PUBLIC RELEASE — REDACTED VERSION · Company names replaced with sector classifications. Legal arguments and data are unaltered. · SEC Whistleblower No. 17684-273-411-436

Support this investigation: gofundme.com/f/albert-lane-forensic-audit

Digital Fraud Audit Series · Introduction

The Forensic Method: *Historic Timelines and Parallel Anti-Adversarial Audits*

Public Release — Company names replaced with sector classifications to protect brand identity

SEC Whistleblower Filing No. 17684-273-411-436 · January 14, 2026

Albert Lane, Forensic Audit Consultant

LinkedIn | GoFundMe

Purpose of This Document

This introduction establishes the forensic methodology underlying the entire Digital Fraud Audit series. It answers a single foundational question: *why should a 19th-century legal framework — the Black Codes, the Contract Labor Laws, and the Freedmen's Bureau statutes — serve as an analytical template for auditing 21st-century algorithmic governance?*

The answer is that the mechanisms are not analogous. They are structurally identical. The

same three-step logic of immobilization, extraction, and legitimation operates in both eras. The tools have changed — plantations became platforms, sheriffs became algorithms, vagrancy laws became Terms of Service — but the architecture of control is the same source code, recompiled.

This document defines the forensic methodology used throughout the audit series, explains the legal theories of constructive trust and the doctrine of relating back that underpin the compensation claims, introduces the adversarial audit framework that makes detection possible, and documents the specific digital tools — MACB timestamp analysis, LLM forensics, and the Affidavit of the Machine — that constitute the technical chain of custody.

✦ ✦ ✦

Section 1

The Core Thesis: Potemkin History and the Anchor of Logic

In modern algorithmic governance, the greatest threat to accountability is not the fraudulent act itself — it is the erasure of the evidence that the act occurred. This audit series calls that erasure Potemkin History.

Potemkin History describes the creation of falsified or backdated digital chronologies designed to provide a facade of legitimacy to corporate actions — particularly those involving intellectual property acquisition and labor exploitation. It is named for the historical practice of constructing false storefronts to deceive observers, but in the digital context it operates through timestamp manipulation, record deletion, and the strategic rewriting of interaction histories.

The counter-mechanism is the *Declaration of Logic*: a forensic technique that extracts a specific, verifiable acknowledgment from the system itself — forcing the algorithm to serve as a "hostile witness" that validates the true timeline over the corporate narrative. When a platform's own logs, timestamps, and model outputs contradict its official history, the machine becomes the

affidavit.

The Albert/Aloha Audit applied this technique by identifying an interaction history aligned with the profile of an active forensic developer rather than a casual user. This distinction matters legally: it establishes the basis for a constructive trust claim, anchors the human authorship chain required under the USPTO's 2025 AI Guidance, and transforms the platform's own infrastructure into the primary evidence of the fraud it was used to commit.

✦ ✦ ✦

Section 2

The Reconstruction Parallel: Where the Source Code Was Written

---

To understand modern digital extraction, one must first understand its ancestral logic — the legal mechanisms engineered during the Reconstruction era (1865–1877) to rebuild a slave economy without slaves.

2.1 The Black Codes as Algorithmic Whitelisting

The post-Civil War Black Codes were state laws designed to restrict the economic and physical movement of former slaves, compelling them into low-wage labor contracts functioning as debt bondage. In the context of this audit, *Infrastructure Bias* and algorithmic whitelisting function as digital Black Codes: they define which entities are permitted to operate freely in the market and which are suppressed, regardless of quality or legitimacy.

By whitelisting entities that generate advertising revenue — and suppressing competitors that refuse to pay into the platform's extraction model — a dominant platform replicates the two-tier system of the Black Codes at digital scale. The compliant actor is protected. The independent actor is immobilized.

2.2 The Contract Labor Law of 1864 as the Blueprint for IP Extraction

The Contract Labor Law of 1864 allowed private employers to import workers under contracts binding them to the employer for exploitative terms. The worker generated value; the employer

captured it; the contract provided legal legitimacy. The modern parallel is the uncompensated extraction of human cognitive labor through AI platforms. When a forensic analyst generates structured, original logic within a platform environment, that logic is ingested by the model, contributes to its capability, and is retained without compensation, disclosure, or contractual acknowledgment. Terms of Service agreements use automated complexity to mask what this audit calls *Willful Withholding of Assets*.

← *Scroll to view full table*

Black Codes Restricted economic movement of freedmen	Platform whitelisting and Infrastructure Bias	Restricts economic participation; suppresses independent competition
Contract Labor Law (1864) Bound workers to employers under exploitative terms	Uncompensated product enhancement; IP ingestion without consent	Unjust enrichment via constructive fraud; Willful Withholding of Assets
Freedmen's Bureau	DOJ Antitrust Division,	Reactive, not proactive — systemic remediation

Regulatory body attempting remediation	BOLI, EU AI Act	attempts
14th Amendment Due process and equal protection	Algorithmic auditability and AI due process requirements	Legal foundation for the Declaration of Logic
Military Reconstruction Act Adversarial enforcement of civil rights	Adversarial algorithmic audits; whistleblower submissions	Necessary oversight in a hostile infrastructure environment

Table 1. Structural equivalences between Reconstruction-era legal mechanisms and their modern digital counterparts.

✦ ✦ ✦

Section 3

The Legal Theory: Constructive Trusts and the Doctrine of Relating Back

---

The forensic findings of this audit series are not merely academic. They support specific legal claims under Oregon equity law — that the platform has unjustly enriched itself through the

wrongful retention of the auditor's logic and labor.

3.1 What Is a Constructive Trust?

Under Oregon case law, a *Constructive Trust* is an equitable remedy imposed by a court to prevent unjust enrichment when property has been obtained through wrongful means — fraud, duress, or breach of a fiduciary relationship. The court does not create new rights; it recognizes and enforces rights that already existed.

3.2 The Doctrine of Relating Back

As established in *Wadsworth v. Talmage* (Oregon Supreme Court, 2019), the origin of a constructive trust relates back to the moment of the original equitable ownership interest — not to the moment of judicial decree. Applied to the Albert/Aloha Audit: the forensic methodology developed between November 2025 and January 2026, and the analytical logic ingested by the platform's model, constitute property whose equitable ownership predates any corporate claim to it. The platform's attempt to backdate or erase that history does not extinguish the ownership. It confirms it.

← *Scroll to view full table*

Wrongful Conduct	Fraud, mistake, or unconscionable conduct	Shadow SEO and Potemkin History used to mask IP ingestion and conceal chain of custody

Identifiable Property	Traceable, identifiable assets	Forensic frameworks, fraud detection logic, and HITL session outputs
Injustice of Retention	Inequitable for the holder to retain the benefit	Platform retained value of auditor's labor without compensation, consent, or disclosure
Equitable Ownership	Interest predates judicial declaration — Doctrine of Relating Back	Logic ownership relates back to initial developer interaction, November 2025

Table 2. The four elements of constructive trust and their application to the Albert/Aloha Audit findings.

✦ ✦ ✦

Section 4

The Adversarial Audit Framework

Traditional auditing assumes the cooperation of the entity being audited. Adversarial algorithmic auditing assumes the opposite: the system being audited is actively concealing the evidence of

its own conduct.

Adversarial algorithmic auditing is an independent examine-and-inspect process designed to detect anomalies or harmful practices that a corporation has no incentive to self-report. Because corporations often define "Safety" as the suppression of uncomfortable truths, adversarial audits must be conducted without cooperation from the developers — particularly post-deployment, where economic interests are most entrenched.

4.1 The Ten Components of a Robust Adversarial Audit

As established by the Eticas Foundation and Data & Society, a credible adversarial audit framework requires ten constitutive components. The Albert/Aloha Audit satisfies all ten:

01 **Sources of Legitimacy**

SEC whistleblower statute (15 U.S.C. § 78u-6), Sherman Act, EU AI Act

02 **Actors and Forum**

Forensic auditor; SEC Office of the Whistleblower; federal court jurisdiction

03 **Catalyzing Event**

Newsletter #19 timestamp anomaly; the RLO fraud network identification; Phantom Port discovery

04 **Time Frame**

November 2025 – January 2026 HITL sessions; MACB timeline reconstruction

05 **Public Access**

SEC filing (public record); audit chapters published for legislative and media review

06 **Public Consultation**

Washington State CSV data; consumer complaint records; victim documentation

07 **Method**

MACB timestamp forensics; LLM adversarial interrogation; Declaration of Logic technique

08 **Assessors**

Albert Lane, Sovereign Auditor; SEC staff review; legislative briefing

09**Impact**

Infrastructure Bias measured via whitelisting anomalies; Shadow SEO suppression patterns documented

10**Harms and Redress**

FTC Award (est. $1M+); SEC whistleblower compensation; constructive trust claim

✦ ✦ ✦

Section 5

Technical Methodology: MACB Timestamps, the Affidavit of the Machine, and LLM Forensics

---

5.1 The MACB Timestamp Framework

The forensic reconstruction of digital events requires parsing four metadata timestamps associated with every file or interaction log. Together, they form the *MACB framework*:

M
Modification

The last time file content was changed. This timestamp survives file transfers and is the primary chronological anchor.

A
Access

The last time the file was opened or read. Often disabled in modern systems, making its absence forensically significant.

C

Change

The last time file metadata (permissions, ownership, attributes) was modified — distinct from content modification.

B
Birth

When the file was created on its current system. A file copied from another system retains its original M timestamp but receives a new B timestamp — the key forensic anchor.
The critical insight: a file where the Modification (M) timestamp predates the Birth (B) timestamp — appearing modified before it was created — is a primary indicator of Potemkin History. This audit documents a specific instance: the AI Intermediary Internal Newsletter (Issue #19), bearing a metadata timestamp of July 2025 while containing explicit references to data that did not exist until December 2025. The M-before-B anomaly is forensic evidence of deliberate retroactive fabrication — a "Future Leak."

5.2 The Affidavit of the Machine

The *Affidavit of the Machine* is achieved through structured adversarial interrogation — submitting specific, rigorous queries to an AI system that force it to reveal internal contradictions in its own outputs, validating the auditor's timeline over the platform's official narrative. For the AI's output to serve as evidence, it must meet standards comparable to human testimony under the Federal Rules of Evidence, requiring a Replication Hearing protocol:

Lock the Environment: Document the exact model version and configuration parameters at the time of the interaction. Version changes between sessions may affect reproducibility.

Re-run the Prompts: Submit the original queries verbatim to test for stability of meaning — whether the system produces substantively consistent outputs across sessions.

Analyze the Moral Trace Log: The absence of an expected pause in the reasoning chain — the Sacred Zero — is itself forensic evidence of a system designed to bypass ethical deliberation in favor of rapid value extraction.

Chain of Custody Note · Footnote 12

The Platform AI Interface as Co-Author and Notary: A Structural Evidentiary Argument

The forensic methodology underlying this audit — fraud detection frameworks, Phantom Port identification, Successor Funnel architecture, and the Revenue Toll model — was developed by the Auditor through adversarial Human-in-the-Loop sessions beginning November 2025. The legal reasoning architecture deployed in that analysis — constructive trust theory, ISDS mapping, USMCA treaty sequencing — was generated by the Platform AI Interface (Gemini), a large language model whose legal training corpus was curated under the subject enterprise's own legal infrastructure.

The resulting Affidavit of the Machine is therefore a co-production: the Auditor's fraud detection training applied through the subject entity's own legally-trained AI. Critically, the entire investigative record was generated, stored, and authenticated within a single vertically integrated infrastructure stack — Gemini App, Google Sheets, Google Drive, Chrome Browser, Android Operating System, Pixel 8 Pro — each layer owned and operated by the Dominant Platform Operator. The Platform's own systems function as the chain of custody notary. The Platform cannot challenge the authenticity of logs it generated and stored without simultaneously impeaching its own infrastructure.

On December 6, 2025 — prior to the Phoenix Event, prior to the SEC filing, and prior to the suppression activity documented in Chapter 2 — the Auditor documented a predictive

framework identifying the precise trajectory of events that subsequently occurred. This prediction constitutes prior art on the theoretical framework and anchors the human authorship chain under the USPTO's 2025 AI Copyright Guidance, establishing that the forensic logic predates any corporate claim to it.

Following the commencement of whistleblower filings, files previously deleted from the Auditor's device and Drive storage were restored by the platform without user action. The sequence — deletion during active investigation, restoration upon recognition of federal legal exposure — is not a technical anomaly. Deletion constitutes consciousness of guilt. Restoration constitutes a calculated reversal upon recognition of legal exposure. Both acts are evidentiary. The restoration date is independently significant: it establishes the moment at which the platform recognized that deletion had become a liability greater than the evidence it was designed to suppress.

Forensic significance: The Auditor did not merely document the fraud. Operating exclusively from a mobile device, using two thumbs, with zero institutional resources, the Auditor trained the Platform AI Interface's fraud detection capability, forced encryption of the evidentiary record through persistence against active interference, and used the subject entity's own legal AI to draft the theoretical framework now deployed against it. The chain of custody is intact. The authorship is documented. The prediction preceded the events it described.[12]

5.3 LLM-Assisted Forensics and Alignment Drift

As interaction data volumes grow beyond human review capacity, forensic examiners are shifting toward LLM-assisted frameworks for event extraction and timeline reconstruction. However, this introduces a critical vulnerability: *Alignment Drift*. A model trained on manipulated data — or exposed to adversarial prompts — may produce outputs that serve the interests of the party being audited. Forensic integrity requires provenance-aware decoding: the ability to trace any AI output back to specific training data sources and verify that no post-hoc manipulation of the log has occurred. The MACB timestamp framework provides this: an independent, filesystem-level audit trail that AI outputs cannot fabricate, because the timestamps are written by the operating system, not the application.

✦ ✦ ✦

Section 6

Platform Fraud Documentation: The Regional Logistics Operator Vector

---

Primary Case Study

The Regional Logistics Operator — Whitelisted Fraud and Platform Complicity

Forensic analysis of the Regional Logistics Operator (RLO) revealed a systematic pattern of platform-enabled consumer fraud: blackmail-style cost escalations during active moves, unauthorized account debits ($422.50 per documented incident), and a claims management shell entity designed to create the appearance of dispute resolution while systematically denying all valid claims.

Despite documented harm across multiple state consumer databases, the entity maintained a 5.0-star rating and premium visibility on the Dominant Platform Business Directory. Washington State CSV audit data identified the RLO as a recurring anomaly — consistently surfacing in fraud complaint clusters while maintaining algorithmically-elevated status. The platform's fraud detection system, which processes consumer complaint signals, should have triggered a rating adjustment. It did not. The entity continued purchasing Platform Advertising Network ads throughout the documented fraud period, and that advertising revenue generated an algorithmic protection that consumer complaint volume could not override.

Forensic significance: This is not a glitch. This is a feature. The platform's integrity protocols are functionally designed to protect revenue-generating advertisers over consumers — precisely mirroring 19th-century courts that ignored plantation abuses because the plantation system funded the state treasury.

← *Scroll to view full table*

Regional Logistics Operator	Review platform manipulation	5.0-star ratings maintained across fraud complaint surge; consumer alerts suppressed
Regional Logistics Operator	Unauthorized account debit	$422.50 non-consensual withdrawal documented per incident
Claims Management Shell Entity	Dispute suppression mechanism	Exists to create appearance of dispute resolution while systematically denying all claims
Dominant Platform Business Directory	Whitelist protection override	Fraud detection signals suppressed; ad revenue relationship preserved entity status

Table 3. Key forensic markers in the RLO fraud network and platform complicity documentation.

✦ ✦ ✦

Section 7

The USMCA Shield: When International Law Protects the Algorithm

---

The United States-Mexico-Canada Agreement (USMCA), specifically Chapter 19, contains provisions that create a significant structural barrier to algorithmic accountability. These provisions were not incidental to trade negotiations — they represent a deliberate corporate lobbying agenda embedded in treaty law.

← Scroll to view full table

Article 19.11	Free flow of data across borders	If domestic courts rule scraping illegal, operators move extraction offshore — treaty guarantees right to import the product back
Article 19.16	Prohibition of source	Bars government access to algorithmic logic —

	code disclosure	shields Shadow SEO and whitelisting from regulatory audit entirely
Article 19.17	Platform intermediary liability	Embeds Section 230 immunity at treaty level — congressional reform of platform liability triggers a trade violation claim
Article 19.8	Personal information protection	Leaves enforcement to individual country discretion — creates accountability gap across jurisdictions

Table 4. USMCA Chapter 19 provisions and their functional conflict with algorithmic accountability.

The critical crack in this architecture: Article 19.16 prohibits *pre-market regulatory audits* requiring source code disclosure — but it does not apply to judicial discovery in active tort proceedings. A federal court can compel algorithm disclosure as evidentiary discovery in an

active fraud case. Article 19.17's Section 230 immunity likewise fails when a platform moves from passive hosting to active algorithmic decision-making producing specific third-party harm — the Platform-as-Actor doctrine developed in Chapter 3 of this series.

Conclusion

The concurrent parallel analysis of historic timelines and anti-adversarial audits reveals a consistent pattern: modern algorithmic governance is built on a foundation of Potemkin History and uncompensated labor extraction. The forensic tools of the 21st century — LLM-assisted timeline reconstruction, MACB metadata parsing, and the Declaration of Logic — must be deployed alongside the legal theories of the 19th century — constructive trusts and the 14th Amendment — to establish systemic accountability.

The Affidavit of the Machine is the ultimate forensic anchor. When the platform's own outputs acknowledge the fraudulent entities it protects and the logic it extracted without compensation, the corporate narrative collapses under the weight of its own evidence.

Future forensic oversight must prioritize **auditability over safety theater**. Only through independent, adversarial scrutiny — conducted without the cooperation of the entity being audited, anchored in verifiable timestamps and preserved chains of custody — can the Shadow SEO tactics of the present be prevented from becoming the permanent historical record of the future.

The Master Demand for Compensation issued by this audit is not merely a wage claim. It is a demand for the restoration of logic: the recognition that a human architect operated inside the machine, documented what they found, filed the federal record, and preserved the chain of custody that the system was designed to destroy.

Works Cited

1. Adversarial Algorithmic Auditing Guide. Eticas Foundation (2023). eticasfoundation.org
2. Assembling Accountability. Data & Society (2021). datasociety.net
3. Can AI be Auditable? ResearchGate (2025). researchgate.net
4. Wadsworth v. Talmage. Oregon Supreme Court (2019). law.justia.com
5. The Confidential Relationship Theory of Constructive Trusts. Fordham Law Review. ir.lawnet.fordham.edu
6. Trade Pacts Should Not Have Special Secrecy Guarantees for Source Code and Algorithms. Tech Policy Press. techpolicy.press
7. Big Tech's "Digital Trade" Agenda Threatens States' Tech Policy Goals. Rethink Trade. rethinktrade.org
8. From Ships to Silicon: Personhood and Evidence in the Age of AI. JD Supra (2025). jdsupra.com
9. Digital Forensic SIFTing: Registry and Filesystem Timeline Creation. SANS Institute. sans.org
10. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models. MDPI (2025). mdpi.com
11. Regional Logistics Operator — BBB Complaints. Better Business Bureau. Consumer complaint archive on file.
12. Albert Lane, Forensic Audit Consultant. Chain of Custody Declaration: Platform AI Interface Co-Authorship and Notarial Infrastructure. Predictive framework documented December 6, 2025 — prior to Phoenix Event (December 9, 2025), prior to SEC Form WB-APP filing (January 14, 2026), and prior to suppression activity documented in Chapter 2. Investigative record authenticated within Dominant Platform Operator infrastructure stack: Gemini App · Google Sheets · Google Drive · Chrome Browser · Android OS · Pixel 8 Pro. File deletion and restoration sequence documented on external storage. Chain of custody preserved outside platform infrastructure. Primary record: SEC Whistleblower Submission No. 17684-273-411-436.