PassLeak

Personal data-leak monitoring + breach-response playbooks. Have I Been Pwned is free but inert; Aura/LifeLock are $200/year bloatware. PassLeak is structured + actionable at $7/month.

Category	Set 6 · Consumer & Family
Customer	Privacy-conscious consumers wanting structured monitoring + response when their data appears in breaches
Monetisation	$7/mo Solo · $12/mo Family (4 users) · $19/mo Pro (with dark-web identity monitoring + recovery support)
Build effort	Med
Plan version	v1.0 — 2026-05

Executive Summary

PassLeak is personal data-leak monitoring + breach-response. The wedge: Have I Been Pwned (free) provides historical leak data but is inert — users check, see they've been in breaches, do nothing because the response is unclear. Aura + LifeLock + Norton 360 charge $150-300/year for bloated identity-protection packages bundling features most users don't need. PassLeak is focused + actionable at $7/mo: continuous monitoring + per-breach structured response playbooks + password-change automation + identity-monitoring at high-risk moments.

Year-1 target: 5,500 paying subscribers generating ■2.5 crore annual revenue against ■40 lakh costs. Cash-positive month 3.

The Problem

Personal data breaches are continuous + cumulative. The average internet user has had email + password combinations exposed in ~7-12 breaches by 2026. Most users either: (1) don't know about breaches affecting them, (2) know via Have I Been Pwned but do nothing because response is unclear, (3) pay $150-300/yr for Aura/LifeLock/Norton bloated packages that bundle 12 features for 1 needed.

The structured response gap. When breach occurs: identify which specific accounts are compromised + change passwords in priority order (banks first + email second + then everything else) + check for unauthorised account access + monitor for downstream fraud + know when to escalate to credit-freeze. This sequence is poorly understood by typical users + poorly served by inert HIBP or bloated competitors.

The Solution

PassLeak structured around continuous monitoring + per-breach action. Onboarding: connect monitored emails (typically 1-4 per user) + phone numbers + optionally credit cards (for transaction monitoring).

Continuous monitoring: real-time leak detection across HIBP + dark-web monitoring + breach-disclosure aggregation.

Per-breach response playbook: when user's data appears in new breach, structured playbook delivered — specific accounts affected + priority password-change order + step-by-step instructions for each account + automated password-change links where supported.

Password-change automation: integration with major service password-change APIs (where available) to one-tap-change instead of manual navigation.

Identity monitoring at high-risk moments (Pro tier): when major breach exposes financial data, escalated identity monitoring + credit-freeze guidance + recovery support.

Three structural differences. First, actionable response (not just notification). Second, focused product (no bundled bloat). Third, fair pricing ($7 vs. $250/yr Aura).

Market Opportunity

Privacy-conscious consumer segment globally: ~50-80M who would pay $7-19/mo for focused breach-response. Growing as breach frequency rises.

At blended ARPU of $108/yr, SAM is $5-9B globally. Realistic 4-year capture: 0.02-0.06% = $1-5.4M ARR.

Adjacent expansion. Year 2: family-tier expansion (kids' digital safety + parent breach monitoring). Small-business tier (sole proprietors needing breach monitoring for business email).

Target Customer

Primary persona: a 38-year-old IT professional aware of digital security + uses HIBP occasionally + frustrated that response is manual. Will pay $7/mo Solo.

Secondary persona: a 42-year-old parent of 2 teenagers wanting family-wide monitoring. Will pay $12/mo Family.

Tertiary persona: a 51-year-old previous identity-theft victim wanting comprehensive monitoring + recovery support. Will pay $19/mo Pro.

Product

Onboarding: monitored emails + phone numbers + optional cards.

Continuous monitoring: real-time leak detection across data sources.

Per-breach response playbook: structured + priority-ordered action plan.

Password-change automation: integration with major services.

Identity monitoring (Pro): escalated when high-risk breach detected.

Family tier: 4-user shared dashboard.

Technical Architecture

Frontend: Next.js + React Native mobile + Chrome extension.

Backend: Python on Hetzner cloud, Postgres.

Data sources: HIBP API + dark-web monitoring partners + breach-disclosure aggregation.

Password-change automation: per-service integration code.

Payments: Stripe + Razorpay.

Compliance: SOC2 + strong privacy posture.

Business Model & Unit Economics

Three tiers. Solo $7/mo or $69/yr. Family $12/mo or $119/yr (4 users). Pro $19/mo or $189/yr (Solo + dark-web monitoring + recovery support).

Conversion: 14-day trial converts at 14%. Distribution: 60% Solo, 25% Family, 15% Pro. Monthly churn under 4%.

Gross margin: 80%. Costs: data-source API fees + dark-web monitoring partner + infrastructure.

LTV: $84 × 22 mo = $185 (Solo); $144 × 26 mo = $374 (Family); $228 × 30 mo = $684 (Pro).

Unit Economics (Year-1 base case)

Year-1 paying subscribers	5,500
Blended ARPU	$130/year
Year-1 revenue	$300,000 (~■2.5 crore)
Gross margin	80%
CAC	$24
Payback	2.6 months
Year-1 all-in costs	~■40 lakh
Year-1 net contribution	~■1.6 crore

Go-to-Market

Channel 1 — Privacy-community organic (40%): r/privacy + privacy-creator partnerships + privacy-focused podcasts.

Channel 2 — Content + SEO (30%): substantive content on breach-response + digital security + password hygiene.

Channel 3 — Post-breach trigger marketing (20%): targeted advertising following major publicised breaches.

Channel 4 — Paid acquisition (10%).

Roadmap (first 12 months)

- Month 1-3: MVP with monitoring + per-breach response + Solo tier. 400 subscribers.
- Month 4-5: Family tier + password-change automation, 1,400 subscribers, ■4 lakh MRR.
- Month 6-8: Pro tier with dark-web monitoring + recovery support, 3,000 subscribers.
- Month 9-10: Chrome extension + mobile apps + expanded integrations, 4,500 subscribers.
- Month 11-12: 5,500 subscribers, ■2.5 crore annualised.

Key Risks

- Data-source partner pricing changes: dark-web monitoring partner cost can rise. Mitigated by multi-source + ability to scale-back coverage if needed.
- Aura / LifeLock pricing aggression: incumbents could compress prices. Mitigated by focused product + transparency.
- Breach-response liability: bad guidance could compound harm. Mitigated by conservative recommendations + professional indemnity + escalation pathways.

- Slow conversion in consumer-privacy segment: privacy-paranoid users are also paid-tool-skeptical. Mitigated by free trial + transparent pricing + clear value.
- Free HIBP competition: many users won't pay when free alternative exists. Mitigated by response-action differentiation that HIBP doesn't provide.