

# Lockette™

## CONFIDENTIAL INVESTMENT MEMORANDUM

---

### Executive Summary

---

Prepared: November 2025  
Desk of Aaron Dyer, Founder & CEO

# EXECUTIVE SUMMARY

---

## THE OPPORTUNITY

The global age verification market stands at **\$2.22 billion USD in 2025** and is projected to reach **\$5 billion USD by 2033** (CAGR 15%). However, current solutions create a fundamental conflict: they achieve compliance at the cost of user privacy, leading to massive user abandonment.

**The Evidence:** - Following UK age verification law enforcement (July 2025), Pornhub experienced a **47% traffic decline** - 3.2 million daily visitors dropped to 2.0 million within two weeks - VPN downloads surged **1,400%** as users sought privacy alternatives - Similar patterns observed across XVideos (47% drop) and OnlyFans (10% drop)

**Source:** BBC News, August 2025; Similarweb Analytics

## THE PROBLEM

Current age verification solutions demand extensive personal information: - Full legal names - Residential addresses - Government-issued photo identification - Facial recognition biometric captures - Credit card details

This creates three critical failures:

- 1. Privacy Violation:** Users must surrender anonymity to access age-restricted content
- 2. Security Risk:** Centralized PII databases create lucrative targets for cybercriminals
- 3. Market Resistance:** Privacy-conscious users abandon compliant platforms entirely

**The Cost of Failure:** - Average data breach cost: **\$4.44 million USD** (2025 global average) - U.S. data breach cost: **\$10.22 million USD** (2025, all-time high) - Healthcare/sensitive data breaches: **\$7.42 million USD** average - Consumer fraud losses: **\$27.2 billion USD** (2024, +19% YoY)

**Source:** Identity Theft Resource Center, 2025 Data Breach Report

## THE LOCKETTE™ SOLUTION

Lockette represents a **fundamental architectural reimaging** of age verification. We accomplish what current solutions claim is impossible:

### Zero PII Storage Architecture

**What We Store:**

```
{  
  deviceHash: "anonymous SHA-256 hash",  
  isValidated: boolean,  
  restrictionLevel: "18+/21+/25+",  
  timestamp: Date,  
  validatorHash: "anonymous SHA-256 hash"  
}
```

**What We Don't Store:** - Names (we don't collect them) - Addresses (we don't collect them) - Photos/biometrics (never leave user's device) - Government IDs (never transmitted) - Browsing history (we don't track it) - Email addresses (not required) - Phone numbers (not required)

### The Technical Breakthrough

Lockette leverages three key innovations:

1. Device-Local Biometric Storage

2. Biometric templates stored in hardware Secure Enclave/TEE
3. Cannot be extracted or transmitted
4. Hardware-attested, tamper-resistant

## **5. Validator Network Integration**

6. Leverages existing in-person ID verification infrastructure
7. Bartenders, bouncers, retail clerks validate using QR codes
8. Time-stamped, location-verified approval process

## **9. Customer Responsibility Model**

10. Business employers approve and vouch for their validators
11. Accountability chain: Validator → Employer → Lockette
12. Instant revocation and re-verification workflow

## **The User Experience**

**Initial Verification (One-Time):** 1. User downloads Lockette app (iOS/Android) 2. User visits age-restricted physical location (bar, dispensary, liquor store) 3. Validator scans user's ID per normal procedures 4. User shows QR code from app 5. Validator scans QR code → user validated 6. **Total time: <60 seconds**

**Return Verification (Every Future Visit):** 1. User visits age-restricted website 2. Site prompts "Verify with Lockette" 3. User approves with biometric/PIN (on-device) 4. Site receives boolean: VERIFIED or NOT VERIFIED 5. **Total time: <2 seconds**

**Privacy preserved: 100%**

# COMPETITIVE ADVANTAGE

## Technical Moat

Current competitors (Yoti, Onfido, Veriff, AU10TIX) operate on a **data collection business model**: - They monetize by selling identity verification services - Revenue depends on processing personal information - Regulatory compliance requires storing audit trails - Architectural incentive to collect and retain data

Lockette operates on a **privacy-as-infrastructure model**: - Revenue from customer API usage (per-verification fees) - Zero dependency on personal data - Compliance through mathematical proof of zero PII storage - Architectural incentive to minimize data collection

**This difference is not incremental—it is categorical.**

Competitors cannot replicate Lockette's architecture without abandoning their entire business model and rebuilding from first principles.

## Regulatory Advantage

**GDPR Compliance (European Union):** - No personal data stored = no GDPR obligations - No data subject access requests - No right-to-be-forgotten complexity - No cross-border data transfer restrictions

**CCPA Compliance (California):** - No personal information = no consumer privacy rights triggers - No opt-out requirements - No sale of personal information concerns

**Sector-Specific Advantages:** - Healthcare: No HIPAA exposure - Financial: No PCI-DSS scope - Adult content: No reputational PII database risks

# MARKET VALIDATION

## Privacy-Sensitive Sectors

Four high-value markets demonstrate acute privacy concerns:

1. **Adult Content Streaming**
2. Market size: \$15 billion USD annually (U.S.)
3. Privacy sensitivity: EXTREME
4. User abandonment evidence: 47% traffic drop with ID requirements
5. **Cannabis Retail (Legal Jurisdictions)**
6. Market size: \$33 billion USD (U.S., 2024)
7. Privacy sensitivity: HIGH (federal illegality stigma)
8. Verification frequency: Every transaction
9. **Alcohol E-Commerce**
10. Market size: \$2.4 billion USD (U.S., 2025)
11. Privacy sensitivity: MODERATE
12. Growth rate: 18% CAGR
13. **Reproductive Healthcare/Contraceptives**
14. Market size: \$1.8 billion USD (contraceptive delivery, U.S.)
15. Privacy sensitivity: EXTREME (post-Dobbs legal environment)
16. User anonymity: Critical requirement

## **First-Mover Advantage**

Lockette is **first-to-market** with zero-PII age verification architecture:

- No deployed competitors with comparable privacy guarantees
- Patent-pending validator network integration model
- Early partnerships with privacy advocacy organizations
- User trust advantage in privacy-sensitive markets

## **BUSINESS MODEL**

### **Revenue Streams**

1. **Customer API Licensing**
2. \$0.05 per verification (Tier 1: <100K monthly verifications)
3. \$0.03 per verification (Tier 2: 100K-1M monthly)
4. \$0.01 per verification (Tier 3: 1M+ monthly)
5. Enterprise custom pricing
6. **Validator Employer Subscriptions**
7. \$49/month per business location (up to 5 validators)
8. \$99/month per location (up to 20 validators)
9. Enterprise pricing for chains (500+ locations)

### **Unit Economics**

**Customer Acquisition Cost (CAC):** - B2B enterprise: \$8,000-\$15,000 (sales-driven) - SMB self-service: \$200-\$500 (digital marketing)

**Lifetime Value (LTV):** - Adult content platform (10M monthly users, 50% active monthly): -  $5M \text{ verifications/month} \times \$0.03 = \$150,000/\text{month}$  - 3-year LTV:  $\$5.4M$  - LTV:CAC ratio: 360:1 (enterprise)

- Regional dispensary chain (50 locations):
- $\$99/\text{month} \times 50 \text{ locations} = \$4,950/\text{month}$
- 3-year LTV:  $\$178,200$
- LTV:CAC ratio: 11:1 (SMB)

**Gross Margin:** - API verification infrastructure: 92% gross margin - Validator subscription: 95% gross margin

## TRACTION & MILESTONES

### Current Status (November 2025)

**Product Development:** -  Core API server architecture complete -  Zero-PII verification model implemented -  Android application (Alpha version) -  Validator QR-based approval workflow operational -  Customer API integration documented -  iOS application (Q1 2025 target)

**Technology Validation:** - Device-local biometric storage: TESTED - Hardware attestation: VALIDATED - QR code validation flow: OPERATIONAL - API latency:  $<300\text{ms}$  (target:  $<500\text{ms}$ )

### Go-To-Market Timeline

**Q1 2025:** - Complete iOS application development - Launch pilot program with 3-5 adult content platforms - Onboard 50-100 validator locations (bars, dispensaries)

**Q2 2025:** - Expand to 500 validator locations - Target 1M user validations - Launch cannabis retail partnerships (3-5 dispensaries/delivery services)

**Q3-Q4 2025:** - Geographic expansion (focus: legalized cannabis states) - Enterprise adult platform partnerships (target: 2-3 major platforms) - Achieve 10M+ total validations

**2026:** - International expansion (UK, Canada, Netherlands) - Additional verticals (reproductive health, alcohol e-commerce) - Target: 50M+ annual verifications

## THE ASK

**Seeking: \$2.5 million USD Seed Round**

**Use of Funds:**

CATEGORY	ALLOCATION	PURPOSE
Engineering & Product	40% (\$1.0M)	iOS development, API scaling, security audits
Go-To-Market	35% (\$875K)	Sales team (2 AEs), marketing, pilot partnerships
Operations & Legal	15% (\$375K)	Regulatory compliance, IP protection, finance/HR
Validator Network Growth	10% (\$250K)	Validator onboarding incentives, location expansion

**Projected Milestones (18-Month Runway):**

- 50+ enterprise customer contracts signed
- 10M+ user verifications processed
- 2,000+ validator locations operational
- \$150K monthly recurring revenue (ARR: \$1.8M)
- Series A positioning (target: \$10M raise, \$40M pre-money)

## INVESTMENT HIGHLIGHTS

- 1. Massive, Growing Market:** \$2.22B → \$5B (2025-2033)
- 2. Proven User Demand:** 47% traffic abandonment demonstrates acute privacy pain point
- 3. Defensible Technology:** Zero-PII architecture cannot be replicated without full system redesign
- 4. Regulatory Tailwinds:** Age verification mandates expanding globally (UK, EU states, U.S. states)
- 5. High-Margin SaaS Economies:** 92-95% gross margins, LTV:CAC >10:1
- 6. Multiple High-Value Verticals:** Adult content, cannabis, alcohol, reproductive health
- 7. Experienced Founding Team:** [Team credentials to be added]

## WHY NOW?

Three converging forces create a unique market window:

- 1. Regulatory Enforcement (2025)**
2. UK Online Safety Act actively enforced (July 2025)
3. U.S. state laws proliferating (Louisiana, Montana, Arkansas, others)
4. EU Digital Services Act age verification requirements
- 5. User Privacy Awareness Peak**
6. \$27.2B consumer fraud losses (2024)
7. Major biometric database breaches (India Aadhar: 1.1B records)
8. Post-Dobbs reproductive privacy concerns
- 9. Technical Enablement**

10. Secure Enclave/TEE now ubiquitous (95%+ smartphones)
11. Hardware attestation standards mature
12. Zero-knowledge proof cryptography practical

**The market needs Lockette's solution NOW. The technology is ready NOW. The regulatory environment demands compliance NOW.**

**This is the moment.**

---

LOCKETTE™ CONFIDENTIAL  
© 2025 Lockette. All Rights Reserved.

For inquiries: [contact information]

---

---

## **APPENDIX: SOURCES & DATA**

All claims in this document are supported by: - Implementation architecture (technical documentation on file) - Public market research (Verified Market Reports, 2025) - Government/regulatory reports (Ofcom UK, BBC News) - Industry analysis (Similarweb, ITRC, cybersecurity firms)

**No projections or claims are made without documented basis.**

For full citations and supporting documentation, see accompanying Market Research & Analysis document.