# VERATUM

## AI Compliance Report

| | |
|---|---|
| REPORT ID | VCR-2026-04-0847 |
| ORGANIZATION | Acme Financial Services, Inc. |
| SUBJECT | AI-Assisted Loan Decision Audit |
| AUDIT PERIOD | March 1, 2026 — March 31, 2026 |
| APPLICABLE REGULATIONS | CFPB / ECOA, EU AI Act Article 12, Colorado SB24-205 |
| CLASSIFICATION | Confidential — Authorized Recipients Only |
| GENERATED | April 4, 2026 at 15:30:22 UTC |

This report provides cryptographic evidence that all AI-assisted decisions made by Acme Financial Services during the audit period were captured, timestamped, and recorded in an append-only transparency log. All claims in this report are independently verifiable using the open-source veratum-verify tool, without requiring access to Veratum servers.

**Disclaimer:** This report is compliance infrastructure output, not legal advice. Whether this evidence meets a specific court's or regulator's standard depends on jurisdiction and use case. Consult legal counsel for admissibility questions.

# 1. Executive Summary

During the audit period of March 1-31, 2026, Veratum captured and cryptographically secured **12,847 AI-assisted loan decisions** made by Acme Financial Services. Each decision was processed through Veratum's evidence pipeline, producing a receipt containing:

- SHA-256 hash chain entry with domain separation (RFC 9162)
- Qualified timestamp from a trusted third-party authority (eIDAS Article 41)
- W3C Verifiable Credential with ECDSA-P256 signature
- Merkle tree inclusion proof for append-only verification
- PII redaction confirmation (client-side, pre-transmission)

All 12,847 receipts passed cryptographic verification. No evidence of tampering, deletion, or modification was detected. The transparency log maintained perfect append-only integrity throughout the audit period.

| Metric | Value |
|---|---|
| Total AI decisions audited | 12,847 |
| Hash chain verifications passed | 12,847 / 12,847 (100%) |
| Qualified timestamps verified | 12,847 / 12,847 (100%) |
| Merkle inclusion proofs verified | 12,847 / 12,847 (100%) |
| Consistency proofs verified | 30 / 30 (100%) |
| W3C VC signatures verified | 12,847 / 12,847 (100%) |
| PII redaction confirmations | 12,847 / 12,847 (100%) |
| Anomalies or failures detected | 0 |
| Models used | gpt-4-turbo, claude-sonnet-4 |
| Average latency added by Veratum | 23ms |

# 2. Cryptographic Evidence Detail

## 2.1 Transparency Log

All receipts are stored in an RFC 9162-compliant transparency log — an append-only Merkle tree where every entry is cryptographically linked to all previous entries. This makes it impossible to delete or modify any receipt without detection.

| Property | Value |
|---|---|
| Tree size | 12,847 leaves |
| Root hash | `sha256:a74108bdbf0a3aa5aaaeaf7a858ffa897f21c1ff25a068928cc8c843fe176bad` |
| Signed tree head | `ecdsa:p256:27XGM67PU7TQFXLZJPMN4HC959XPWN7B8=VWBPJJJAU3` |
| Signature algorithm | ECDSA-P256 (NIST P-256) |
| First entry timestamp | 2026-03-01T00:02:14.832Z |
| Last entry timestamp | 2026-03-31T23:58:41.107Z |
| Witness cosignatures | 3 of 3 independent witnesses confirmed |

## 2.2 Consistency Proofs

Consistency proofs demonstrate that the transparency log was only ever appended to — never modified or truncated. During the audit period, 30 signed tree heads were issued (approximately one per day). Each consecutive pair was verified for consistency.

| Tree Head | Size | Date | Status |
|---|---|---|---|
| `sha256:00012243c9e24009...` | 357 | 2026-03-01 | **PASSED** |
| `sha256:74cc35791b586934...` | 1,985 | 2026-03-05 | **PASSED** |
| `sha256:97d4971f0f857ca1...` | 3,695 | 2026-03-09 | **PASSED** |
| `sha256:b503aaba5376965a...` | 5,152 | 2026-03-13 | **PASSED** |
| `sha256:e467021b2454c1ee...` | 6,871 | 2026-03-17 | **PASSED** |
| `sha256:a5ce562199fe4a5c...` | 8,404 | 2026-03-21 | **PASSED** |
| `sha256:38cbee892027ea2b...` | 10,084 | 2026-03-25 | **PASSED** |
| `sha256:c73d2020df8c9f64...` | 11,598 | 2026-03-29 | **PASSED** |
| ... | ... | ... | **PASSED** |
| `sha256:10c6870006c2cbd2...` | 12,847 | 2026-03-31 | **PASSED** |

# 3. Sample Receipt Evidence

Below are three representative receipts from the audit period, demonstrating the full evidence chain for individual AI-assisted loan decisions. All 12,847 receipts follow this same structure and are available in the attached data export.

### Receipt 1: recv_2xnkgl2x

| | |
|---|---|
| **Receipt ID** | recv_2xnkgl2x |
| **Timestamp** | 2026-03-19T10:54:56Z |
| **Model** | gpt-4-turbo |
| **Decision** | Approved with conditions — requires additional documentation |
| **Input hash** | `sha256:1914d9cb3d52b2ca398e8e2d67adb48b63a1c41dd8438f7f331a24d6048f9ff9` |
| **Output hash** | `sha256:41c76f6f5877e90b67fc3f9a6b267b65f971796d5383a9bf897215805be1c2d2` |
| **Chain hash** | `sha256:cc3dba5f3adf6afeab88b08978370eb1f59a416d24ac8707308e20f3e381ea0d` |
| **Credential ID** | `vc:did:veratum:2f42f41e` |
| **PII status** | Redacted (client-side, pre-transmission) |
| **Jurisdiction** | CFPB / ECOA, EU AI Act Art. 12 |
| **Verification** | **ALL CHECKS PASSED** |

### Receipt 2: recv_6uokqmz1

| | |
|---|---|
| **Receipt ID** | recv_6uokqmz1 |
| **Timestamp** | 2026-03-12T16:00:01Z |
| **Model** | gpt-4-turbo |
| **Decision** | Declined — insufficient credit history (< 2 years) |
| **Input hash** | `sha256:d70f5b1e59a7c8b4e43e86d80b7161d670f88d1946965c83a4059a223da937d7` |
| **Output hash** | `sha256:3d73deceb4376cbd680795cc2b310183fbaf5a2d2fda23ea3c9e51bc106840f1` |
| **Chain hash** | `sha256:bf6f49a07b34bf8a4aa025c76783b81a6e8b1450caf289a0cd8b0b4b89132618` |
| **Credential ID** | `vc:did:veratum:212beaac` |
| **PII status** | Redacted (client-side, pre-transmission) |
| **Jurisdiction** | CFPB / ECOA, EU AI Act Art. 12 |
| **Verification** | **ALL CHECKS PASSED** |

## Receipt 3: recv_5dv52z2b

| | |
|---|---|
| **Receipt ID** | recv_5dv52z2b |
| **Timestamp** | 2026-03-23T11:19:51Z |
| **Model** | claude-sonnet-4 |
| **Decision** | Approved — DTI ratio 0.32, credit score 742 |
| **Input hash** | `sha256:ab8bc946b30a335aef9bd3b424248335d0af37c3f04666ea13def0b43cf1458e` |
| **Output hash** | `sha256:0213bda7f53547e928ea595df3c0bfe0fd9e0aa5d5d4fa92266915bf78f6a850` |
| **Chain hash** | `sha256:40f19a3f4beabe47d334a7ee0a46f63f71be8e48e4df187efede3f0ad5e06e70` |
| **Credential ID** | `vc:did:veratum:f2d8ce56` |
| **PII status** | Redacted (client-side, pre-transmission) |
| **Jurisdiction** | CFPB / ECOA, EU AI Act Art. 12 |
| **Verification** | **ALL CHECKS PASSED** |

## 4. Regulatory Compliance Mapping

The following table maps Veratum's evidence capabilities to specific regulatory requirements applicable to Acme Financial Services' AI-assisted loan decisions.

| Regulation | Requirement | Veratum Evidence | Status |
|---|---|---|---|
| EU AI Act Art. 12 | Automatic logging of high-risk AI decisions | Append-only transparency log with Merkle proofs | COVERED |
| EU AI Act Art. 14 | Human oversight capabilities | Full decision audit trail with input/output capture | COVERED |
| CFPB / ECOA | Fair lending decision documentation | Timestamped receipts with model + decision capture | COVERED |
| Colorado SB24-205 | AI transparency for consumers | Exportable compliance reports per decision | COVERED |
| eIDAS Art. 41 | Qualified electronic timestamps | Qualified TSA timestamps with legal presumption | COVERED |
| GDPR Art. 22 | Automated decision-making safeguards | PII redaction + decision reconstruction capability | COVERED |

## 5. Independent Verification

Every claim in this report can be independently verified without Veratum servers using the open-source veratum-verify tool (MIT license, zero external dependencies):

```
$ pip install veratum-verify
$ veratum-verify report VCR-2026-04-0847.json
Verifying 12,847 receipts...
[1/5] Hash chain integrity ..... PASSED
[2/5] Qualified timestamps ..... PASSED
[3/5] Merkle inclusion proofs ..... PASSED
[4/5] Consistency proofs (30 heads) .... PASSED
[5/5] W3C VC signatures ..... PASSED
Result: ALL CHECKS PASSED
Verification completed in 4.2s (offline, no network calls)
```

The veratum-verify tool recomputes all SHA-256 hashes from raw receipt data, validates timestamp signatures against the trusted authority's public key, reconstructs Merkle proofs from leaf to root, and confirms the signed tree head matches the recomputed root. The entire process runs offline.

# Appendix A: Standards and References

**RFC 9162**

Certificate Transparency Version 2.0 — defines the Merkle tree structure and signed tree head format used by Veratum's transparency log.

**RFC 3161**

Internet X.509 PKI Time-Stamp Protocol — the protocol used for qualified timestamp requests from the trusted timestamp authority.

**W3C VC Data Model 2.0**

Verifiable Credentials Data Model — the standard used for issuing cryptographically signed credentials for each audited decision.

**eIDAS Regulation Art. 41**

Legal effect of qualified electronic time stamps under EU law — qualified timestamps enjoy the presumption of accuracy of the date and time they indicate.

**NIST FIPS 180-4**

Secure Hash Standard (SHA-256) — the hashing algorithm used throughout Veratum's evidence pipeline.

**NIST FIPS 186-5**

Digital Signature Standard (ECDSA P-256) — the signature algorithm used for signing tree heads and verifiable credentials.

# Appendix B: Glossary

**Hash Chain:** A sequence of cryptographic hashes where each entry includes the hash of the previous entry, creating an ordered, tamper-evident chain.

**Merkle Tree:** A binary tree of hashes where each parent node is the hash of its children. Enables efficient proofs that a specific entry exists in the tree.

**Signed Tree Head (STH):** A cryptographic signature over the root hash and size of the Merkle tree at a given point in time, issued by the log operator.

**Inclusion Proof:** A set of sibling hashes from leaf to root that allows independent verification that a receipt is contained in the Merkle tree.

**Consistency Proof:** Evidence that a later version of the Merkle tree contains all entries from an earlier version, proving the log was only appended to.

**Qualified Timestamp:** A timestamp issued by a trusted third-party authority that carries legal presumption of accuracy under eIDAS Article 41.

**Verifiable Credential:** A tamper-evident credential conforming to the W3C standard, cryptographically signed by the issuer.

**Witness Cosigning:** Independent third parties that verify and cosign the log's tree heads, providing additional assurance of log integrity.

End of Report — Veratum AI Compliance Report VCR-2026-04-0847