

Data Liability Assessment

Tier 2 Full Opinion Report

Company: Everalbum Mock (Synthetic Data)

Date: 2026-10-10

File: ever_user_export_2019.csv

Contact: counsel@example.com

Records: 25,000

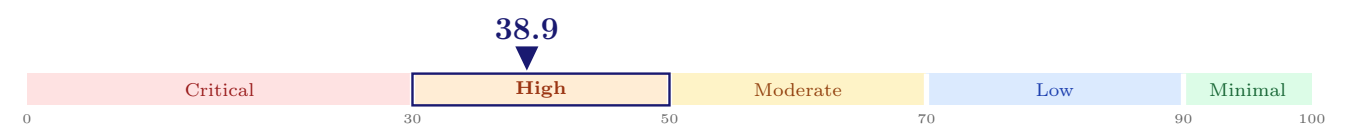
SHA-256: 47faa7420de83a03...

Note: Illustrative mock report. Synthetic data modeled on the public FTC record in FTC v. Everalbum (2021); not Everalbum’s actual data. Shows what LQ would flag for a file like this.

Executive Summary

LQ Score

Risk classification: **HIGH RISK**



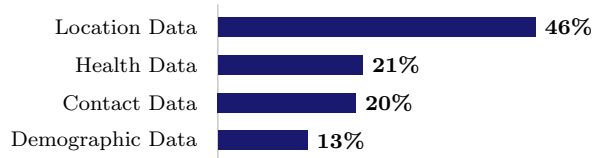
Modeled Exposure

Inherent, directional (USD). Scales with record count.



Where the Exposure Comes From

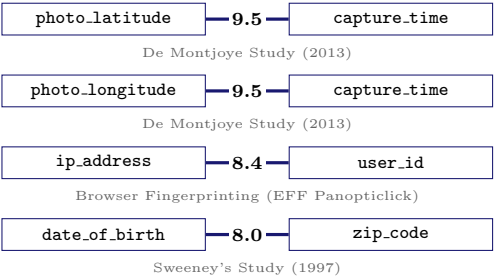
Share of base PII risk (sensitivity × density) by data domain



Not detected: Identification Data, Financial Data, Sensitive Beliefs, Credentials.

Re-identification Linkages

Fields that identify people in combination



Number on each link is its linkage weight (risk amplifier).

What Diligence Should Confirm First

- Biometrics.** Was informed written consent obtained before biometric data was collected, and is a published retention and destruction schedule in place?
 - Minors.** Could any data subjects be children (under 13 in the US, or under the applicable age elsewhere)? If so, confirm age-gating and verifiable parental consent.
 - Location data.** Was specific opt-in consent obtained for precise location data, and has it been sold or shared with third parties?
- All follow-up questions, with their legal basis, are on page 3.

Coverage. All 25,000 rows and 17 columns read. Pattern and checksum checks on every value; NLP on a reproducible sample (seed 42). This report measures what personal data is present, not whether it is lawfully held.

Risk Detail

Data Domains Detected

Domain	Present	Density
Identification Data	No	—
Financial Data	No	—
Health Data	Yes	High
Location Data	Yes	High
Contact Data	Yes	High
Demographic Data	Yes	High
Sensitive Beliefs	No	—
Credentials	No	—

Linkage Risk Profile

Linkage Category	Status
Demographic Combinations	Detected
Location Combinations	Detected
Health Combinations	Not Detected
Financial Patterns	Not Detected
Professional/Social Context	Not Detected

Linkage categories represent “toxic pairs and triplets” — combinations of quasi-identifiers that enable re-identification through the mosaic effect, even without direct identifiers.

Key Observations

- High density of health data detected, representing the primary regulatory exposure in this dataset.
- 2 linkage categories detected, indicating moderate re-identification risk through the mosaic effect.
- Global/Multi-jurisdictional jurisdiction context amplifies base risk exposure.

Rating Classification

LQ Score	Risk Class	Typical Diligence Considerations
90–100	Minimal	Standard governance
70–89	Low	Standard representations & warranties typically sufficient
50–69	Moderate	Consider enhanced controls and targeted diligence
30–49	High	Consider specific indemnity or escrow
0–29	Critical	Consider remediation before close, specific indemnity or escrow

Follow-up Questions for Counsel

This scan measures what personal data is present, not whether it is lawfully held. The questions below are generated from this dataset's findings and declared context by a fixed rules table, and identify what diligence should confirm. Finding-specific questions appear first.

Topic	Question and basis
Biometrics	Was informed written consent obtained before biometric data was collected, and is a published retention and destruction schedule in place? Basis: Illinois BIPA (740 ILCS 14/15); Texas CUBI; GDPR Art. 9
Minors	Could any data subjects be children (under 13 in the US, or under the applicable age elsewhere)? If so, confirm age-gating and verifiable parental consent. Basis: COPPA (16 CFR Part 312); GDPR Art. 8
Location data	Was specific opt-in consent obtained for precise location data, and has it been sold or shared with third parties? Basis: CPRA sensitive personal information (§1798.121); FTC actions against location data brokers
Calls and texts	If phone numbers are used for marketing calls or texts, do consent records exist that meet TCPA requirements? Basis: TCPA (47 U.S.C. §227)
Re-identification	Has the target described this data as anonymized or de-identified? The field combinations detected can enable re-identification. Confirm what de-identification standard was applied and whether recipients are contractually barred from re-identifying it. Basis: GDPR Recital 26; HIPAA de-identification (45 CFR §164.514(b)); CCPA deidentified data (§1798.140)
EU and UK subjects	What lawful basis supports processing of EU and UK personal data, and what mechanism (adequacy, SCCs, BCRs) covers any transfer outside the EEA or UK? Basis: GDPR Art. 6 and Chapter V; UK GDPR
Canadian subjects	If Canadian residents are included, does consent meet PIPEDA's meaningful-consent standard? For Quebec residents, was a privacy impact assessment completed before any transfer outside Quebec? Basis: PIPEDA Sch. 1, Principle 4.3; Quebec Law 25 (Private Sector Act, s. 17)
AI training	Does the original notice or consent cover use of this data to train machine-learning models? Regulators have ordered deletion of models trained on improperly obtained data. Basis: FTC orders requiring model deletion (e.g. Everalbum, 2021)
<i>Asked for every dataset</i>	
Provenance	How was this dataset collected or acquired, and do records show its source and chain of custody? Basis: General diligence; supports representations on lawful collection
Notice and purpose	What privacy notice was in effect when the data was collected, and does it cover the target's current use and the buyer's intended use? Basis: FTC Act §5; GDPR Arts. 13–14; CCPA §1798.100
Incidents	Has this dataset, or any system holding it, been subject to a breach, security incident, complaint or regulatory inquiry? Basis: State breach notification laws; GDPR Arts. 33–34; PIPEDA s. 10.1
Contracts	Do customer contracts, data processing agreements or licences restrict transfer of this data to an acquirer or limit its intended use? Basis: Contractual diligence

Bases are cited as starting points for counsel's analysis, not as conclusions about whether a requirement applies.

Declared Context

These inputs were declared by the user, not detected in the data. They adjust the score and exposure band.

Jurisdiction	Global / Multi-Jurisdictional
Organization revenue	Under \$50M annual revenue
Infraction history	No Infraction History
Intended use	LLM Training (External API)

Scan Coverage

- Rows and columns: all 25,000 rows and 17 columns were read.
- Column headers: every column name was checked against the PII definitions; 14 of 17 columns were identified by header.
- Pattern, checksum and keyword checks: every non-empty value in the 3 columns not identified by header (53,233 values, no sampling).
- NLP entity recognition: a reproducible random sample of up to 300 values per column (seed 42) in 3 columns (900 values analyzed), extrapolated to the full column.

Methodology Summary

The LQ Legal Risk Engine employs a multi-layer analysis framework:

- 1. **PII Detection Framework** — Structured detection hierarchy using header analysis, pattern matching, and NLP-based entity recognition to identify 70+ PII types with associated risk weights.
- 2. **Linkage Risk Analysis** — Evaluation of “toxic pairs” (quasi-identifier combinations) that enable re-identification even without direct identifiers. Based on established privacy research including the Mosaic Effect principle.
- 3. **Context-Adjusted Risk Calculation** — Base asset risk is amplified by contextual factors including regulatory jurisdiction, organizational profile, infraction history, and intended data use.
- 4. **Exposure Modeling** — Inherent exposure is modeled directionally using a square-root sensitivity model with a baseline of \$250 per record, loosely anchored to published per-record breach cost research (e.g. IBM/Ponemon). It is not fitted to enforcement outcomes.

For detailed methodology documentation: <https://liabilityquant.com/methodology>

Regulatory Compliance Reference

Risk Factor	Relevant Regulatory Frameworks
Direct Identifiers	GDPR Art. 4 (personal data definition), CCPA §1798.140 (personal information), PIPEDA
Sensitive/Special Category Data	GDPR Art. 9 (special categories), HIPAA (PHI), BIPA (biometrics), state genetic privacy laws
Linkage & Re-identification Risk	GDPR Recital 26 (identifiability standard), FTC Act §5 (unfair practices)
Data Processing Activities	GDPR Art. 6 (lawful basis), CCPA §1798.100 (disclosure requirements)
Minor/Child Data	COPPA (under 13), GDPR Art. 8 (child consent), state student privacy laws (FERPA)
Cross-Border Transfers	GDPR Chapter V, adequacy decisions, Standard Contractual Clauses

This mapping is provided as educational context. Consult qualified legal counsel for jurisdiction-specific compliance guidance.

Disclaimers & Limitations

This assessment provides a **standardized, directional measure of inherent privacy exposure** to support due diligence, M&A valuations, and cyber insurance underwriting purposes.

- **Not Legal Advice.** This report is a quantitative risk assessment tool. It does not constitute legal advice and should not be relied upon as such. Consult qualified legal counsel for compliance guidance specific to your jurisdiction and circumstances.
- **What This Report Does Not Assess.** This report measures the personal data *present* in the file and how linkable it is (inherent exposure). It does not assess the existence or validity of consent; lawful basis for processing; data provenance; prior breaches or regulatory history (beyond context declared by the user); cross-border transfer restrictions and mechanisms, including Quebec Law 25; or contractual commitments such as privacy policies and DPAs. These factors can substantially reduce or increase actual exposure and should be established in diligence. This report supplements, and does not replace, legal due diligence.
- **Declared Context.** Jurisdiction, infraction history and intended data use are declared by the user, not detected in the data. Results depend on the accuracy of those declarations.
- **Methodology Scope.** The LQ engine analyzes structured data files for PII patterns. Limitations include: unstructured text fields may not be fully scanned; contextual PII specific to niche industries may not be detected; obfuscated or encoded identifiers may not be recognized.
- **Exposure Estimate.** The modeled exposure band is a directional, model-based estimate of inherent exposure, shown as a fixed range rather than a single figure. Actual penalties depend on specific breach circumstances, regulatory discretion, cooperation efforts, and applicable case law.
- **Data Handling.** Liability Quant does not retain uploaded file contents. Only metadata (file hash, scores, session information) is stored for audit trail purposes per industry best practices.
- **Point-in-Time Assessment.** This report reflects the analyzed file as of the assessment date. Regular re-assessment is recommended as data and regulatory landscapes evolve.