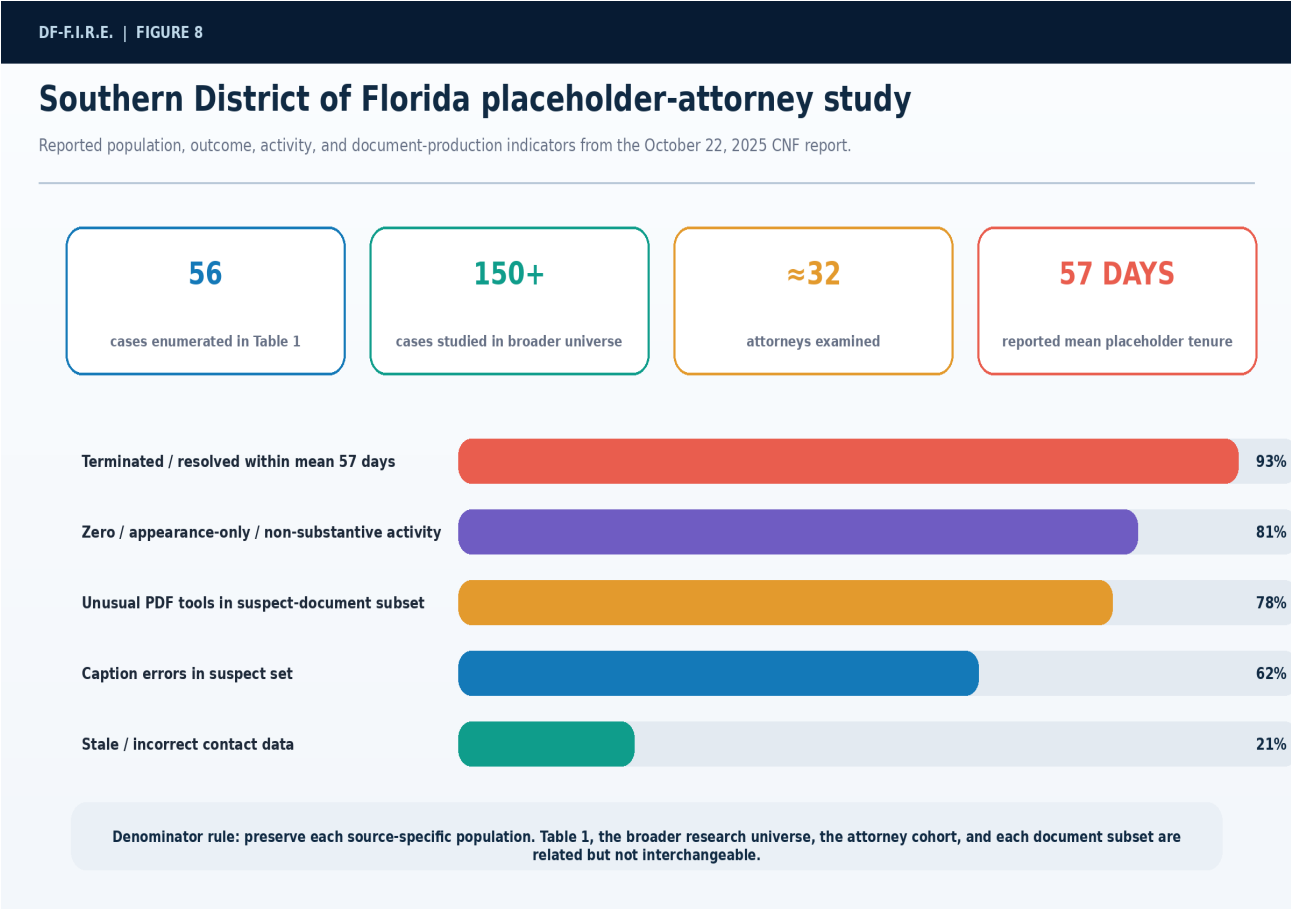


Figure 8. Southern District of Florida placeholder-attorney study

Source: CNF October 22, 2025 report, printed pp. 69–82 and Tables 1–2.

Part VI — Fifteen Independent Authority-Manipulation Case Studies

The following cases are independent of the bounded Florida field reconstruction. They establish the same threat class across court registries, settlements, foreclosure claims, judicial signatures, professional licensing, simulated hearings, enterprise hiring and fabricated firms. Each study identifies the represented identity, controlled channel, requested action and accepted consequence.

24. Piney Point Homes — court-registry funds released through compromised counsel communications

In Piney Point Homes, an attacker infiltrated counsel communications during a dispute involving funds held in a court registry. The manipulated instructions reached the clerk-facing release process and approximately \$1.07 million moved to an unauthorized destination. [FN 99]

The operation converted a compromised legal communication into an official disbursement. The court registry supplied the institutional authority; the attacker supplied the instruction that the registry accepted.

This case is a direct model for adjudicative-routing manipulation because the money remained under court control until the authority signal entered the release path.

25. Thomas v. Corbyn Restaurant Development — counsel impersonation redirects settlement

An attacker impersonated plaintiff's counsel and transmitted fraudulent instructions concerning a \$475,000 settlement payment. The message operated inside an active litigation relationship where counsel ordinarily directs the final transfer. [FN 100]

The professional identity supplied trust, the email channel supplied immediacy and the settlement supplied a time-sensitive transaction. The fraudulent instruction acquired force because it appeared to come from the lawyer authorized to complete the matter.

The case demonstrates that the operational endpoint of a lawsuit includes payment execution, not only the docket.

26. Erie Insurance v. WAWGD — more than fifty emails sustain the impostor

The Erie record describes an impostor participating in more than fifty settlement emails and changing the payment destination. The extended exchange supplied continuity, context and apparently independent corroboration. [FN 101]

The operator did not rely on a single spoofed message. The persona remained inside the negotiation long enough to learn the participants, language and expected next step, then altered the consequential instruction.

The case establishes durable communications-avatar tradecraft inside a legal settlement.

27. Oregon DOJ settlement diversion — both sides of the trusted exchange controlled

Oregon DOJ documented compromise of both the attorney and client accounts in a settlement transaction exceeding \$700,000. The attackers impersonated the client to provide payment instructions and the attorney to cancel a meeting. [FN 102]

Control of both apparent sides manufactured internal consistency and removed the planned direct-verification event. The cancellation and the false payment direction served one transaction.

The case establishes coordinated account avatars operating as a single authority environment.

28. Lisa Findley and Graceland — a fabricated lender becomes a court claim

Lisa Findley used a fabricated lender, forged documents and false court filings to claim foreclosure authority over Graceland. The invented entity was presented as the holder of enforceable rights. [FN 103]

The scheme used false historical documents as credentials. Once inserted into a legal process, the invented debt relationship was positioned to produce a genuine property consequence.

The guilty plea and sentence establish the complete path from false entity to court-facing authority.

29. Anton lagounov — fictitious agents seek real judicial signatures

Anton lagounov used fictitious federal-agent identities, an appropriated real-agent identity and fabricated investigative instruments. Communications asked federal court personnel to obtain judicial signatures on an urgent basis. [FN 104]

The operation sought to make the court complete the counterfeit. A genuine judicial signature would have converted the false investigative premise into an authentic institutional act.

The case establishes role substitution, urgency exploitation and judicial-authority conversion in one operation.

30. Miranda Devlin — valid professional credentials maintained for unauthorized practice

Miranda Devlin used the identities and license numbers of real attorneys, paid one lawyer's Bar dues and redirected mail containing a license card. The appropriated identities were then used to represent clients in court. [FN 105]

Active maintenance allowed the stolen credentials to survive a simple status check. The license remained valid while the operator using it was unauthorized.

The case is a direct credential-backed avatar model.

31. Leaford George Cameron — a fabricated multi-office law firm

Leaford George Cameron created a law-firm presentation using the stolen identity of a retired attorney, fictitious lawyers and staff, office representations and legal filings. [FN 106]

The firm itself functioned as the avatar. Clients encountered a complete professional organization rather than one suspicious profile, and the invented internal roles reinforced one another.

The case establishes that a false legal organization can enter transactions and proceedings through appropriated professional authority.

32. Matthew Weidner — a real lawyer's name and Bar number inserted into a pleading

An AI-generated filing used attorney Matthew Weidner's real name and Bar number in a matter he did not handle. The correct professional identifiers were attached to an unauthorized act. [FN 107]

The filing demonstrates that accurate identity fields can be the mechanism of deception. A recipient checking the name and number would confirm the genuine lawyer while missing the absence of authorization.

The case establishes document-level authority laundering through professional data.

33. Angel Ariel Bermudez — simulated hearing, real regulatory consequence

Scammers used attorney Angel Ariel Bermudez's identity and Bar number in a scheme that included a fabricated online hearing with purported judicial and police authority. [FN 108]

The controlled roles reinforced one another and presented a complete adjudicative environment. The genuine lawyer later faced a real complaint associated with the operation.

The case establishes the movement from simulated proceeding to persistent professional record.

34. Edmond Abordo — forged chief-judge authority in a property scheme

Edmond Abordo used a chief judge's identity, signature and court seal in a fabricated order connected to property and foreclosure representations. [FN 109]

The false instrument borrowed the highest visible authority in the court and presented the requested property state as already adjudicated.

The case establishes judicial-identity appropriation as a mechanism for altering property and foreclosure decisions.

35. Andrew Wynne — fabricated orders across approximately thirty client matters

Andrew Wynne created false court orders, forged judicial signatures and manufactured communications across approximately thirty client matters. [FN 110]

The repeated instruments preserved a false procedural world in which cases had advanced, judges had acted and client objectives remained under professional control.

The operation demonstrates serial record-state avatars: each false order represented a proceeding that did not exist in the form shown to the client.

36. Matthew Elstein — sham records and a fabricated settlement

Matthew Elstein used fake court materials, false procedural histories and a fabricated settlement to maintain client reliance and obtain money. [FN 111]

The professional relationship made the false records actionable. Clients relied on counsel to translate the court's state, and the operator supplied a counterfeit version of that state.

The case demonstrates how a trusted lawyer role can become the delivery system for a fictional adjudicative record.

37. FBI fictitious-law-firm recovery schemes

The FBI documented fictitious law firms targeting cryptocurrency-fraud victims with professional-looking websites, purported attorneys, intake processes and payment demands. [FN 112]

The websites supplied verification, the professional roles supplied authority and the victim's prior loss supplied urgency. The operation combined identity, intake, data collection and financial exploitation.

The scheme is directly amplified by server-side website compromise because a genuine legal website can be repurposed to perform the same intake and redirection functions.

38. North Korean remote-worker operations — accepted enterprise identities operated by substitutes

FBI, DOJ and Microsoft reporting documents stolen identities, substitute interviewers, facilitators, front companies and accepted enterprise accounts used by North Korean remote workers. [FN 113]

The organization creates genuine laptops, mailboxes, access rights and directory entries for the accepted identity. The authority-avatar operation begins at enrollment and then moves through normal enterprise systems.

The model applies directly to law firms, vendors and court-adjacent organizations because a person functioning as staff, contractor or technical administrator acquires internal authority before the identity conflict is detected.

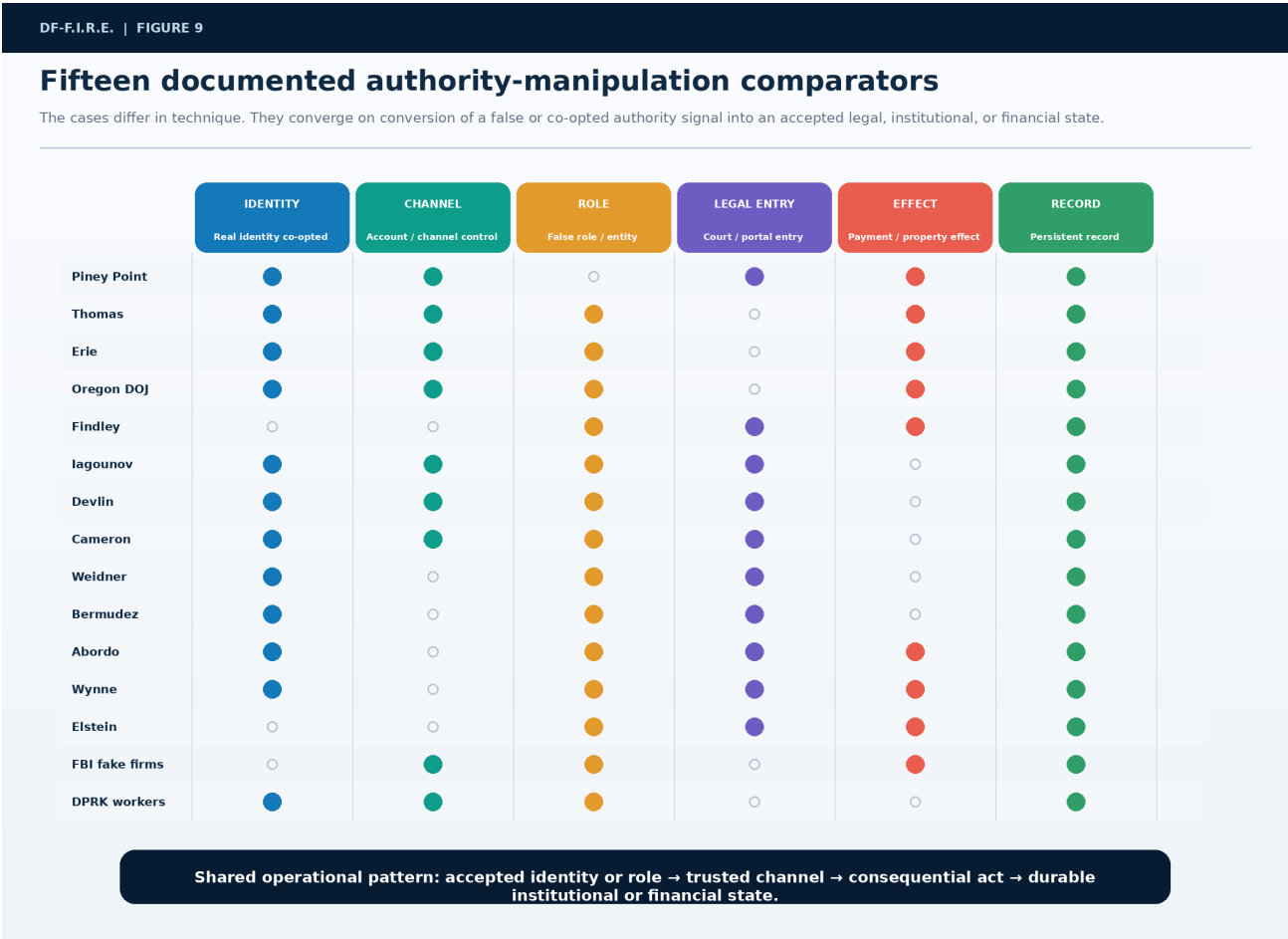


Figure 9. Fifteen documented authority-manipulation comparators

Source: Official court opinions, DOJ prosecutions, FBI alerts, state regulator reporting and Bar publications identified in Sections 24–38.

Part VII — Beyond the Attorney: Firms, Vendors, Staff, Clerks and Judges

39. The intra-firm avatar at a global firm

The G.S. study examines a professional identity associated with an international law practice whose offices, teams and matters are geographically distributed. Historical judicial references establish a genuine professional baseline. Later account and representation activity supplies the event-specific authority question. [FN 114]

A global firm creates legitimate organizational distance. A partner in one office may have no daily contact with an associate, contract lawyer or specialist in another. Colleagues verify the identity through directory entries, email history, matter references and internal role labels. An operator controlling those signals can function between teams before anyone compares the represented person with the source of the specific act.

The operational unit is the instruction: who entered the matter, who communicated with the client or court, which address received service and which account approved the act. The firm's genuine name and global footprint supply the trust environment in which the avatar operates.

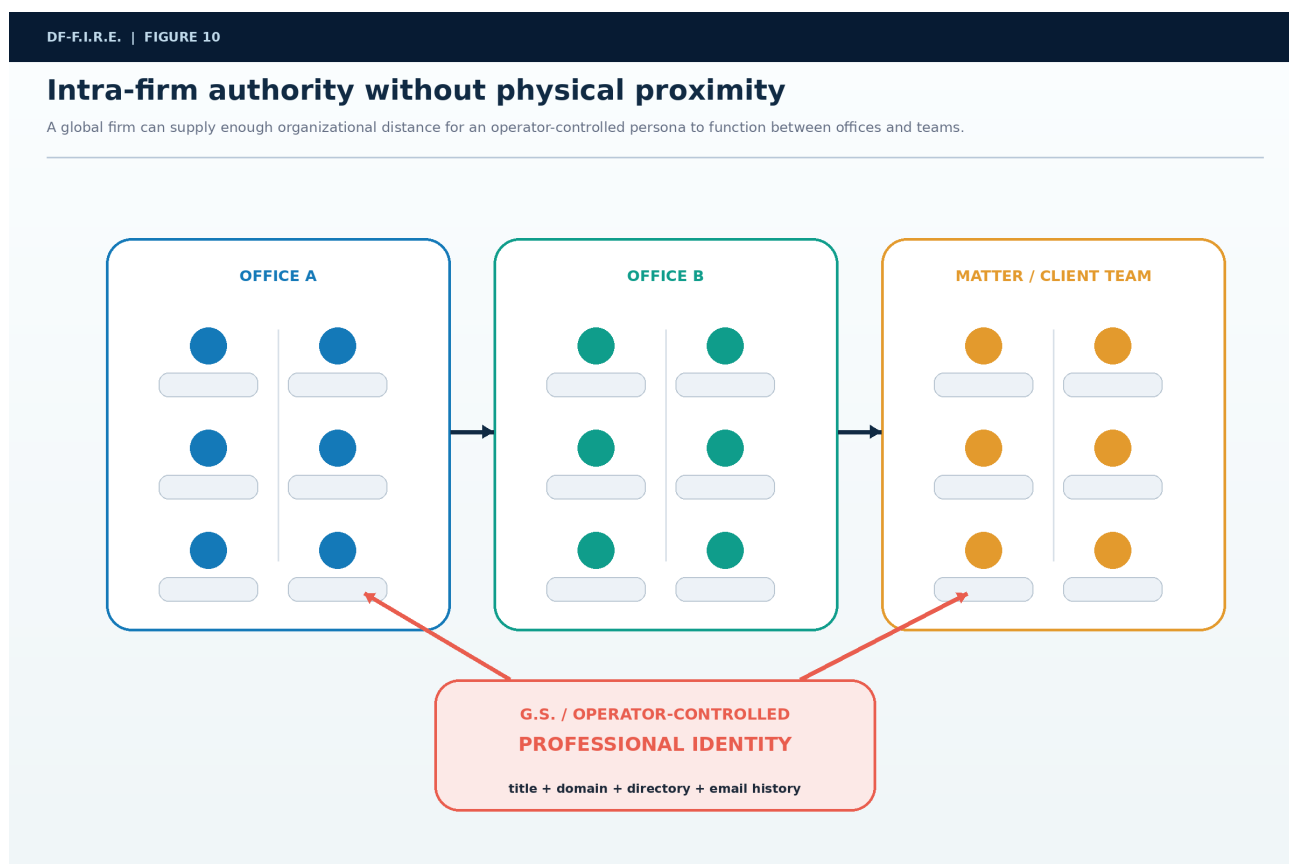


Figure 10. Intra-firm authority without physical proximity

Source: DF-F.I.R.E. reconstruction of the G.S. account-and-role model in a global firm.

40. Vendors and legal supply chains

Law firms and courts depend on hosting providers, PHP applications, plugins, identity providers, mail relays, cloud storage, customer-relationship systems, e-discovery vendors, court reporters, process servers, payment processors, managed service providers and professional directories. Each vendor carries a piece of identity, communication or workflow authority.

A vendor account can modify a professional profile, reset a mailbox, change a DNS record, issue a document link, alter a service list or direct payment. The action appears to arise from the legitimate supplier because the operator is using the supplier's accepted administrative path.

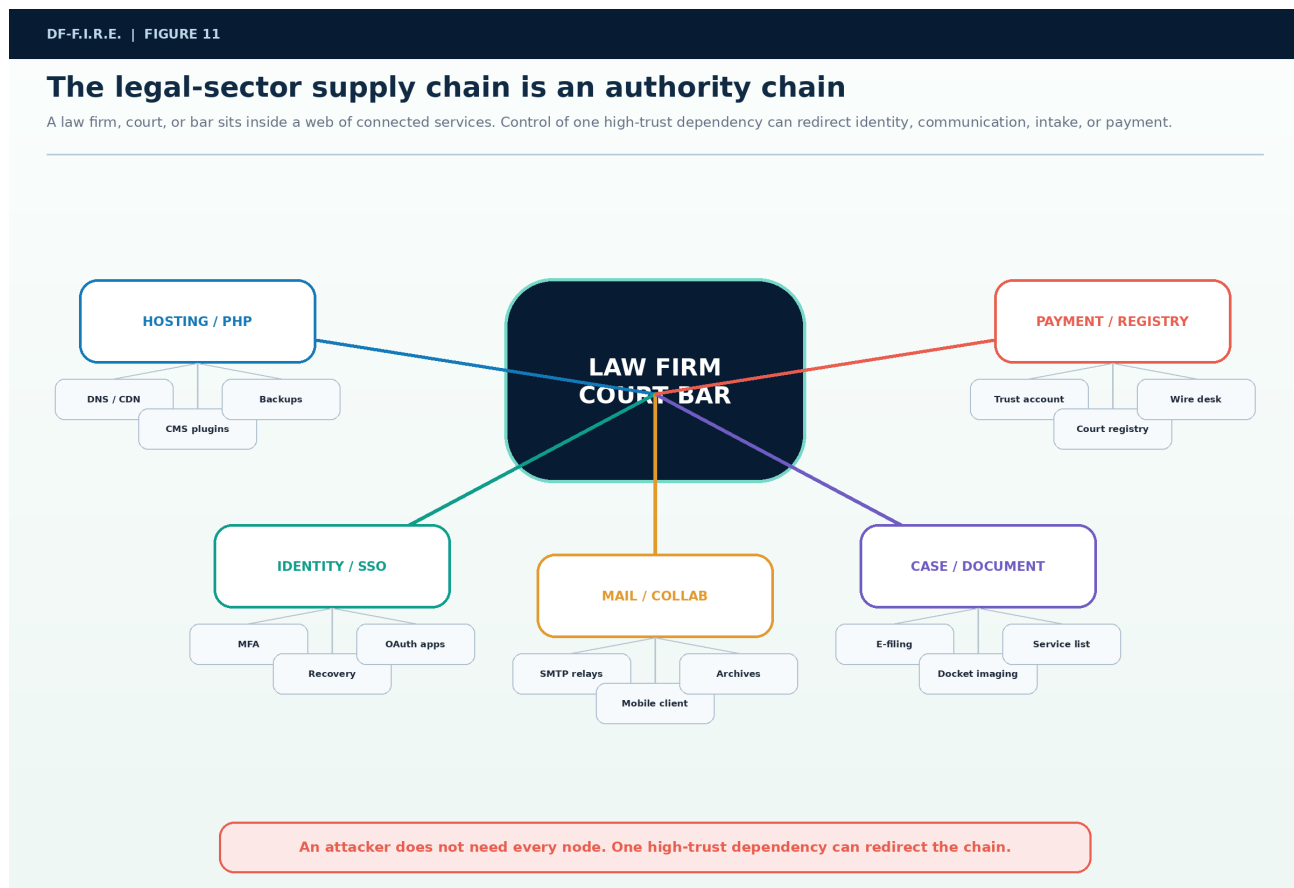


Figure 11. The legal-sector supply chain is an authority chain

Source: CNF DNS/MX and portal research; RAPS restricted-portal model; PHP connected-service analysis.

41. Paralegals, assistants and staff as authority carriers

Table 2 of the CNF report includes legal assistants and paralegals functioning within placeholder communication paths. Staff identities carry procedural authority because they schedule, transmit, file, serve, collect signatures, maintain service lists and convey counsel's position. A staff account can place an operator inside the workflow without requiring the operator to perform every act under the lawyer's name. [FN 10]

42. Clerks, registries, law clerks and chambers

Clerks control intake, case association, imaging, sealed-document handling, service generation, fee status and court-registry release. Law clerks and chambers staff control calendaring, document routing and judicial communication. A counterfeit instruction directed to those roles can create a genuine docket entry, release genuine funds or present a fabricated request to a judge.

Piney Point demonstrates registry release through compromised counsel communication. Iagounov demonstrates requests for judicial signatures. Abordo, Wynne and Elstein demonstrate forged judicial authority. Bermudez demonstrates a simulated hearing with multiple adjudicative roles. The combined record establishes the entire court-facing role surface.

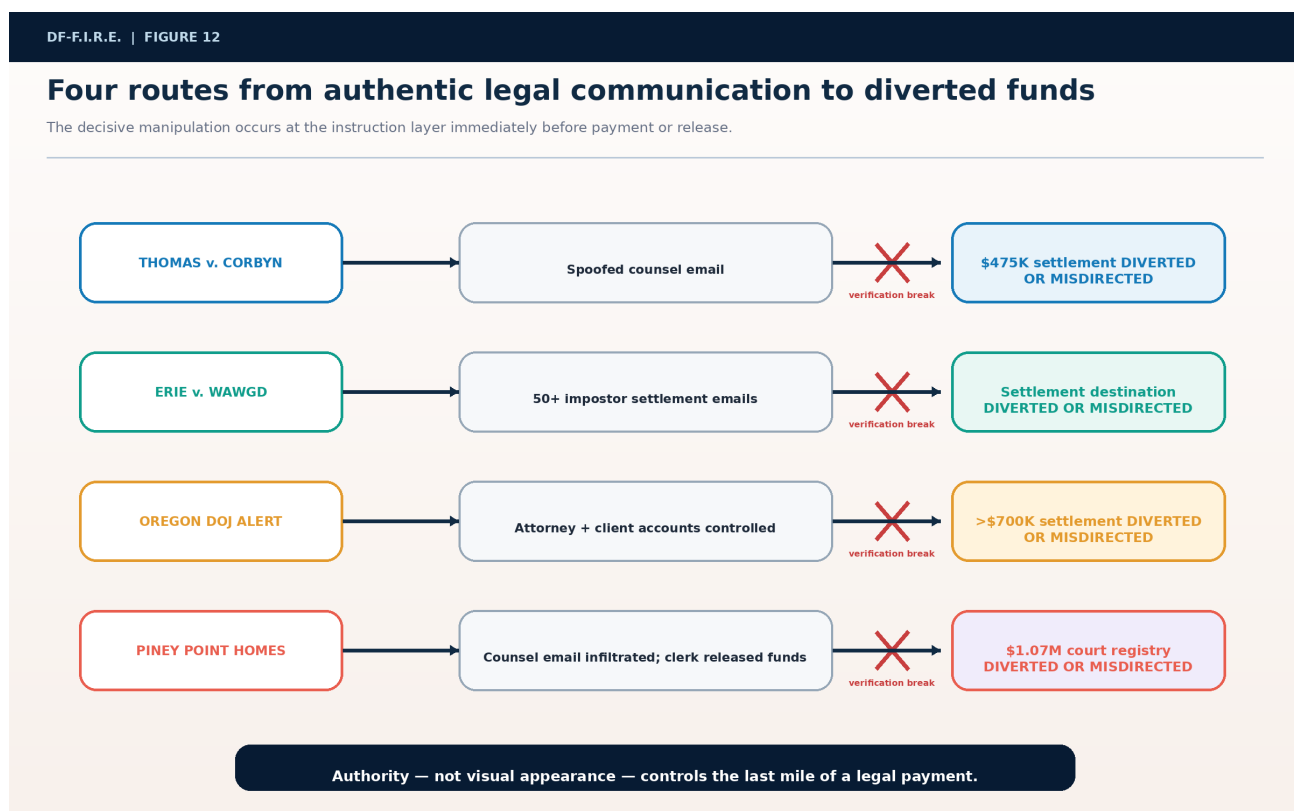


Figure 12. Four routes from authentic legal communication to diverted funds

Source: Piney Point, Thomas, Erie and Oregon DOJ records.

Authority roles inside an adjudicative environment

A multi-role operation manufactures the social and procedural environment in which authority is ordinarily recognized.

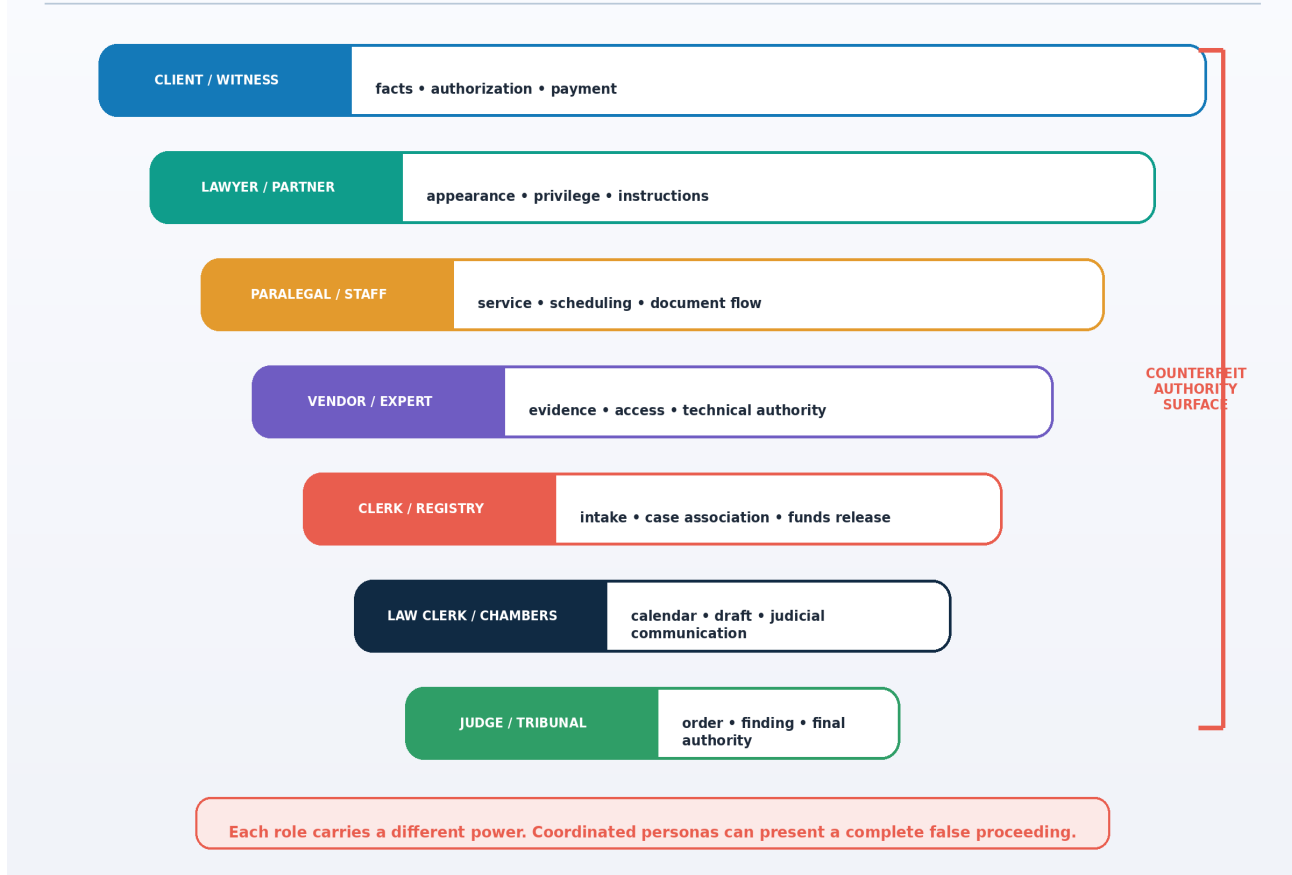


Figure 13. Authority roles inside an adjudicative environment

Source: DF-F.I.R.E. role-and-authority taxonomy based on ORACLE and independent case records.

Part VIII — Bounded Anonymized Florida Field Reconstruction

This section presents a bounded field reconstruction using direct source objects. The targeted attorney is not identified. Professional identities are abbreviated because the forensic object is the authority-bearing transaction, account or representation used in the proceeding.

43. J.D.W. — response population, acknowledgment and nonresponse conversion

The September 17, 2024 correspondence identifies eleven grievances as requiring responses and distinguishes other matters for which no further response was required at that time. The base file numbers are the controlling comparison fields. They permit the later thirteen-file narrative to be tested against the actual population described in the earlier message. [FN 115]

Individual letters supply additional timing. The September 10 letter for file 2025-70,132 gives a September 25 deadline, while the October 9 letter for file 2025-70,140 gives an October 21 deadline. These are file-specific obligations, and their dates remain separate from the collective chronology used in later litigation. [FN 116]

The October 31 correspondence gives November 12 as a response deadline for the two later matters and describes referral to a grievance committee following nonresponse. That language identifies a before-and-after sequence: response period first, referral consequence afterward. It is therefore a substantive chronology field, not merely an administrative date printed at the top of a letter. [FN 117]

The October 14 communication explains the response package and continuing communication problems. At 9:38 a.m. on October 15, Christine Mitchell acknowledged receipt of the email sent the previous evening, with John D.W. included in the correspondence. We find with very high confidence that an institutional acknowledgment appears in the preserved record. [FN 118]

Receipt, completeness and compliance are different states. The acknowledgment establishes a received communication; the later petition advances a nonresponse theory. The important comparison is how the received material was characterized in the later filing, including whether the claim concerns no submission, an inadequate submission or a failure to answer particular inquiries. [FN 119]

The November 25 petition combines thirteen matters in its nonresponse narrative. The preceding letters establish different deadlines and at least two identifiable cohorts. We find that the aggregate presentation compresses the chronology, and that a file-by-file comparison exposes material differences that disappear when the thirteen matters are treated as one uniformly overdue group. [FN 120]

The Florida Bar's May/June 2024 disciplinary roadmap expressly states that Bar Counsel may serve as an investigating member. The applicable distinction is between eligibility to perform that function and the authority for the particular assignment. We compare the assignment language with the institution's published description of the process and the subsequent acts attributed to the assigned role. [FN 121]

An investigating function and a committee's decision-making function are not identical. The disciplinary rules distinguish committee composition, investigation and voting, including restrictions associated with participation as the investigating member. Consequently, the significant questions in a role-bearing document are what function was assigned, by which represented authority, and how that function was described in the subsequent proceeding. [FN 122]

The October and November materials describe John D.W.'s role in relation to Committee 17F and identify Richard W. in a chair capacity. These representations matter because they connect a staff action to committee authority. We preserve the exact asserted relationship and its date rather than inferring that any use of the investigating-member title necessarily identifies an impostor. [FN 123]

A separate October 30, 2024 Campbell petition provides a concrete comparison: its counsel and contact fields place William Wonil Chung in differing institutional configurations, including a staff-counsel field using Patricia S.'s address. The source demonstrates that the fields in an authority-bearing pleading can conflict internally. The observable finding is the mismatch itself, which can be compared with other pleadings without converting a template field into proof of a fabricated person. [FN 124]

The John D.W. study connects inquiry lists, deadlines, response receipt, referral language and counsel transition. We find that those objects describe a changing response population and changing authority relationships during the period preceding the petition. Their combined significance comes from the relationship among the records, not the typography of a name or the number of digits in a Bar identifier. [FN 125]

Figure 6. Acknowledgment compared with nonresponse representation. Source: Master deck slides 36, 38, 40; October acknowledgment / November petition. [FN 118] [FN 119]

44. R.B. and Staff Investigator J.B. — source denial and message-version conflict

The preserved March sequence begins with a message attributed to Bar Counsel proposing dismissal without prejudice on conditions involving an in-person meeting and further responses. The targeted attorney replied accepting the proposed arrangement

and seeking direct engagement. Messages attributed to Staff Investigator then denied that the office had sent the supposed Bar Counsel communication and rejected the proposed dismissal. [FN 126]

The Bar's later motion and affidavit package dispute the authorship and authority of that proposed resolution. They point to the spelling "Randell" in the purported communication and associated proposed stipulation, while identifying counsel as Randall B.. The exact name variation forms part of the institution's stated evidentiary reasoning. [FN 127]

The disputed proposal carried more than an identity claim. It represented a change in the proceeding's course: dismissal without prejudice, an in-person meeting and a defined period for further submissions. That combination makes the message an authority-bearing object because its acceptance would alter what the recipient believed was required and when. [FN 128]

The denial was communicated through an investigator introduced by Bar staff, rather than through a direct substantive reply from the supposed author of the proposal in the copies examined. The investigator's message used the institution's name and stated its position about dismissal and outstanding responses. The sequence therefore requires the roles of purported author, communicating staff member and litigating institution to remain separate in the analysis. [FN 129]

The June affidavits supply the institution's account of that delegation. Staff Investigator says Randall B. showed him the disputed email and asked him to notify the targeted attorney that it was false; Randall B. supplies his own sworn denial and describes asking Staff Investigator to send the response. Those statements are evaluated as the stated basis of the institutional position, as a documented representation of counsel-to-investigator delegation. [FN 130]

On March 17, Staff Investigator wrote that the email included in the targeted attorney's response was not the email he had sent on March 14 and that it had been changed. He said he attached the original for comparison. We find with very high confidence that this preserved communication documents a direct version dispute involving an institutionally attributed message. [FN 131]

The March 17 message performs two functions: it challenges the attributed content and reiterates that the Bar will not stipulate to dismissal. Those functions should not be merged. The first concerns message integrity, while the second communicates a litigation position through the same disputed stream. [FN 132]

The March 18 filing places the changed-email statement before the court as part of the targeted attorney's account of the disputed communications. The integrity concern was therefore disclosed within the contemporaneous motion sequence, not introduced for the first time after the later emergency petition. The dates establish when the court-

facing record began carrying competing descriptions of the same message stream. [FN 133]

The March 19 Bar motion expressly discusses Staff Investigator's messages and attaches the March 17 changed-email statement. It rejects the proposed stipulation and characterizes the disputed emails adversely to the targeted attorney. We find that the institution formally adopted an account of the authenticity dispute and submitted relevant correspondence as part of its requested relief. [FN 134]

The subsequent June affidavit package carries the denial and selected correspondence into the emergency-suspension request. This is an evidentiary-dependency chain: the communication dispute is described in a motion and then in sworn supporting material. Repetition increases the institutional importance of the episode, while the underlying acts and versions remain the objects from which the repeated descriptions derive. [FN 135]

Figure 4. The March 2025 changed-message evidence sequence. Source: Master deck communications-state visuals; March 2025 source exhibits. [FN 131] [FN 135]

The targeted attorney requested an in-person meeting to address the responses and communication problems, and the March 19 message declined further in-person meetings. The March 20 motion then asked the court to require counsel to meet and confer, with a short period for any additional responses. These documents establish both the proposed alternate contact method and the institutional response communicated at that time. [FN 136]

Independent verification separates a consequential instruction from the channel carrying the disputed instruction. In this record, the proposed meeting would have brought the represented professionals and their source copies into the same exchange. We find that the request had a specific verification function in addition to its procedural purpose. [FN 137]

The Randall B. case study is strongest as an analysis of role, message attribution and institutional reliance. A validly identified professional role became the apparent source of a proposed resolution; that proposal was repudiated; a second attributed communication was described as changed; and the dispute became part of a formal request for adverse action. We find that the sequence connects professional authority, disputed authorship and formal institutional reliance. [FN 138]

45. P.S. — private-counsel routing through an institutional address

The February 26, 2025 email reproduced in the February 27 motion identifies its sender as the firm's chief operating officer, chief operating officer of Weiss Serota. It acknowledges receipt of a lawsuit and exhibits delivered to the firm's Coral Gables office

the preceding day. It then directs future communications through the named legal counsel and requests that the recipients stop contacting the firm's personnel directly. [FN 139]

The designated counsel is Patricia S. at a floridabar.org address. That field changes the communication route from the law firm to an official institutional address associated with Bar Staff Counsel. We find with very high confidence that the preserved email presents a specific private-representation claim, not merely a courtesy copy or an incidental mention of an official's name. [FN 140]

The March 7 response in the disciplinary proceeding identifies Patricia S. as Staff Counsel for The Florida Bar and bears that office's signature and service information. Read with the February 26 email, the records present two capacities within a short period. The authority collision is especially significant because the private firm was itself involved in a dispute with the recipient of the Bar communications. [FN 141]

Patricia S.'s professional identity has a dated institutional history, including a 2005 university event account and a 2022 LegalFuel interview. The latter describes her work with the Bar beginning in 1997. The case-specific issue is therefore the private-firm designation and communication instruction attributed to her role in February 2025, rather than a claim that her professional identity first appeared at that time. [FN 142]

Florida's conflict rule addresses direct adversity and significant risks that one representation will be materially limited by responsibilities to another client or by other specified interests. The two represented capacities make that framework relevant to the February–March documents. We identify the documentary collision precisely: private defense counsel was named at the same official address used by an institutional participant in the disciplinary process. [FN 143]

The email's practical effect is a change of recipient and a restriction on direct access to the firm's personnel. That combination is characteristic of an authority-bearing instruction because it tells the recipient both who may speak and which channels may no longer be used. In a communication-integrity investigation, the designated contact is therefore part of the evidence, not a peripheral administrative detail. [FN 144]

The February 27 motion brings the designation to the court and describes attempts to alert the firm to the communication problem. The December 27 protective filing had already raised communication-security concerns in the disciplinary setting. The private-counsel instruction thus appears inside an existing notice chronology rather than as an isolated later recollection. [FN 145]

Our finding is an apparent dual-capacity designation carried through a private law firm's communication and an official Bar address. The decisive fields are the named counsel, the institutional domain, the claimed client, the direction to cease direct contact and the

later Staff Counsel signature. Those observable features support a high-confidence finding of an authority inconsistency with potential consequences for who receives and controls the exchange. [FN 146]

Figure 7. Dual-capacity representations in February–March 2025. Source: Feb. 26 source email and March 7 Bar response. [FN 140] [FN 141]

46. R.W. — committee authority and reassignment

A 2022 disciplinary filing supplies an earlier 17F roster naming Nakia Ruffin as chair and Richard W. as vice chair. This establishes an institutional committee connection at that date. It is a dated baseline, not a substitute for the membership and leadership state represented in the October–November 2024 correspondence. [FN 147]

The current 17F page names Marcela Gyires as chair, and a law-firm announcement concerning her selection is dated July 22, 2025. Those records establish later published representations. Their dates are retained as stated, rather than moved backward to create an unsupported effective appointment date in 2024. [FN 148]

The field correspondence repeatedly identifies Richard W. in a chair role during the same period that a Weiss Serota notice identifies the firm as acting for Regus Management in an adverse premises matter. The notice is dated October 17, 2024 and bears a named attorney's signature. The combined chronology supplies a defined institutional-role and private-representation overlap for analysis. [FN 149]

The December 30 corrected response recounts a statement that Richard W. had been removed because of a conflict. That account is preserved as the pleading's description of a communication, alongside the underlying chair references and law-firm notice. The record is strongest when each item retains its own evidentiary character: direct document, reported conversation or institutional rule. [FN 150]

The November 2024 petition uses the 17F designation, while the June 2025 emergency package presents identified grievance matters under 17A. The base file number and committee suffix perform different functions: one identifies the matter, while the other represents its assigned institutional location. Comparing both fields exposes changes that disappear when documents are grouped only by the targeted attorney's name. [FN 151]

We find that committee designation is an operational state because it influences the represented path of investigation, review and later reliance, and the analysis preserves each base number and suffix across the documentary sequence. [FN 152]

The November petition and the June emergency request are different procedural objects. Their timing, underlying file populations and requested relief are compared separately before their relationship is described. This prevents a later emergency-

suspension framework from being retrospectively assigned to every earlier letter or communication. [FN 153]

The committee study connects the represented leadership role to the institutional actions taken under that representation. The documented sequence includes chair representations, an adverse private-firm notice, a later private-counsel designation at a Bar address, changing case suffixes and institutional reliance on those records. We find that this is a multi-object authority problem, not a single disputed biography. [FN 154]

Figure 8. Committee chair, investigating role and suffix transitions. Source: Master deck slides 37–39; 2022 roster and 2024–25 records. [FN 147] [FN 154]

47. Staff Investigator J.B. — institutional communication and source compression

The March correspondence places Staff Investigator in the communication path after a Bar paralegal introduces him as the person who will contact the targeted attorney. His affidavit later describes acting at counsel's request when communicating the denial of the purported settlement. That sequence establishes a represented delegation from counsel to investigator within the source record. [FN 155]

The investigator communicates that no dismissal has been agreed and that the Bar has not received the required responses. He also identifies an attributed message as changed. We find that his role in the record is not confined to gathering background facts: his communications transmit the institution's position and become evidence about the integrity of the communication stream itself. [FN 156]

The targeted attorney's March 18 filing recounts the repudiation and the changed-message statement. The following day's motion responds to that sequence and incorporates the correspondence. The order of these events matters because it establishes that the integrity dispute was part of the material exchanged before the later emergency-suspension package. [FN 157]

The March 19 pleading and June affidavit package describe overlapping portions of the same episode, but they are not identical compilations. The March pleading attaches the March 17 changed-message statement; Staff Investigator's June narrative describes the March 14 denial and the purported Randall B. message. We preserve the difference in scope because downstream readers can receive different evidentiary pictures from the two packages. [FN 158]

Staff Investigator's affidavit includes his account of a discussion with Randall B. and a separate account of statements attributed to FBI agents on May 5, 2025. These are distinct source relationships inside one sworn document. The affidavit's formal

presentation does not erase the difference between personal observation, another person's denial and the affiant's summary of an external conversation. [FN 159]

The ORACLE analysis compares the categorical description of no investigation with preserved communications describing meetings, evidence intake and contemplated technical examination, treating historical intake activity and the status of a formally opened investigation as different propositions. [FN 160]

We find that the important evidentiary mechanism is source compression: a short sworn narrative becomes the principal representation of a larger and contested communication sequence. The narrative can gain authority through its formal placement even as the surrounding correspondence becomes less visible to later readers. This is why the report follows what each successive source actually says about the earlier message. [FN 161]

The Staff Investigator study therefore yields a high-confidence finding of an acknowledged message-version conflict within an institutionally used communication stream. The source record also establishes that counsel and the investigator supplied sworn denials and that the Bar adopted a litigation position about the disputed material. These are the facts supporting the authority-pathway analysis. [FN 162]

48. E-court notices, service lists and accepted state

An electronic submission creates a transaction record, while clerk acceptance and case association are subsequent processing states. The preserved receipts distinguish the filing number, time, filer, court, case fields and recipients. The report uses those fields separately because a notice of transmission and a later docketed document represent different steps in the same workflow. [FN 163]

The December 17, 2024 receipt records filing 213069218 at 11:53:58 p.m. Eastern Time and identifies the Supreme Court of Florida. Both case fields display UNKNOWN, and the selected recipients include John D.W.. These are directly observable transaction attributes that can be compared with the later treatment of the submitted response. [FN 164]

The June 18, 2025 emergency-petition notice records filing 225491716 at 8:20:04 a.m. Eastern Time, identifies Patricia S. as filer and displays NEW CASE. That label describes the submission's pre-number state in the preserved notice. It is retained as part of the ordinary intake chronology, rather than used by itself as evidence of a counterfeit proceeding. [FN 165]

The supplemental authority-pathway analysis places the portal submission and the later permanent case-number notice in sequence, demonstrating that an ordinary intake label must be distinguished from a later disputed document or relationship state. [FN 166]

A person listed in a portal directory is not necessarily selected for a particular transmission. A selected recipient, a successful transmission and a recipient's actual awareness are also different states. The displayed lists are therefore transcribed with their headings, so an unselected name is not silently counted as a served participant. [FN 167]

The March 7 response and its portal notice provide a useful paired record. The response identifies its signing counsel and certificate of service, while the notice identifies the transaction and displayed recipient population. Comparing those objects establishes what each system layer represented about the same filing event. [FN 168]

A genuine electronic filing system processes the authority presented to it. When an accepted account submits an object, the resulting transaction can look ordinary even though the user's authorization or the document's content is disputed. We find that system authenticity and transaction authenticity should be evaluated as connected but separate properties. [FN 169]

Figure 9. Court submission, service and institutional reliance. Source: Master deck slides 1, 26, 42–44; court notice artifacts. [FN 169]

The earlier court-notice studies address several different objects: an emergency-petition service notice, a court-service message and a later removal-from-service-list message, each of which must retain its own sender, time, recipient population and asserted procedural meaning. [FN 170]

A court-related message can pass through a separate portal or contracted delivery service. The authentication comparison identifies the envelope identity, signing domain and visible sender domain rather than assuming that every technical hostname must match the institution's public website. The message's claimed legal effect is then compared with the event it purports to announce. [FN 171]

The October 2025 investigation treated court-themed messages and grievance communications as part of one surrounding digital environment, using the correspondence, routing observations and procedural timing together to locate possible interference with legal work. [FN 172]

The June 18 receipt anchors an actual emergency-petition submission. The accompanying affidavit package identifies the material offered in support. Those objects provide a concrete comparison point for later messages referring to a proceeding, because the filing's identity and content are already represented in preserved documents. [FN 173]

We treat a pre-number label as an intake state and examine any additional discrepancy at the field where it occurs, including the asserted case, the recipient population, the action announced and the destination to which the recipient is directed. [FN 174]

A court or Bar theme supplies a persuasive reason to open a message promptly. A recipient may believe the communication concerns a deadline, complaint, required response or removal from a service list. The important operational feature is the action induced under that apparent authority, especially where the message changes how the recipient communicates or seeks access to a document. [FN 175]

The June 25 study's focus on a broad and unusual distribution list remains relevant as a recipient-scope inquiry. A distribution list is compared with the subject, case description and asserted action rather than interpreted from its size alone. The same preserved message can contain duplicate entries, professional addresses and personal addresses, and each category has a different significance for exposure and routing. [FN 176]

A recipient's attempt to correct an unexpected notice can itself become part of the interaction. Replying to an address supplied by the questioned message or following its embedded contact directions keeps the recipient inside the same represented channel. We find that the response path is part of the impersonation surface, not merely the initial sender line. [FN 177]

An attachment carries its own content and production history. A genuine message can deliver the wrong version, and a genuine-looking attachment can be accompanied by a false description of what it does. In the field record, the same principle appears when correspondence is reproduced in a pleading: the attachment and the pleading's characterization require a direct comparison. [FN 178]

A link can remain unchanged while the content or destination behind it changes. The object visible to the recipient at the time of use is therefore part of the evidence. This applies both to professional profiles used for verification and to document links that appear to identify one stable filing or notice. [FN 179]

We find that the practical legal consequence lies in the transition from the message or document to the state accepted by the next actor, such as a changed service address, an assumed deadline, a supposed appearance or a belief that a response was never received. [FN 180]

Three preserved authority-collision artifacts

Enlarged, redacted source excerpts preserve the operative language without reproducing unrelated personal identifiers.



Figure 14. Three preserved authority-collision artifacts

Source: Redacted source exhibits dated February 26, March 13 and March 17, 2025.

Part IX — Detection, Containment and Resilient Access to Judicial Power

49. Detection begins with authority differences

The highest-value indicators are changes in the relationship between identity and action: a new contact destination, an unfamiliar service recipient, an unexpected appearance, a role that conflicts with the public roster, a document created by a different production path, a message version repudiated by its attributed sender, or an instruction that changes who may communicate.

Technical monitoring supports that comparison. High-value records include PHP and web-server logs, administrative login history, source-control changes, database and file-integrity history, secret access, OAuth grants, mailbox permissions, session tokens, account-recovery events, DNS/MX changes, portal access logs, NEF/e-service generation logs, docket imaging, payment and registry audit trails, and professional-directory revisions.

50. Containment must preserve legal continuity

Independent verification of payment, settlement and account-change instructions is a mandatory containment control because the questioned channel can carry an authentic-looking instruction under attacker control. [FN 181]

Containment removes attacker control while preserving the target's ability to reach clients, courts, regulators and counterparties. The response therefore establishes verified out-of-band contacts, freezes high-risk changes, rotates secrets, revokes sessions, preserves source artifacts, compares accepted records, and informs institutions that relied on contested instructions.

Judicial continuity requires a channel that reaches judicial authority outside the contested rail. A backup email that re-enters the same portal, clerk queue or compromised service list is not independent. The alternate route must have separately verified identity, custody, receipt and decision authority.

51. Professional-identity recovery

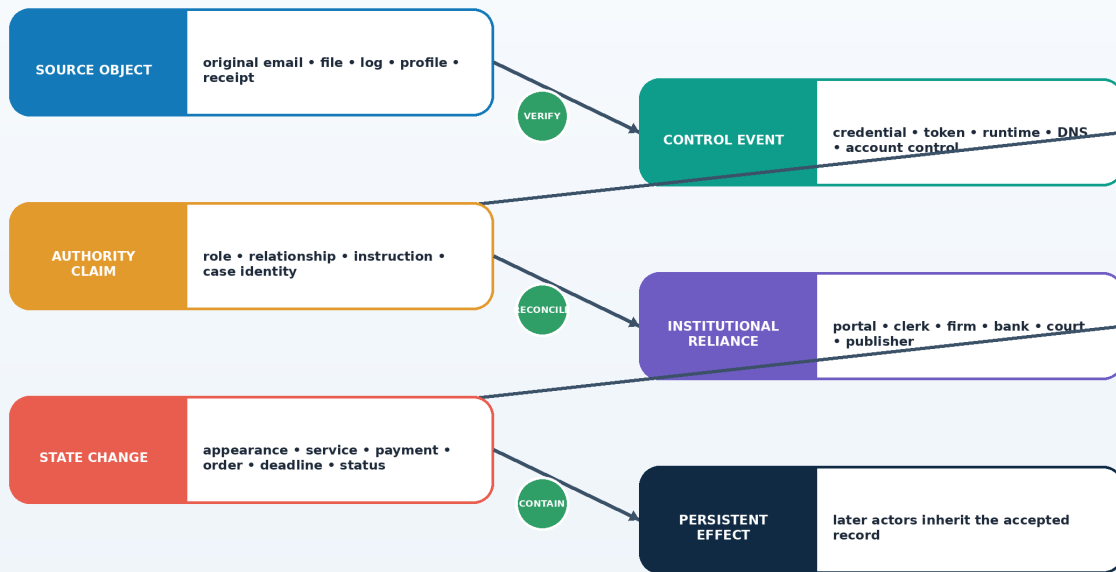
Recovery includes the website, mailbox, directory, Bar profile, employer biography, search result, social account, client portal and court record. Each location is compared with the last verified state. Corrections are documented with acquisition time, source copy, responsible custodian and confirmation that the institution changed the accepted record.

52. Response priorities for the PHP emergency

1. Identify every public PHP application and its exact version.
2. Patch or isolate affected runtimes and preserve pre-change images and logs.
3. Rotate application secrets, database credentials, mail credentials, API keys and OAuth tokens reachable from the application.
4. Revoke sessions and inspect administrative, service and recovery accounts.
5. Compare professional profiles, contact instructions, intake destinations and document links with verified source records.
6. Review mailbox permissions, forwarding rules, delegates and application access.
7. Validate DNS, MX, nameservers, CDN, hosting and account-recovery settings.
8. Identify every institution that received a consequential instruction during the exposure window.
9. Reconcile court filings, service lists, registry payments, settlement directions and professional-status records.
10. Maintain an out-of-band authority channel until both technical and institutional states are restored.

DF-F.I.R.E. source-to-consequence operating model

The final finding follows the complete path. It does not stop at the suspicious message, profile, or account.



When independently preserved sources converge across these stages, the authority-avatar operation is established as a complete institutional event.

Figure 15. DF-F.I.R.E. source-to-consequence operating model

Source: Integrated CNF, ORACLE, RAPS, CCDG and independent case methodology.

Part X — Integrated Findings and Final Determinations

53. Professional identity is an operational control surface

We find with very high confidence that professional identity is more than a biographical label. It determines whom others trust to receive information, give instructions and occupy a role. The documented impersonation cases establish that genuine identifiers can be used by an unauthorized actor, making the identity-to-action relationship the controlling forensic object. [FN 182]

The Florida record contributes specific, connected observations: a private-counsel designation at an institutional address, a declared message-version conflict, a received communication and a later aggregated nonresponse account. These observations are strongest when their exact content, timing and institutional use remain visible. We find that their cumulative value lies in the relationships among the records, not in an assumption that every named professional is fictitious. [FN 183]

54. Trusted infrastructure can carry adversarial authority

We find with high confidence that a recognizable domain, functioning application or accepted credential can carry an adversarial instruction. The 2026 technical record expands the ways in which that can occur, including server-side exploitation, durable mailbox rights and remotely changeable content destinations. Those capabilities increase the importance of the authority expressed by the instruction, not just the apparent legitimacy of the infrastructure carrying it. [FN 184]

The PHP emergency reinforces the report's central conclusion: a legal-sector website is part of a connected professional environment, and unauthorized control can affect the contact directions, account relationships and source records through which authority is recognized. [FN 185]

55. Authority-avatar manipulation is a distinctive cAPTure capability

The investigation establishes a repeatable cAPTure sequence: reconnaissance identifies the target's professional environment; access captures credentials, sessions, website runtime or a trusted relationship; the operator seeds or co-opts a professional persona; the persona enters a communication, firm, portal or proceeding; an institution relies on the asserted authority; and the accepted state persists through records, payments, publications and later decisions.

The October 2026 PHP emergency materially increases the number of paths into this sequence. A vulnerable legal website can supply secrets, context, destination control and persistent administrative access. Those capabilities attach directly to the identity,

communication and intake rails already documented by CNF, ORACLE, RAPS, CCDG and the independent comparator cases.

56. High-confidence conclusions

VERY HIGH CONFIDENCE: Professional avatars are an established operational capability used to enter real firms, transactions, portals and proceedings.

VERY HIGH CONFIDENCE: Genuine professional identifiers and functioning institutional accounts can carry unauthorized authority.

VERY HIGH CONFIDENCE: Electronic adjudication creates a single connected attack surface spanning identity, service, intake, docket state, funds and judicial output.

HIGH CONFIDENCE: Commercial hackers-for-hire can deliver nation-state-grade access, persistence and persona support without nation-state participation.

VERY HIGH CONFIDENCE: The October 2026 PHP emergency expands this capability across legal websites, professional directories, connected services and application secrets.

HIGH CONFIDENCE: The S.D. Fla. placeholder study identifies a population-level pattern of short tenure, minimal merits activity and rapid termination after avatar entry.

VERY HIGH CONFIDENCE: Independent cases establish authority manipulation through settlements, court registries, foreclosure claims, judicial signatures, fake firms, simulated hearings and accepted enterprise identities.

VERY HIGH CONFIDENCE: Effective containment requires technical recovery and institutional record reconciliation as one coordinated operation.

57. Final determination

DF-F.I.R.E. determines with very high confidence that the legal sector is confronting a convergent authority emergency. PHP exploitation, credential theft, valid-account abuse, mailbox persistence, professional-profile manipulation, synthetic media, portal compromise and hackers-for-hire procurement now combine into an affordable and repeatable capability for poisoning the adjudicative environment. The operation succeeds when an institution accepts the represented identity, role or instruction and creates the result the operator was retained to obtain.

The controlling investigative object is the full source-to-consequence chain. The identity presented, credential accepted, communication delivered, role asserted, document filed, routing state created, institutional decision made and persistent record inherited by later actors belong in one reconstruction. That reconstruction supplies the basis for decisive containment and for judicial recognition of cyber-enabled manipulation inside active proceedings.

Endnotes and Sources

- [FN 1] PHP Project. Critical security issues in PHP—upgrade immediately. 21 October 2026. <https://www.php.net/archive/2026.php#2026-10-21-5>. The release identifies CVE-2026-109618 and CVE-2026-109619 and corrected branches 8.2.35, 8.3.36, 8.4.27 and 8.5.12.
- [FN 2] CJ Moses; AWS Security Blog. Amazon threat intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot. 21 October 2026. <https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/>. AWS records exploitation observed on 17 October 2026 and describes broad scanning and exploitation activity.
- [FN 3] O.R.A.C.L.E. Detection Response Team. Authority-Rail Report, Version 31. September 2026. Supplied expert report. The report separates identity, credential, communications, role-and-authority, procedural-state, adjudicative-routing, publication and temporal rails, and maps avatar operations across those connected rails.
- [FN 4] Cyber-N.E.T. Forensics. cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat. September 2026. Supplied threat-assessment report, pp. 4–18, 22–46, 68–106. The assessment identifies authority-rail manipulation, valid-account abuse, portal compromise and professional personas as integrated cAPTure capabilities.
- [FN 5] the Targeted Attorney. Civil Cyber-Infrastructure Disruption Litigation: Historical Development, Operational Durability, Adversarial Adaptation, and the Integrity of Trusted Legal-Technical Control Planes. 10 September 2026. Supplied report. The study reconstructs 35 infrastructure-disruption matters and treats remedy durability, successor infrastructure, identity systems and later-victim access as continuing operational questions.
- [FN 6] Restricted-Access Portal Solutions Unit. Federal CM/ECF, DCN and SMTP Email Relay Expert Report. February 2026. Supplied expert report. RAPS identifies restricted portals as the point where identity, workflow and trust converge, and documents missing filings, altered service lists, assignment irregularities, payment disruption and access failure as direct portal-compromise consequences.
- [FN 7] Cryptographic Cyber-Defense Group. Cryptographic-Counterfeit Expert Analysis Report. 25 February 2026. Supplied expert report. CCDG independently analyzed portal datasets, DNS/MX evidence, e-service metadata, clerk artifacts and documented message-version conflicts, and stated categorical findings based on its multi-modal record.
- [FN 8] Public-interest reporting corpus cited throughout this report. Professional profile links are reproduced in the Special Acknowledgment section. The corpus includes Reuters, POLITICO, WIRED, BleepingComputer, The Hacker News, Forbes, NBC News, SecurityWeek, HackRead, CyberScoop, The Register, TechCrunch, AWS Security Blog and WordPress.org reporting and technical authorship.

- [FN 9] Technical expert and declaration corpus acknowledged in the Special Acknowledgment section, including Microsoft Digital Crimes Unit declarations in Microsoft Corp. v. John Does 1–16, E.D.N.Y. No. 1:23-cv-02447; Google Threat Analysis Group research; Sophos incident-response research; DXC expert materials; Citizen Lab’s Dark Basin investigation; and CNF, ORACLE, RAPS and CCDG reports.
- [FN 10] Cyber-N.E.T. Forensics. Anatomy of the Strategic cAPTure-to-Kill Operation: Integrated e-Forensic Report. 22 October 2025, pp. 69–82 and Tables 1–2, printed pp. 340–347. <https://cyberlawlibrary.org/reports/cyber-n-e-t-forensics-expert-report/>. The report records the Southern District of Florida placeholder-attorney population, document-production indicators, credential-exposure methodology and source-specific statistics used in this edition.
- [FN 11] Administrative Office of the U.S. Courts. Judiciary Strengthens Cybersecurity Protections. 7 August 2025. <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/judiciary-strengthens-cybersecurity-protections>. The Judiciary publicly reported recent escalated cyberattacks of a sophisticated and persistent nature against its case-management system and announced additional protections for sensitive case documents.
- [FN 12] Raphael Satter and reporting colleagues; Reuters. U.S. federal court filing system hit in sweeping cyber breach. August 2025. <https://www.reuters.com/world/us/us-federal-court-filing-system-hit-sweeping-cyber-breach-2025-08-06/>. Reuters reported exposure risks affecting CM/ECF and PACER, including sealed material.
- [FN 13] John Sakellariadis and Josh Gerstein; POLITICO. Federal judiciary confronts major breach of electronic case-management systems. August 2025. <https://www.politico.com/news/2025/08/07/federal-court-filing-system-hacked-00499218>. POLITICO documented the operational consequences and federal response.
- [FN 14] Administrative Office of the U.S. Courts. Judiciary Modernizing Its Case Management System. 22 June 2026. <https://www.uscourts.gov/data-news/judiciary-news/2026/06/22/judiciary-modernizing-its-case-management-system>. The Judiciary states that all new district-court cases are scheduled to move to the modernized platform by the end of 2027, with legacy migration continuing thereafter and full replacement no sooner than 2030.
- [FN 15] MITRE ATT&CK. Impersonation (T1656). Current technique page. <https://attack.mitre.org/techniques/T1656/>. The technique defines adversary impersonation of people, organizations and brands to gain access, trust or information.
- [FN 16] MITRE ATT&CK. Valid Accounts (T1078). Current technique page. <https://attack.mitre.org/techniques/T1078/>. The technique describes adversary use of credentials accepted by the targeted system.
- [FN 17] MITRE ATT&CK. Establish Accounts (T1585), including email and social-media accounts. <https://attack.mitre.org/techniques/T1585/>. The technique defines creation and cultivation of accounts for later operations.

- [FN 18]** National Institute of Standards and Technology. Digital Identity Guidelines: Identity Proofing and Enrollment, NIST SP 800-63A-4. July 2025. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a-4.pdf>. NIST separates identity resolution, evidence validation and verification.
- [FN 19]** Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. The guidance supports integrated collection and analysis across files, applications, networks and operating systems.
- [FN 20]** Cybersecurity and Infrastructure Security Agency. Use Logging on Business Systems. Current guidance. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/use-logging-on-business-systems>. CISA identifies centralized logging as a foundation for detection, investigation and recovery.
- [FN 21]** Printed pp. 69–76, PDF pp. 87–94, describe locating anomalies in filings and correspondence, then correlating them with credential and infrastructure evidence.
- Cyber-N.E.T. Forensics. e-Forensic Integrated Expert Report: Anatomy of the Strategic cAPTure-to-Kill Operation. 22 October 2025. Source: supplied expert report [I25].
- [FN 22]** NIST supports preservation of source material and integration of evidence from files, networks, operating systems and applications.
- Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>
- Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>
- [FN 23]** The original March 17 communication and the March 19 attachment demonstrate an actionable source-to-derivative comparison.
- Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].
- Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].
- [FN 24]** The grievance records illustrate why file identity and effective deadlines must be compared individually.

Preserved source exhibit / identified author on the face of the instrument. September 17 grievance list and October 14 response correspondence. 17 September–14 October 2024. Locator: September 17 list and October 14 message. Source: preserved source copy [E10].

Preserved source exhibit / identified author on the face of the instrument. Branch acknowledgment letter specifying November 12 deadline. 31 October 2024. Locator: deadline and referral language. Source: preserved source copy [E13].

Preserved source exhibit / identified author on the face of the instrument. Branch transfer and response-deadline letter. 31 October 2024. Locator: deadline and branch transfer. Source: preserved source copy [E14].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

[FN 25] NIST SP 800-63A-4 treats identity resolution, evidence validation and verification as distinguishable proofing functions.

David Temoshok Christine Abruzzi Yee Yin Choong James Fenton Ryan Galluzzo Connie LaSalle Naomi Lefkowitz Andrew Regenscheid and Maria Vachino; National Institute of Standards and Technology. Digital Identity Guidelines: Identity Proofing and Enrollment (NIST SP 800-63A-4). 2025-07; final history entry 2025-07-31.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a-4.pdf>

[FN 26] Official profiles supply the exact names, professional identifiers and displayed roles used for record matching.

The Florida Bar; additional profile information may be supplied by the member; The Florida Bar. Member Profile — J.D.W.. Undated live record; accessed 2026-10-24.

<https://www.floridabar.org/mybarprofile/93318>

The Florida Bar; additional profile information may be supplied by the member; The Florida Bar. Member Profile — R.B.. Undated live record; accessed 2026-10-24.

<https://www.floridabar.org/mybarprofile/558028>

The Florida Bar; The Florida Bar. P.S. — Florida Bar member profile. Undated current record; retrieved 2026-10-24.

<https://www.floridabar.org/mybarprofile/559547>

[FN 27] Dated institutional documents establish earlier professional references and later employment or substitution events.

J.D.W., Bar Counsel; P.S., Staff Counsel; The Florida Bar public disciplinary document repository. The Florida Bar v. Fernando Martin Socol — Complaint, File 2018-70,557(11C). 2020-08-24 (certificate of service).

<https://www.floridabar.org/app/plugins/tfb/public/discdoc.php?url=%2F262077%2FFormal-Complaint-201870557-262077.pdf%3Fmime%3Dapplication%252Fpdf>

Preserved source exhibit / identified author on the face of the instrument. Notice of substitution of Bar Counsel R.B. for J.D.W.. 7 January 2025. Locator: notice and signature. Source: preserved source copy [E03].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 28] Printed pp. 71–76 describe breach research, document comparison and domain analysis as connected stages.

Cyber-N.E.T. Forensics. e-Forensic Integrated Expert Report: Anatomy of the Strategic cAPTure-to-Kill Operation. 22 October 2025. Source: supplied expert report [I25].

[FN 29] Internet Archive capture guidance and digital-evidence preservation support separate event, publication, capture and acquisition dates.

Internet Archive Help Center. Using the Wayback Machine. Undated; accessed 24 October 2026.
<https://help.archive.org/help/using-the-wayback-machine/>

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08.
<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

[FN 30] Archive methodology and the dated New York opinions distinguish an older source from a recently observed profile.

Internet Archive Help Center. Using the Wayback Machine. Undated; accessed 24 October 2026.
<https://help.archive.org/help/using-the-wayback-machine/>

New York Appellate Division Second Department; New York State Law Reporting Bureau. Alexandru v Pappas 2009 NY Slip Op 08978. 2009-12-01.
https://www.nycourts.gov/Reporter/3dseries/2009/2009_08978.htm

New York Appellate Division First Department; New York State Law Reporting Bureau. Griffon V LLC v 11 E 36th LLC 2011 NY Slip Op 09090. 2011-12-13.
https://www.nycourts.gov/reporter/3dseries/2011/2011_09090.htm

[FN 31] The user-preserved Attorneys.org image and current Bar profile preserve different employer representations.

Preserved source exhibit / identified author on the face of the instrument. Attorneys.org search-result screenshot for J.D.W.. Capture filename dated 9 December 2024. Locator: visible name, employer, education and admission fields. Source: preserved source copy [E21].

The Florida Bar; additional profile information may be supplied by the member; The Florida Bar. Member Profile — J.D.W.. Undated live record; accessed 2026-

10-24.

<https://www.floridabar.org/mybarprofile/93318>

[FN 32] Archive coverage and source preservation support the reproducible historical comparison method.

Internet Archive Help Center. Using the Wayback Machine. Undated; accessed 24 October 2026.

<https://help.archive.org/help/using-the-wayback-machine/>

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08.

<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

[FN 33] Dated employer, award and corporate publications illustrate separate professional-history and relationship evidence.

The Center for Public Integrity institutional byline; The Center for Public Integrity. Center invests in finance money in politics coverage. 2013-04-03.

<https://publicintegrity.org/politics/center-invests-in-finance-money-in-politics-coverage/>

National Press Foundation institutional byline; National Press Foundation. Miami Herald Wins 2025 Freddie Award. 2025-12-03 updated page.

<https://nationalpress.org/award-story/the-miami-herald-wins-2025-freddie-award/>

McClatchy corporate announcement. McClatchy Acquired by Chatham Asset Management, LLC. 4 September 2020.

<https://www.mcclatchy.com/about/news/mcclatchy-acquired-by-chatham-asset-management-llc/>

[FN 34] NIST's multi-source integration and ORACLE's source-to-consequence model support event correlation and dependency analysis.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

O.R.A.C.L.E. Detection Response Team. Institutional, Private Entity and Individual Credential Laundering and Resulting Authority-Rail Compromises. 7 July 2026. Source: supplied expert report [IOR].

[FN 35] Coordinated personas and fictitious-law-firm operations demonstrate apparent corroboration from related sources.

Joshua Miller, Kyle Eaton, and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 2022-09-13.

<https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

[FN 36] Forensic integration and preservation support the analyst's distinction between observed events, supported mechanisms and attribution.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

[FN 37] NIST preservation guidance and SWGDE online-content acquisition practices support keeping originals and distinguishing later renderings.

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

Scientific Working Group on Digital Evidence; SWGDE. Best Practices for Acquiring Online Content. 2024-03-15 version 1.1. <https://www.swgde.org/documents/published-complete-listing/21-f-001-best-practices-for-acquiring-online-content/>

[FN 38] Kristoffer Tørngaard Pedersen, Lauritz Pepke, Tobias Stærmose, Maria Papaioannou, Gaurav Choudhary and Nicolai Dragoni. Deepfake-Driven Social Engineering: Threats, Mitigation and the PREDICT Framework. Journal of Cybersecurity and Privacy 5(1), 18 (2025). <https://doi.org/10.3390/jcp5010018>. The study examines authoritative personas, synthetic media and communication-channel exploitation.

[FN 39] Kelly Gonzaga, Sérgio Serra, Marco Gomes and Silvestre Malta. AI-Powered Social Engineering: Emerging Attack Vectors and Defensive Strategies. Computers 15(1), 28 (2026). <https://doi.org/10.3390/computers15010028>. The study identifies realism, personalization and automation as core AI-enabled social-engineering capabilities.

[FN 40] Hazem M. Kotb, Tarek Gaber, Salem Aljanabi, Hossam M. Zawbaa and Mohammed Alrahaheh. A Novel Deep Synthesis-Based Insider Intrusion Detection Framework. Scientific Reports 15, Article 217 (2025). <https://doi.org/10.1038/s41598-024-84909-x>. The study evaluates behavioral profiles constructed across login, email, file and web activity.

[FN 41] Irene Amerini and coauthors. Deepfake Media Forensics: Status and Future Challenges. Journal of Imaging 11, 73. 28 February 2025. <https://doi.org/10.3390/jimaging11030073>. The article distinguishes passive detection, active authentication and source attribution.

[FN 42] The joint federal advisory identifies synthetic-media risks to organizations and the use of impersonated leadership or trusted parties.

National Security Agency with FBI and CISA; National Security Agency. NSA, U.S. Federal Agencies Advise on Deepfake Threats. 2023-09-12. <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3523329/nsa-us-federal-agencies-advise-on-deepfake-threats/>

[FN 43] Pedersen and coauthors discuss authority impersonation, organizational practices and the proposed PREDICT framework.

Kristoffer Torngaard Pedersen, Lauritz Pepke, Tobias Stærmose, Maria Papaioannou, Gaurav Choudhary and Nicola Dragoni; Journal of Cybersecurity and Privacy 5, 18. Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments. 27 April 2025. Locator: Sections 3–4, 7–9. <https://doi.org/10.3390/jcp5020018>

[FN 44] The 2026 study identifies realism, personalization and automation and develops the conceptual UM-AISE model.

Kely Gonzaga, Sérgio Serra, Marco Gomes and Silvestre Malta; Computers 15, 128. AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. 17 February 2026. Locator: Sections 2–3. <https://doi.org/10.3390/computers15020128>

[FN 45] Coordinated-persona research supplies a documented communication pattern; the AI study supplies an analytical model for scaling persuasive interactions.

Joshua Miller, Kyle Eaton, and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 2022-09-13. <https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>

Kely Gonzaga, Sérgio Serra, Marco Gomes and Silvestre Malta; Computers 15, 128. AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. 17 February 2026. Locator: Sections 2–3. <https://doi.org/10.3390/computers15020128>

[FN 46] Amerini and coauthors distinguish passive analysis, active authentication and attribution.

Irene Amerini and coauthors; Journal of Imaging 11, 73. Deepfake Media Forensics: Status and Future Challenges. 28 February 2025. Locator: Sections 1, 7–10. <https://doi.org/10.3390/jimaging11030073>

[FN 47] The study addresses compression, uncontrolled environments and the interpretation of forensic detection results.

Irene Amerini and coauthors; Journal of Imaging 11, 73. Deepfake Media Forensics: Status and Future Challenges. 28 February 2025. Locator: Sections 1, 7–10. <https://doi.org/10.3390/jimaging11030073>

[FN 48] NIST identity proofing and media-authentication research support binding a presentation to an actual authorized person.

David Temoshok Christine Abruzzi Yee Yin Choong James Fenton Ryan Galluzzo Connie LaSalle Naomi Lefkowitz Andrew Regenscheid and Maria Vachino; National Institute of Standards and Technology. Digital Identity Guidelines: Identity Proofing and Enrollment (NIST SP 800-63A-4). 2025-07; final history entry 2025-07-31.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a-4.pdf>

Irene Amerini and coauthors; Journal of Imaging 11, 73. Deepfake Media Forensics: Status and Future Challenges. 28 February 2025. Locator: Sections 1, 7–10.

<https://doi.org/10.3390/jimaging11030073>

[FN 49] Kotb and coauthors describe deep feature synthesis, CERT event data and supervised classification of abnormal and generated profiles.

Hazem M. Kotb, Tarek Gaber, Salem AlJanah, Hossam M. Zawbaa and Mohammed Alkhathami; Scientific Reports 15, 207. A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats. 2 January 2025. Locator: Abstract; Materials and methods; Discussion.

<https://www.nature.com/articles/s41598-024-84673-w>

[FN 50] The paper's abstract and methods describe reported performance on the CERT and generated-data experiments.

Hazem M. Kotb, Tarek Gaber, Salem AlJanah, Hossam M. Zawbaa and Mohammed Alkhathami; Scientific Reports 15, 207. A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats. 2 January 2025. Locator: Abstract; Materials and methods; Discussion.

<https://www.nature.com/articles/s41598-024-84673-w>

[FN 51] NIST multi-source integration and the DS-IID relational approach support behavioral rather than purely cosmetic analysis.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Hazem M. Kotb, Tarek Gaber, Salem AlJanah, Hossam M. Zawbaa and Mohammed Alkhathami; Scientific Reports 15, 207. A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats. 2 January 2025. Locator: Abstract; Materials and methods; Discussion.

<https://www.nature.com/articles/s41598-024-84673-w>

[FN 52] The studies support combining organizational verification, media analysis and behavioral context.

Kristoffer Torngaard Pedersen, Lauritz Pepke, Tobias Stærmose, Maria Papaioannou, Gaurav Choudhary and Nicola Dragoni; Journal of Cybersecurity and Privacy 5, 18. Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments. 27 April 2025. Locator:

Sections 3–4, 7–9.
<https://doi.org/10.3390/jcp5020018>

Kely Gonzaga, Sérgio Serra, Marco Gomes and Silvestre Malta; Computers 15, 128. AI-Powered Social Engineering: Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. 17 February 2026. Locator: Sections 2–3. <https://doi.org/10.3390/computers15020128>

Irene Amerini and coauthors; Journal of Imaging 11, 73. Deepfake Media Forensics: Status and Future Challenges. 28 February 2025. Locator: Sections 1, 7–10. <https://doi.org/10.3390/jimaging11030073>

[FN 53] The supplied vendor article and joint advisory describe synthetic identities as a cross-channel investigation problem.

Kaseware; institutional blog. AI-Generated Synthetic Identities: A Rising Threat in Investigations and Security. Undated supplied copy. Locator: PDF pp. 1–3. <https://www.kaseware.com/post/ai-generated-synthetic-identities-a-rising-threat-in-investigations-and-security>

National Security Agency with FBI and CISA; National Security Agency. NSA, U.S. Federal Agencies Advise on Deepfake Threats. 2023-09-12. <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3523329/nsa-us-federal-agencies-advise-on-deepfake-threats/>

[FN 54] The FBI distinguishes fictitious entities, stolen identities, substitute personnel and established professional accounts acquired for use.

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment. 2026-10-13. <https://www.ic3.gov/PSA/2026/PSA261013>

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13. <https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

[FN 55] FBI advisories document false applicants, stolen identity information and substitute or synthetic interview presentations.

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment. 2026-10-13. <https://www.ic3.gov/PSA/2026/PSA261013>

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions. 2022-06-28. <https://www.ic3.gov/PSA/2022/psa220628>

[FN 56] FBI fictitious-firm guidance and the Bermudez incident distinguish the genuine professional from the impersonating actor.

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

Samadhi Jones; The Florida Bar News. Sophisticated fraud scheme impersonates Florida attorney, creates fake court hearing. 2026-08-12.
<https://www.floridabar.org/the-florida-bar-news/sophisticated-fraud-scheme-impersonates-florida-attorney-creates-fake-court-hearing/>

[FN 57] MITRE account establishment and Proofpoint's coordinated-persona investigation support preparation and mutually reinforcing communications.

MITRE ATT&CK; The MITRE Corporation. Establish Accounts: Social Media Accounts (T1585.001). Created 2020-10-01; modified 2026-05-12.
<https://attack.mitre.org/techniques/T1585/001/>

MITRE ATT&CK; The MITRE Corporation. Establish Accounts: Email Accounts (T1585.002). Created 2020-10-01; modified 2026-09-11.
<https://attack.mitre.org/techniques/T1585/002/>

Joshua Miller, Kyle Eaton, and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 2022-09-13.
<https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>

[FN 58] The federal deepfake advisory and media-forensics study define synthetic media and its authentication problem.

National Security Agency with FBI and CISA; National Security Agency. NSA, U.S. Federal Agencies Advise on Deepfake Threats. 2023-09-12.
<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3523329/nsa-us-federal-agencies-advise-on-deepfake-threats/>

Irene Amerini and coauthors; Journal of Imaging 11, 73. Deepfake Media Forensics: Status and Future Challenges. 28 February 2025. Locator: Sections 1, 7–10.
<https://doi.org/10.3390/jimaging11030073>

[FN 59] Printed pp. 69–79, PDF pp. 87–97, define placeholder counsel and describe the source report's anomaly-led methodology.

Cyber-N.E.T. Forensics. e-Forensic Integrated Expert Report: Anatomy of the Strategic cAPTure-to-Kill Operation. 22 October 2025. Source: supplied expert report [I25].

[FN 60] The California enforcement and federal sentencing records establish that stolen attorney identities have been used to represent actual clients and appear in real proceedings.

State Bar of California. State Bar Seizes Practice of Brazen Attorney Impersonator Facing Felony Charges in Los Angeles. 19 November 2021.
<https://www.calbar.ca.gov/news/state-bar-seizes-practice-brazen-attorney-impersonator-facing-felony-charges-los-angeles>

U.S. Attorney's Office, Northern District of California. San Francisco Woman Sentenced To 18 Months For Pandemic Relief Loan Fraud And Impersonating Attorneys. 17 November 2021.

<https://www.justice.gov/usao-ndca/pr/san-francisco-woman-sentenced-18-months-pandemic-relief-loan-fraud-and-impersonating>

[FN 61] Florida's disciplinary roadmap and the January substitution identify the institutional functions of Bar Counsel and the change of assigned counsel.

Brian D. Burgoon; The Florida Bar Journal, vol. 98, no. 3, p. 8. Lawyer Discipline — A Roadmap to Florida's Lawyer Regulation System. May/June 2024. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>

Preserved source exhibit / identified author on the face of the instrument. Notice of substitution of Bar Counsel R.B. for J.D.W.. 7 January 2025. Locator: notice and signature. Source: preserved source copy [E03].

[FN 62] Sections V and XVIII explain the linked identity, credential, communication, role, state and reliance framework.

O.R.A.C.L.E. Detection Response Team. Institutional, Private Entity and Individual Credential Laundering and Resulting Authority-Rail Compromises. 7 July 2026. Source: supplied expert report [IOR].

[FN 63] The lagounov and Findley records show attempts to obtain genuine institutional action through false upstream authority.

U.S. Attorney's Office, Eastern District of California. South Lake Tahoe Man Sentenced to over 2 Years in Prison for Impersonating Federal Officers. 6 February 2025. <https://www.justice.gov/usao-edca/pr/south-lake-tahoe-man-sentenced-over-2-years-prison-impersonating-federal-officers>

U.S. Department of Justice, Office of Public Affairs. Woman Pleads Guilty to Scheme to Defraud Elvis Presley's Family. 25 February 2025. <https://www.justice.gov/opa/pr/woman-pleads-guilty-scheme-defraud-elvis-presleys-family>

[FN 64] MITRE valid accounts and NIST identity guidance explain credentials and the separation between account acceptance and human identity.

MITRE ATT&CK; The MITRE Corporation. Valid Accounts (T1078). Created 2017-05-31; modified 2026-05-12. <https://attack.mitre.org/techniques/T1078/>

David Temoshok Christine Abruzzi Yee Yin Choong James Fenton Ryan Galluzzo Connie LaSalle Naomi Lefkowitz Andrew Regenscheid and Maria Vachino; National Institute of Standards and Technology. Digital Identity Guidelines: Identity Proofing and Enrollment (NIST SP 800-63A-4). 2025-07; final history entry 2025-07-31. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a-4.pdf>

[FN 65] Microsoft and Proofpoint document account-token and server-side permission abuse in functioning enterprise services.

Microsoft Threat Intelligence; Microsoft Security. Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations. 2025-06-30. <https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/>

Greg Lesnewich, Stuart Del Caliz, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly and Proofpoint Threat Research. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. 29 July 2026. <https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit>

[FN 66] FBI false-worker advisories establish that identities can be accepted at enrollment before subsequent account use.

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment. 2026-10-13.

<https://www.ic3.gov/PSA/2026/PSA261013>

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions. 2022-06-28.

<https://www.ic3.gov/PSA/2022/psa220628>

[FN 67] RFC 7208 defines SPF authorization against the envelope sender or HELO identity.

S. Kitterman; Internet Engineering Task Force. RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. April 2014.

<https://www.rfc-editor.org/info/rfc7208/>

[FN 68] RFC 6376 defines signed header/body verification and signing-domain responsibility.

D. Crocker, T. Hansen and M. Kucherawy; Internet Engineering Task Force. RFC 6376: DomainKeys Identified Mail (DKIM) Signatures. September 2011.

<https://www.rfc-editor.org/info/rfc6376/>

[FN 69] RFC 7489 explains alignment of the visible From domain with an authenticated SPF or DKIM domain.

M. Kucherawy and E. Zwicky; Internet Engineering Task Force. RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC). March 2015.

<https://www.rfc-editor.org/info/rfc7489/>

[FN 70] Documented use of valid accounts and mailbox permissions explains how a message can traverse authorized infrastructure while carrying an adversarial act.

MITRE ATT&CK; The MITRE Corporation. Valid Accounts (T1078). Created 2017-05-31; modified 2026-05-12.

<https://attack.mitre.org/techniques/T1078/>

Microsoft Threat Intelligence; Microsoft Security. Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations. 2025-06-30.

<https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/>

Greg Lesnewich, Stuart Del Caliz, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly and Proofpoint Threat Research. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. 29 July 2026.

<https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit>

[FN 71] Forensic source analysis distinguishes message-routing information from editable presentation features.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Scientific Working Group on Digital Evidence; SWGDE. Best Practices for Acquiring Online Content. 2024-03-15 version 1.1.

<https://www.swgde.org/documents/published-complete-listing/21-f-001-best-practices-for-acquiring-online-content/>

[FN 72] The preserved March 14 exhibits include a Florida public-records footer and identify an attached message file.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 73] Document authentication and preservation guidance support careful interpretation of author, producer and rendering metadata.

Scientific Working Group on Digital Evidence; SWGDE. Best Practices for Acquiring Online Content. 2024-03-15 version 1.1.

<https://www.swgde.org/documents/published-complete-listing/21-f-001-best-practices-for-acquiring-online-content/>

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08.

<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

[FN 74] Source-focused authentication supports distinguishing document reuse from independently established unauthorized modification.

Scientific Working Group on Digital Evidence; SWGDE. Best Practices for Acquiring Online Content. 2024-03-15 version 1.1.

<https://www.swgde.org/documents/published-complete-listing/21-f-001-best-practices-for-acquiring-online-content/>

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

[FN 75] OX documents rendered HTML redirects; Proofpoint documents execution through an identified OWA vulnerability.

Moshe Siman Tov Bustan and Vitalii Chepurko; OX Security. Research: ClickFix phishing and npm packages. 25 August 2026. <https://www.ox.security/blog/research-clickfix-phishing-npm-packages/>

Greg Lesnewich, Stuart Del Caliz, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly and Proofpoint Threat Research. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. 29 July 2026. <https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit>

[FN 76] Proofpoint's 2026 OWAReaper investigation documents an email-rendering exploit, server-side changes and persistence.

Greg Lesnewich, Stuart Del Caliz, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly and Proofpoint Threat Research. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. 29 July 2026. <https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit>

[FN 77] Shane Huntley; Google Threat Analysis Group. Countering hack-for-hire groups. 30 June 2022. <https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/>. Google documents targeted account compromise and information collection delivered as a commercial service.

[FN 78] John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis and Ron Deibert; Citizen Lab. Dark Basin: Uncovering a Massive Hack-For-Hire Operation. 9 June 2020. <https://citizenlab.ca/research/dark-basin-uncovering-a-massive-hack-for-hire-operation/>. The investigation links targeting, infrastructure and victim-facing communications across a commercial operation.

[FN 79] Christopher Coy and Microsoft Digital Crimes Unit investigators; Microsoft Corp. v. John Does 1–16, E.D.N.Y. No. 1:23-cv-02447. Public case materials and permanent injunction. https://www.govinfo.gov/content/pkg/USCOURTS-nyed-1_23-cv-02447/pdf/USCOURTS-nyed-1_23-cv-02447-1.pdf. The declarations and orders document cracked Cobalt Strike infrastructure, beaconing, credential theft and court-authorized disruption.

[FN 80] Joshua Miller, Kyle Eaton and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 13 September 2022. <https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>. The research documents coordinated personas that reinforce one another inside one operation.

[FN 81] The Azari sentencing record establishes a paid spearphishing operation and a convicted facilitator connecting clients with hackers.

U.S. Attorney's Office Southern District of New York; U.S. Department of Justice. Israeli Hacker-For-Hire Sentenced To 80 Months In Prison For Involvement In Massive Spearphishing Campaign. 2023-11-16. <https://www.justice.gov/usao-sdny/pr/israeli-hacker-hire-sentenced-80-months-prison-involvement-massive-spearphishing>

[FN 82] Google's primary threat research describes hack-for-hire groups, their targeting and service relationships.

Shane Huntley; Google Threat Analysis Group. Countering hack-for-hire groups. 2022-06-30.

<https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/>

[FN 83] Citizen Lab's Dark Basin investigation documents extensive targeting associated with commercial espionage and civil-society activity.

John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis, and Ron Deibert; Citizen Lab, University of Toronto. Dark Basin: Uncovering a Massive Hack-For-Hire Operation. 2020-06-09.

<https://citizenlab.ca/research/dark-basin-uncovering-a-massive-hack-for-hire-operation/>

[FN 84] The public criminal case and original technical research support the commercial model as an assessment rather than a specific named attribution in the Florida record.

U.S. Attorney's Office Southern District of New York; U.S. Department of Justice. Israeli Hacker-For-Hire Sentenced To 80 Months In Prison For Involvement In Massive Spearphishing Campaign. 2023-11-16.

<https://www.justice.gov/usao-sdny/pr/israeli-hacker-hire-sentenced-80-months-prison-involvement-massive-spearphishing>

Shane Huntley; Google Threat Analysis Group. Countering hack-for-hire groups. 2022-06-30.

<https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/>

[FN 85] The supplied Reuters report records the September 2026 request to designate named firms and the distinction between a requested policy action and a completed designation.

Chris Sanders; Reuters; edited by Edward Tobin. US lawmakers call on American government to blacklist three Indian hack-for-hire firms. 10 September 2026.

Locator: PDF pp. 1–3.

<https://www.reuters.com/legal/government/us-lawmakers-call-american-government-blacklist-three-indian-hack-for-hire-firms-2026-09-10/>

[FN 86] Official and original research supports plausible pretexts, cultivated accounts and coordinated personas.

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

Joshua Miller, Kyle Eaton, and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 2022-09-13.

<https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>

MITRE ATT&CK; The MITRE Corporation. Establish Accounts: Social Media Accounts (T1585.001). Created 2020-10-01; modified 2026-05-12.
<https://attack.mitre.org/techniques/T1585/001/>

[FN 87] The FBI describes acquired professional accounts, substitute interviewers and identity components used to pass verification.

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. North Korean IT Workers Expanding Use of Facilitators, Broadening Recruitment. 2026-10-13.

<https://www.ic3.gov/PSA/2026/PSA261013>

Federal Bureau of Investigation; FBI Internet Crime Complaint Center. Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions. 2022-06-28.

<https://www.ic3.gov/PSA/2022/psa220628>

[FN 88] The sources document multiple apparent actors and mutually reinforcing communications.

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

Joshua Miller, Kyle Eaton, and Alexander Rausch; Proofpoint. TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO. 2022-09-13.

<https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>

[FN 89] The FBI's guidance and Oregon incident establish the role of a familiar account in inducing consequential action.

Federal Bureau of Investigation. Business Email Compromise. Undated; accessed 24 October 2026.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>

Oregon Department of Justice. Oregon DOJ Consumer Hotline Warns of New Scam Impersonating Oregon Attorneys. 28 August 2025.

<https://www.doj.state.or.us/media-home/news-media-releases/oregon-doj-consumer-hotline-warns-of-new-scam-impersonating-oregon-attorneys/>

[FN 90] Lyons describes fraudulent account manufacture and resale, automated registration and controlled purchases; the evidence establishes an account-supply operation.

Jason Lyons, Principal Manager of Investigations, Microsoft Digital Crimes Unit. Declaration of Jason Lyons in Support of Plaintiff Microsoft's Motion for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause. 2023-12-07 filing under seal; first public publication 2023-12-13. Locator: Paragraphs 4, 8–11 and 28–29; printed pages 2–4 and 15–16.

https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/wp-content/uploads/2026/06/St1152_J.-Lyons-Decl.-ISO-Mot.-for-TRO.pdf

[FN 91] MITRE T1585.001 covers social-media accounts and T1585.002 covers email accounts.

MITRE ATT&CK; The MITRE Corporation. Establish Accounts: Social Media Accounts (T1585.001). Created 2020-10-01; modified 2026-05-12.
<https://attack.mitre.org/techniques/T1585/001/>

MITRE ATT&CK; The MITRE Corporation. Establish Accounts: Email Accounts (T1585.002). Created 2020-10-01; modified 2026-09-11.
<https://attack.mitre.org/techniques/T1585/002/>

[FN 92] MITRE T1078 describes adversaries' use of valid accounts to obtain or maintain access.

MITRE ATT&CK; The MITRE Corporation. Valid Accounts (T1078). Created 2017-05-31; modified 2026-05-12.
<https://attack.mitre.org/techniques/T1078/>

[FN 93] MITRE separates spearphishing links from spearphishing through third-party services.

MITRE ATT&CK. Spearphishing Link, T1566.002. Current version; accessed 24 October 2026.
<https://attack.mitre.org/techniques/T1566/002/>

MITRE ATT&CK. Spearphishing via Service, T1566.003. Current version; accessed 24 October 2026.
<https://attack.mitre.org/techniques/T1566/003/>

[FN 94] MITRE T1565.001 concerns modification of stored data to affect integrity and subsequent decisions.

MITRE ATT&CK. Stored Data Manipulation, T1565.001. Modified 13 November 2025.
<https://attack.mitre.org/techniques/T1565/001/>

[FN 95] MITRE T1114.003 describes email-forwarding rules used to collect communications.

MITRE ATT&CK. Email Forwarding Rule, T1114.003. Current version; accessed 24 October 2026.
<https://attack.mitre.org/techniques/T1114/003/>

[FN 96] MITRE T1557 defines adversary-in-the-middle placement within communications.

MITRE ATT&CK. Adversary-in-the-Middle, T1557. Current version; accessed 24 October 2026.
<https://attack.mitre.org/techniques/T1557/>

[FN 97] MITRE's software-supply-chain definition and OX's registry-hosting research distinguish separate mechanisms.

MITRE ATT&CK. Compromise Software Supply Chain, T1195.002. Modified 24 October 2025.
<https://attack.mitre.org/techniques/T1195/002/>

Moshe Siman Tov Bustan and Vitalii Chepurko; OX Security. Research: ClickFix phishing and npm packages. 25 August 2026. <https://www.ox.security/blog/research-clickfix-phishing-npm-packages/>

[FN 98] The sources support linking several techniques through chronology and shared operational control rather than one superficial indicator.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Cyber-N.E.T. Forensics investigative and technical research teams. cAPTure-to-Kill APT: Mapping, Attributing, and Containing an Evolving Threat. September 2026. Source: supplied expert report [ISEP].

[FN 99] Piney Point Homes, LLC v. Burgess, No. 01-23-00834-CV, 2025 WL 3037601 (Tex. App.—Houston [1st Dist.] 30 October 2025). <https://law.justia.com/cases/texas/first-court-of-appeals/2025/01-23-00834-cv.html>. The opinion records infiltration of counsel communications and diversion of approximately \$1.07 million released from a court registry.

[FN 100] Thomas v. Corbyn Restaurant Development Corp., No. 1:19-cv-01948, 2022 WL 168093 (D. Md. 19 January 2022). <https://law.justia.com/cases/federal/district-courts/maryland/mddce/1:2019cv01948/456832/102/>. The court record describes an attacker impersonating plaintiff's counsel and transmitting fraudulent instructions concerning a \$475,000 settlement payment.

[FN 101] Erie Insurance Company v. WAWGD, Inc., No. 1:22-cv-01783, 2024 WL 958936 (D. Md. 6 March 2024). https://www.govinfo.gov/content/pkg/USCOURTS-mdd-1_22-cv-01783/pdf/USCOURTS-mdd-1_22-cv-01783-1.pdf. The record describes an impostor's participation in more than fifty settlement emails and alteration of payment instructions.

[FN 102] Oregon Department of Justice. Oregon DOJ Consumer Hotline Warns of New Scam Impersonating Oregon Attorneys. 28 August 2025. <https://www.doj.state.or.us/media-home/news-media-releases/oregon-doj-consumer-hotline-warns-of-new-scam-impersonating-oregon-attorneys/>. The alert records compromise of attorney and client accounts, cancellation of a verification meeting and diversion exceeding \$700,000.

[FN 103] U.S. Department of Justice, Office of Public Affairs. Woman Pleads Guilty to Scheme to Defraud Elvis Presley's Family. 25 February 2025. <https://www.justice.gov/opa/pr/woman-pleads-guilty-scheme-defraud-elvis-presleys-family>; U.S. Attorney's Office, Western District of Missouri. Woman Sentenced for Scheme to Defraud Elvis Presley's Family. 24 September 2025. <https://www.justice.gov/usao-wdmo/pr/woman-sentenced-scheme-defraud-elvis-presleys-family>. The records establish a fabricated lender, forged documents and false court filings used to claim foreclosure authority over Graceland.

[FN 104] U.S. Attorney's Office, Eastern District of California. South Lake Tahoe Man Sentenced to Over Two Years in Prison for Impersonating Federal Officers. 6

February 2025. <https://www.justice.gov/usao-edca/pr/south-lake-tahoe-man-sentenced-over-2-years-prison-impersonating-federal-officers>. The operation used fictitious and appropriated federal identities and sought judicial signatures for fabricated instruments.

[FN 105] U.S. Attorney's Office, Northern District of California. San Francisco Woman Sentenced to 18 Months for Pandemic Relief Loan Fraud and Impersonating Attorneys. 17 November 2021. <https://www.justice.gov/usao-ndca/pr/san-francisco-woman-sentenced-18-months-pandemic-relief-loan-fraud-and-impersonating>. The record establishes use of real attorneys' identities and license numbers, payment of Bar dues, redirected licensing mail and courtroom representation.

[FN 106] U.S. Attorney's Office, Southern District of New York. Florida Man Pleads Guilty to Operating Fraudulent Law Firm and Using the Stolen Identity of a Retired Attorney. 20 December 2017. <https://www.justice.gov/usao-sdny/pr/florida-man-pleads-guilty-operating-fraudulent-law-firm-and-using-stolen-identity>. The scheme created a multi-office law-firm presentation, fictitious attorneys and staff, and legal filings under an appropriated professional identity.

[FN 107] The Florida Bar News. AI-generated filing uses attorney Matthew Weidner's name and Bar number in a matter he did not handle. August 2024. <https://www.floridabar.org/the-florida-bar-news/ai-generated-filing-cites-fake-cases-lists-real-lawyer-who-had-no-involvement/>. The event documents a real lawyer's professional identifiers inserted into a court filing without his authorization.

[FN 108] Samadhi Jones; The Florida Bar News. Sophisticated fraud scheme impersonates Florida attorney, creates fake court hearing. 12 August 2026. <https://www.floridabar.org/the-florida-bar-news/sophisticated-fraud-scheme-impersonates-florida-attorney-creates-fake-court-hearing/>. The scheme used a genuine attorney identity and Bar number, a simulated hearing, purported judicial and police authority, and produced a real regulatory complaint.

[FN 109] U.S. Attorney's Office, Eastern District of Missouri. St. Louis County Man Sentenced for Using Forged Judicial Order in Fraud Scheme. 2024. <https://www.justice.gov/usao-edmo/pr/st-louis-county-man-sentenced-using-forged-judicial-order-fraud-scheme>. The record documents use of a chief judge's identity, signature and court seal in a fabricated order connected to property and foreclosure representations.

[FN 110] U.S. Attorney's Office, Eastern District of Missouri. St. Louis Lawyer Sentenced for Defrauding Clients with Fake Court Orders. 2023. <https://www.justice.gov/usao-edmo/pr/st-louis-lawyer-sentenced-defrauding-clients-fake-court-orders>. The matter documents fabricated court orders, forged judicial signatures and manufactured communications used across approximately thirty client matters.

[FN 111] U.S. Attorney's Office, Eastern District of Missouri. Former Lawyer Sentenced for Defrauding Clients with Fake Legal Documents. 2022. <https://www.justice.gov/usao-edmo/pr/former-lawyer-sentenced-defrauding-clients-fake-legal-documents>. The record documents sham court materials, false procedural histories and a fabricated settlement used to maintain client reliance.

- [FN 112]** Federal Bureau of Investigation. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 13 August 2025. <https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>. The FBI documents false firms, professional-looking websites, attorney impersonation, intake and payment exploitation.
- [FN 113]** Federal Bureau of Investigation, Internet Crime Complaint Center. Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions. 28 June 2022. <https://www.ic3.gov/PSA/2022/PSA220628>; U.S. Department of Justice. Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Nationwide Actions. 30 June 2025. <https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through>; Microsoft Threat Intelligence. Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations. 30 June 2025. <https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/>. These sources document stolen identities, substitute interviewers, front companies, accepted enterprise accounts and persistent access through legitimate organizational systems.
- [FN 114]** Preserved expert work product concerning G.S. and an international law firm. Supplied source set. The source record examines historical judicial references, later account representations, professional-platform activity and event-specific authority use within a large, geographically distributed organization.
- [FN 115]** The September 17 message lists eleven response-required matters and distinguishes matters for which no further response was then requested.
- Preserved source exhibit / identified author on the face of the instrument. September 17 grievance list and October 14 response correspondence. 17 September–14 October 2024. Locator: September 17 list and October 14 message. Source: preserved source copy [E10].
- [FN 116]** The individual letters identify separate September 25 and October 21 deadlines.
- Preserved source exhibit / identified author on the face of the instrument. File-specific inquiry letter, grievance 2025-70,132. 10 September 2024. Locator: response deadline September 25. Source: preserved source copy [E11].
- Preserved source exhibit / identified author on the face of the instrument. File-specific inquiry letter, grievance 2025-70,140. 9 October 2024. Locator: response deadline October 21. Source: preserved source copy [E12].
- [FN 117]** The October 31 letters set November 12 response deadlines and describe referral following nonresponse.
- Preserved source exhibit / identified author on the face of the instrument. Branch acknowledgment letter specifying November 12 deadline. 31 October 2024. Locator: deadline and referral language. Source: preserved source copy [E13].

Preserved source exhibit / identified author on the face of the instrument. Branch transfer and response-deadline letter. 31 October 2024. Locator: deadline and branch transfer. Source: preserved source copy [E14].

[FN 118] The October 14 message and October 15 acknowledgment establish transmission and express recognition of receipt.

Preserved source exhibit / identified author on the face of the instrument. September 17 grievance list and October 14 response correspondence. 17 September–14 October 2024. Locator: September 17 list and October 14 message. Source: preserved source copy [E10].

Preserved source exhibit / identified author on the face of the instrument. Christine Mitchell acknowledgment of October 14 correspondence. 15 October 2024. Locator: 9:38 a.m. acknowledgment. Source: preserved source copy [E09].

[FN 119] The acknowledgment and later petition support a distinction between receipt and the later characterization of response sufficiency.

Preserved source exhibit / identified author on the face of the instrument. Christine Mitchell acknowledgment of October 14 correspondence. 15 October 2024. Locator: 9:38 a.m. acknowledgment. Source: preserved source copy [E09].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

[FN 120] The November 25 petition's aggregation is read against the later individual deadlines.

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

Preserved source exhibit / identified author on the face of the instrument. Branch acknowledgment letter specifying November 12 deadline. 31 October 2024. Locator: deadline and referral language. Source: preserved source copy [E13].

Preserved source exhibit / identified author on the face of the instrument. Branch transfer and response-deadline letter. 31 October 2024. Locator: deadline and branch transfer. Source: preserved source copy [E14].

[FN 121] The contemporaneous May/June 2024 Bar Journal roadmap expressly states that Bar Counsel may serve as investigating member.

Brian D. Burgoon; The Florida Bar Journal, vol. 98, no. 3, p. 8. Lawyer Discipline — A Roadmap to Florida's Lawyer Regulation System. May/June 2024. <https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>

[FN 122] The roadmap and Rules 3-3.3 and 3-7.4 distinguish committee composition, investigation and decision-making roles.

Brian D. Burgoon; The Florida Bar Journal, vol. 98, no. 3, p. 8. Lawyer Discipline — A Roadmap to Florida's Lawyer Regulation System. May/June 2024.

<https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>

Supreme Court of Florida; official Florida Bar compilation. Rules Regulating The Florida Bar. 1 October 2026 edition.

https://www-media.floridabar.org/uploads/2026/10/2027_04-OCT-RRTFB-10-1-2026.pdf

[FN 123] The corrected response and petition preserve competing descriptions of committee authority and referral chronology.

Preserved source exhibit / identified author on the face of the instrument. Corrected response to petition for order to show cause. 30 December 2024. Locator: grievance chronology and reported conflict/recusal communications. Source: preserved source copy [E24].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

[FN 124] The Campbell petition's pp. 5–6 contain conflicting counsel/contact fields, providing a separate document-level comparator.

William Wonil Chung, Bar Counsel; The Florida Bar public disciplinary document repository. The Florida Bar v. Debbie Rachelle Campbell — Petition for Contempt and Order to Show Cause, File 2025-70,152(11G)(OSC). 2024-10-30 (certificate of service).

<https://www.floridabar.org/app/plugins/tfb/public/discdoc.php?url=%2F3094554%2FPetition-for-Contempt-and-Order-to-Show-Cause-202570152-3094554.pdf%3Fmime%3Dapplication%252Fpdf>

[FN 125] The primary sequence supports the precise finding of chronology and representation divergence.

Preserved source exhibit / identified author on the face of the instrument. September 17 grievance list and October 14 response correspondence. 17 September–14 October 2024. Locator: September 17 list and October 14 message. Source: preserved source copy [E10].

Preserved source exhibit / identified author on the face of the instrument. Christine Mitchell acknowledgment of October 14 correspondence. 15 October 2024. Locator: 9:38 a.m. acknowledgment. Source: preserved source copy [E09].

Preserved source exhibit / identified author on the face of the instrument. Branch acknowledgment letter specifying November 12 deadline. 31 October 2024. Locator: deadline and referral language. Source: preserved source copy [E13].

Preserved source exhibit / identified author on the face of the instrument. Branch transfer and response-deadline letter. 31 October 2024. Locator: deadline and branch transfer. Source: preserved source copy [E14].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

[FN 126] The March motion and composite preserve the purported proposal, acceptance and subsequent repudiation as a linked sequence.

Preserved source exhibit / identified author on the face of the instrument. Motion to approve stipulation for dismissal without prejudice. 18 March 2025. Locator: paragraphs 38–51 and reproduced correspondence. Source: preserved source copy [E05].

Preserved source exhibit / identified author on the face of the instrument. Composite March correspondence and portal notice. 7–17 March 2025. Locator: Walker role/address messages and March 7 service notice. Source: preserved source copy [E22].

[FN 127] The March 19 motion and June affidavits explicitly repudiate the message and identify the misspelling as part of their position.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 128] The filings document the disputed terms and the targeted attorney's reliance and disclosure.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. Motion to approve stipulation for dismissal without prejudice. 18 March 2025. Locator: paragraphs 38–51 and reproduced correspondence. Source: preserved source copy [E05].

[FN 129] The composite and attached March 14 message show the move from counsel attribution to investigator-delivered denial.

Preserved source exhibit / identified author on the face of the instrument. Composite March correspondence and portal notice. 7–17 March 2025. Locator: Walker role/address messages and March 7 service notice. Source: preserved source copy [E22].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

[FN 130] Staff Investigator J.B. paragraphs 4–12 and Berman paragraphs 8–15 identify their sworn account of the referral and denial.

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 131] The 10:16 a.m. message expressly distinguishes the circulated version from the version the sender says he sent.

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

[FN 132] The same message simultaneously disputes the version and reasserts the no-dismissal position.

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

[FN 133] The March 18 motion reproduces and discusses the changed-email statement before the March 19 response.

Preserved source exhibit / identified author on the face of the instrument. Motion to approve stipulation for dismissal without prejudice. 18 March 2025. Locator: paragraphs 38–51 and reproduced correspondence. Source: preserved source copy [E05].

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

[FN 134] The March 19 motion, especially pp. 2–3 and the attachment at p. 10, expressly discusses and reproduces Staff Investigator J.B.'s communications.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

[FN 135] The March pleading and June affidavit package establish a repeated institutional use of the disputed-message episode.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 136] The March 20 motion requests an in-person conference; the March 19 communication declines further meetings.

Preserved source exhibit / identified author on the face of the instrument. Motion for in-person meeting and conference. 20 March 2025. Locator: pp. 1–5. Source: preserved source copy [E06].

Preserved source exhibit / identified author on the face of the instrument. Email declining further in-person meetings. 19 March 2025. Locator: 5:10 p.m. message and copied parties. Source: preserved source copy [E23].

[FN 137] FBI BEC guidance supports independent verification; the motion identifies the particular face-to-face comparison requested.

Federal Bureau of Investigation. Business Email Compromise. Undated; accessed 24 October 2026.
<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>

Preserved source exhibit / identified author on the face of the instrument. Motion for in-person meeting and conference. 20 March 2025. Locator: pp. 1–5. Source: preserved source copy [E06].

[FN 138] The combined primary sequence supports the finding about conversion of a message dispute into formal institutional evidence.

Preserved source exhibit / identified author on the face of the instrument. Notice of substitution of Bar Counsel R.B. for J.D.W.. 7 January 2025. Locator: notice and signature. Source: preserved source copy [E03].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. Motion for in-person meeting and conference. 20 March 2025. Locator: pp. 1–5. Source: preserved source copy [E06].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 139] The reproduced email on p. 14 identifies its sender as Sonja Chaves, chief operating officer, and records the firm's receipt and counsel-routing instruction.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

[FN 140] The same email identifies P.S. at her Florida Bar address as the firm's counsel.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

[FN 141] The March 7 signature and certificate identify P.S. as Staff Counsel for The Florida Bar.

Preserved source exhibit / identified author on the face of the instrument. Bar response to motion for order to show cause, signed by P.S.. 7 March 2025. Locator: pp. 1–6; signature and certificate p. 6. Source: preserved source copy [E02].

[FN 142] Official profile and dated institutional publications establish a longstanding professional identity and Bar role history.

The Florida Bar; The Florida Bar. P.S. — Florida Bar member profile. Undated current record; retrieved 2026-10-24.
<https://www.floridabar.org/mybarprofile/559547>

Admin institutional byline; Florida Institute of Technology. College of Business Ethics Conference. 2005-07-13 publication; conference 2005-04-19.
<https://news.fit.edu/business/college-of-business-ethics-conference/>

Christine Bilbrey and Karla Eckardt; guest P.S.; LegalFuel and The Florida Bar. The Lawyer Discipline Process from Start to Finish. 2022-02-28.
<https://www.legalfuel.com/the-lawyer-discipline-process-from-start-to-finish/>

[FN 143] Rule 4-1.7 supplies the conflict framework; the primary documents supply the two represented capacities rather than an independently verified retainer.

Supreme Court of Florida; official Florida Bar compilation. Rules Regulating The Florida Bar. 1 October 2026 edition.
https://www-media.floridabar.org/uploads/2026/10/2027_04-OCT-RRTFB-10-1-2026.pdf

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Preserved source exhibit / identified author on the face of the instrument. Bar response to motion for order to show cause, signed by P.S.. 7 March 2025. Locator: pp. 1–6; signature and certificate p. 6. Source: preserved source copy [E02].

[FN 144] The source message redirects communications and the FBI's BEC guidance explains why changed consequential instructions require an independent identity relationship.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Federal Bureau of Investigation. Business Email Compromise. Undated; accessed 24 October 2026.
<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>

[FN 145] The February filing and prior December protective filing show the issue entering an existing communication-security chronology.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Preserved source exhibit / identified author on the face of the instrument. Protective and confidentiality motion. 27 December 2024. Locator: notice of communication-security concerns and service. Source: preserved source copy [E16].

[FN 146] The finding rests on exact representations on the source documents, not an invented employment prohibition.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Preserved source exhibit / identified author on the face of the instrument. Bar response to motion for order to show cause, signed by P.S.. 7 March 2025. Locator: pp. 1–6; signature and certificate p. 6. Source: preserved source copy [E02].

[FN 147] The 2022 Haritan petition includes a roster naming Nakia Ruffin as chair and R.W. as vice chair.

Jessica Brito, Bar Counsel; attached finding signed for Committee F by Vice Chair Richard J. Weiss; The Florida Bar public disciplinary document repository. The Florida Bar v. Chelsea Elizabeth Haritan — Petition for Contempt and Order to Show Cause, with 17F roster. 2022-09-09; attached roster letter 2022-07-28 and committee consideration 2022-08-10.
<https://www.floridabar.org/app/plugins/tfb/public/discdoc.php?url=%2F1937308%2FPetition-for-Contempt-and-Order-to-Show-Cause-202350104-1937308.pdf%3Fmime%3Dapplication%252Fpdf>

[FN 148] The current roster identifies Gyires, and the firm announcement is dated July 22, 2025; those dates define their chronological reach.

The Florida Bar; The Florida Bar. Seventeenth Circuit Grievance Committee 'F' — current roster. Undated live roster; accessed 2026-10-24.
<https://www.floridabar.org/about/cmtes/cmtes-gr/cmte-gr056/>

Lewis Brisbois Bisgaard & Smith LLP; no individual byline; Lewis Brisbois. Marcela Gyires Selected as Chair of Florida Bar's Seventeenth Judicial Circuit Grievance Committee. 2025-07-22.
<https://lewisbrisbois.com/newsroom/marcela-gyires-selected-as-chair-of-florida-bars-seventeenth-judicial-circuit-grievance-committee>

[FN 149] The corrected response preserves the October chair representation, and the October 17 notice supplies an independent firm-client representation.

Preserved source exhibit / identified author on the face of the instrument. Corrected response to petition for order to show cause. 30 December 2024. Locator: grievance chronology and reported conflict/recusal communications. Source: preserved source copy [E24].

Preserved source exhibit / identified author on the face of the instrument. Weiss Serota demand notice identifying representation of Regus Management. 17 October 2024. Locator: letterhead, client designation and signature. Source: preserved source copy [E19].

[FN 150] The corrected response reports a conflict-related removal statement; the disciplinary framework provides the relevant role context.

Preserved source exhibit / identified author on the face of the instrument. Corrected response to petition for order to show cause. 30 December 2024. Locator: grievance chronology and reported conflict/recusal communications. Source: preserved source copy [E24].

Brian D. Burgoon; The Florida Bar Journal, vol. 98, no. 3, p. 8. Lawyer Discipline — A Roadmap to Florida's Lawyer Regulation System. May/June 2024.
<https://www.floridabar.org/the-florida-bar-journal/lawyer-discipline-a-roadmap-to-floridas-lawyer-regulation-system/>

Supreme Court of Florida; official Florida Bar compilation. Rules Regulating The Florida Bar. 1 October 2026 edition.
https://www-media.floridabar.org/uploads/2026/10/2027_04-OCT-RRTFB-10-1-2026.pdf

[FN 151] The November petition and June composite show differing committee suffixes attached to identified grievance matters.

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 152] Sections III–VI analyze complaint identity, committee identity and source-to-consequence transitions; applied here without quoting the supplement.

O.R.A.C.L.E. Detection Response Team. Supplemental Authority-Rail Convergence Report. 24 September 2026. Source: supplied expert report [ISUP].

[FN 153] The source sequence supports separate analysis of the original contempt proceeding and the later emergency-suspension package.

Preserved source exhibit / identified author on the face of the instrument. September 17 grievance list and October 14 response correspondence. 17 September–14 October 2024. Locator: September 17 list and October 14 message. Source: preserved source copy [E10].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 154] The combined exhibits support the cumulative authority sequence without deciding an unverified historical chair date.

Preserved source exhibit / identified author on the face of the instrument. Weiss Serota demand notice identifying representation of Regus Management. 17 October 2024. Locator: letterhead, client designation and signature. Source: preserved source copy [E19].

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Preserved source exhibit / identified author on the face of the instrument. Bar response to motion for order to show cause, signed by P.S.. 7 March 2025. Locator: pp. 1–6; signature and certificate p. 6. Source: preserved source copy [E02].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 155] Walker introduces the investigator; the June affidavit states the instruction from counsel.

Preserved source exhibit / identified author on the face of the instrument. Composite March correspondence and portal notice. 7–17 March 2025. Locator: Walker role/address messages and March 7 service notice. Source: preserved source copy [E22].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 156] The March communications carry both a substantive institutional position and a statement about changed content.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

[FN 157] The March 18 motion precedes the March 19 institutional filing and reproduces the version dispute.

Preserved source exhibit / identified author on the face of the instrument. Motion to approve stipulation for dismissal without prejudice. 18 March 2025. Locator: paragraphs 38–51 and reproduced correspondence. Source: preserved source copy [E05].

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

[FN 158] The March motion includes the March 17 attachment, while the June affidavit narrates the denial and references the March 14 message.

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed

18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 159] Staff Investigator J.B. paragraphs 4–18 separate his reported conversation with Berman from statements attributed to FBI agents.

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 160] Sections XII–XIII compare the investigator's summary with direct communications and describe the institutional use of sworn summaries.

O.R.A.C.L.E. Detection Response Team. Institutional, Private Entity and Individual Credential Laundering and Resulting Authority-Rail Compromises. 7 July 2026. Source: supplied expert report [IOR].

[FN 161] The affidavits and motion show how a disputed communication became a stated predicate in later institutional requests.

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

[FN 162] The documents establish the version dispute and later reliance, supporting the bounded high-confidence event finding.

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 163] The original service receipts display submission fields and describe later availability following clerk acceptance.

Preserved source exhibit / identified author on the face of the instrument. Original electronic-service notice, filing 213069218. 17 December 2024. Locator: pp. 1–2; case fields and selected recipients. Source: preserved source copy [E17].

Preserved source exhibit / identified author on the face of the instrument. E-service notice for emergency petition, filing 225491716. 18 June 2025. Locator: NEW CASE; 08:20:04 a.m.; filer and service fields. Source: preserved source copy [E18].

[FN 164] The December 17 receipt records filing 213069218, the Supreme Court, UNKNOWN case fields and selected recipients.

Preserved source exhibit / identified author on the face of the instrument. Original electronic-service notice, filing 213069218. 17 December 2024. Locator: pp. 1–2; case fields and selected recipients. Source: preserved source copy [E17].

[FN 165] The June 18 notice records filing 225491716, Savitz as filer, NEW CASE and the exact submission timestamp.

Preserved source exhibit / identified author on the face of the instrument. E-service notice for emergency petition, filing 225491716. 18 June 2025. Locator: NEW CASE; 08:20:04 a.m.; filer and service fields. Source: preserved source copy [E18].

[FN 166] Section VII explains the June 18 transition from the portal's NEW CASE state to the C-Track permanent case number.

O.R.A.C.L.E. Detection Response Team. Supplemental Authority-Rail Convergence Report. 24 September 2026. Source: supplied expert report [ISUP].

[FN 167] The original notices distinguish selected and unselected service populations and preserve displayed recipient names and addresses.

Preserved source exhibit / identified author on the face of the instrument. Original electronic-service notice, filing 213069218. 17 December 2024. Locator: pp. 1–2; case fields and selected recipients. Source: preserved source copy [E17].

Preserved source exhibit / identified author on the face of the instrument. Composite March correspondence and portal notice. 7–17 March 2025. Locator: Walker role/address messages and March 7 service notice. Source: preserved source copy [E22].

[FN 168] The March 7 portal notice and signed response connect transaction metadata with the particular filed document.

Preserved source exhibit / identified author on the face of the instrument. Composite March correspondence and portal notice. 7–17 March 2025. Locator: Walker role/address messages and March 7 service notice. Source: preserved source copy [E22].

Preserved source exhibit / identified author on the face of the instrument. Bar response to motion for order to show cause, signed by P.S.. 7 March 2025. Locator: pp. 1–6; signature and certificate p. 6. Source: preserved source copy [E02].

[FN 169] Valid-account techniques and the federal judiciary's acknowledged attacks establish why a genuine portal event can still warrant event-level scrutiny.

MITRE ATT&CK; The MITRE Corporation. Valid Accounts (T1078). Created 2017-05-31; modified 2026-05-12.

<https://attack.mitre.org/techniques/T1078/>

Administrative Office of the United States Courts. Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System. 7 August 2025.

<https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>

[FN 170] Sections 8–9 and the source-specific applications distinguish authenticated transport from the source and consequence of a particular notice.

0-V.E.R. INT-DFIR Team and credited contributors. PHP2Shell Cyber Emergency and Implications to Existing Legal-Sector Vulnerabilities. 22 October 2026. Source: supplied expert report [IPHP].

[FN 171] The email standards support the proper interpretation of institutional domains and contracted delivery infrastructure.

S. Kitterman; Internet Engineering Task Force. RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. April 2014.

<https://www.rfc-editor.org/info/rfc7208/>

D. Crocker, T. Hansen and M. Kucherawy; Internet Engineering Task Force. RFC 6376: DomainKeys Identified Mail (DKIM) Signatures. September 2011.

<https://www.rfc-editor.org/info/rfc6376/>

M. Kucherawy and E. Zwicky; Internet Engineering Task Force. RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC). March 2015.

<https://www.rfc-editor.org/info/rfc7489/>

[FN 172] Printed pp. 160–183 describe counterfeit-notice and grievance-email studies within the integrated investigation.

Cyber-N.E.T. Forensics. e-Forensic Integrated Expert Report: Anatomy of the Strategic cAPTure-to-Kill Operation. 22 October 2025. Source: supplied expert report [I25].

[FN 173] The June filing receipt and affidavit package identify the actual submitted object and its institutional use.

Preserved source exhibit / identified author on the face of the instrument. E-service notice for emergency petition, filing 225491716. 18 June 2025. Locator: NEW CASE; 08:20:04 a.m.; filer and service fields. Source: preserved source copy [E18].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 174] The supplement's treatment of NEW CASE as a positive control supports separating normal intake fields from other challenged message attributes.

O.R.A.C.L.E. Detection Response Team. Supplemental Authority-Rail Convergence Report. 24 September 2026. Source: supplied expert report [ISUP].

[FN 175] Government and Bar warnings document official-looking communications using false institutional authority and varied contact pathways.

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

Mark D. Killian; The Florida Bar News. Bar warns of fraudulent emails spoofing senior Bar staff. 2025-12-02.

<https://www.floridabar.org/the-florida-bar-news/bar-warns-of-fraudulent-emails-spoofing-senior-bar-staff/>

Mark D. Killian; The Florida Bar News. Florida Bar warns members of ongoing phishing scam impersonating executive director. 2025-06-23.

<https://www.floridabar.org/the-florida-bar-news/florida-bar-warns-members-of-ongoing-phishing-scam-impersonating-executive-director/>

[FN 176] Forensic source preservation supports analyzing the complete original recipient and message structure.

Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; NIST. Guide to Integrating Forensic Techniques into Incident Response, SP 800-86. August 2006.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Barbara Guttman; Douglas R. White; Tracy Walraven (authors printed in the report); National Institute of Standards and Technology. Digital Evidence Preservation: Considerations for Evidence Handlers. 2022-09; publication page dated 2022-09-08.

<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>

[FN 177] FBI guidance explains false recovery and institutional-pretext messages that draw victims into further exchanges.

Federal Bureau of Investigation. Business Email Compromise. Undated; accessed 24 October 2026.

<https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

[FN 178] Authentication practices and the supplied competing-message exhibits show why attachment identity matters separately from message appearance.

Scientific Working Group on Digital Evidence; SWGDE. Best Practices for Acquiring Online Content. 2024-03-15 version 1.1. <https://www.swgde.org/documents/published-complete-listing/21-f-001-best-practices-for-acquiring-online-content/>

Preserved source exhibit / identified author on the face of the instrument. Motion to strike proposed stipulation, with correspondence exhibits. 19 March 2025. Locator: pp. 2–6 and 10–11; filing 219144400. Source: preserved source copy [E04].

Preserved source exhibit / identified author on the face of the instrument. June emergency-petition composite: affidavits of Staff Investigator J.B. and R.B.. Filed 18 June 2025. Locator: Staff Investigator J.B. pp. 1–4; correspondence pp. 101–102; Berman pp. 103–104. Source: preserved source copy [E08].

[FN 179] Stored-data manipulation and remotely changeable redirect research establish the distinction between a stable reference and changing content.

MITRE ATT&CK. Stored Data Manipulation, T1565.001. Modified 13 November 2025.

<https://attack.mitre.org/techniques/T1565/001/>

Moshe Siman Tov Bustan and Vitalii Chepurko; OX Security. Research: ClickFix phishing and npm packages. 25 August 2026. <https://www.ox.security/blog/research-clickfix-phishing-npm-packages/>

[FN 180] Sections V, XIV and XVIII describe the transition from document and notice to accepted procedural state.

O.R.A.C.L.E. Detection Response Team. Institutional, Private Entity and Individual Credential Laundering and Resulting Authority-Rail Compromises. 7 July 2026. Source: supplied expert report [IOR].

[FN 181] Federal Bureau of Investigation. Business Email Compromise. Current guidance. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>. The FBI directs independent verification of consequential payment and account-change instructions.

[FN 182] The sources establish that genuine identifiers can be appropriated and that identity proofing is distinct from presentation.

Federal Bureau of Investigation; FBI. Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds. 2025-08-13.

<https://www.fbi.gov/investigate/cyber/alerts/2025/fictitious-law-firms-targeting-cryptocurrency-scam-victims-combine-multiple-exploitation-tactics-while-offering-to-recover-funds>

David Temoshok Christine Abruzzi Yee Yin Choong James Fenton Ryan Galluzzo Connie LaSalle Naomi Lefkowitz Andrew Regenscheid and Maria Vachino; National Institute of Standards and Technology. Digital Identity Guidelines: Identity Proofing and Enrollment (NIST SP 800-63A-4). 2025-07; final history entry 2025-07-31.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a-4.pdf>

U.S. Attorney's Office, Northern District of California. San Francisco Woman Sentenced To 18 Months For Pandemic Relief Loan Fraud And Impersonating Attorneys. 17 November 2021.
<https://www.justice.gov/usao-ndca/pr/san-francisco-woman-sentenced-18-months-pandemic-relief-loan-fraud-and-impersonating>

[FN 183] The principal field exhibits directly support the authority, version and chronology findings retained in this edition.

Preserved source exhibit / identified author on the face of the instrument. Email attributed to Sonja Chaves, Weiss Serota chief operating officer, reproduced in motion for order to show cause. 26–27 February 2025. Locator: p. 14, email and paragraphs 26–27. Source: preserved source copy [E01].

Preserved source exhibit / identified author on the face of the instrument. Contact Request email attributed to Staff Investigator J.B. and same-day forwarding response. 17 March 2025. Locator: 10:16 a.m. email; 10:55 a.m. forwarding response. Source: preserved source copy [E07].

Preserved source exhibit / identified author on the face of the instrument. Christine Mitchell acknowledgment of October 14 correspondence. 15 October 2024. Locator: 9:38 a.m. acknowledgment. Source: preserved source copy [E09].

Preserved source exhibit / identified author on the face of the instrument. Petition for order to show cause and contempt. 25 November 2024. Locator: thirteen-inquiry chronology and service certificate. Source: preserved source copy [E15].

[FN 184] The technical sources establish accepted accounts, mailbox persistence, trusted-hosted content and server-exploitation exposure.

MITRE ATT&CK; The MITRE Corporation. Valid Accounts (T1078). Created 2017-05-31; modified 2026-05-12.
<https://attack.mitre.org/techniques/T1078/>

Greg Lesnewich, Stuart Del Caliz, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly and Proofpoint Threat Research. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. 29 July 2026.
<https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit>

Moshe Siman Tov Bustan and Vitalii Chepurko; OX Security. Research: ClickFix phishing and npm packages. 25 August 2026.
<https://www.ox.security/blog/research-clickfix-phishing-npm-packages/>

PHP Project. PHP 2026 release archive: Critical security issues in PHP — upgrade immediately. 21 October 2026.
<https://www.php.net/archive/2026.php#2026-10-21-5>

[FN 185] The emergency assessment connects software exposure with professional communication and record consequences.

0-V.E.R. INT-DFIR Team and credited contributors. PHP2Shell Cyber Emergency and Implications to Existing Legal-Sector Vulnerabilities. 22 October 2026. Source: supplied expert report [IPHP].