
VALIDECK
Search with Confidence

Mission & Vision

Vision:

Build a **privacy-first transaction data infrastructure** for commerce, where transaction records are **customer-controlled, secure, and interoperable**.

Long-term: *Embed ValiDeck's patented tokenization architecture into payment acceptance environments, powering a global privacy-first commerce network and search built on pseudonymous customer transaction records and reviews.*

Mission:

Develop a privacy-first data infrastructure that enables:

- **Customers** to capture and manage their transaction records in a secured repository under their control;
- **Businesses** to run privacy-compliant loyalty programs without collecting personal identifiers.
- **Enterprises** to use verified, privacy-protected transaction data to improve decision-making and customer engagement.

Current Focus: *building the reference implementation (a payment transaction simulator, PoS integration layer, and Loyalty Server) toward enterprise pilot readiness.*

Market / Problem



Customer transaction records are scattered and siloed. A few large merchants, such as Amazon, keep purchase histories in the customer's platform account; most businesses hand over a copy as an email or printed invoice. Every copy lives in a separate silo, tied to the customer's identity, in a format the customer cannot aggregate or reuse.



There is no widely adopted infrastructure today for customers to retain and reuse transaction records pseudonymously across merchants. Conventional anonymization of granular transaction data can remain vulnerable to re-identification, so in practice records are often either deleted or kept in personally attributable form.

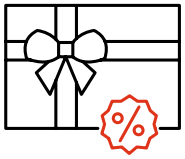


Customers lack a unified, reusable record of what they purchase across merchants, limiting their ability to analyze spending, plan purchases, or derive value from their own transaction data.



Businesses have limited visibility beyond their own customer relationships and typically rely on identity-based profiles to personalize offers and run loyalty programs.

Market / Problem



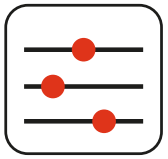
The loyalty management software market is estimated at USD 16.4 billion in 2026, projected to reach USD 32.5 billion by 2031 at a ~15% CAGR (Mordor Intelligence, 2026).



In the absence of a privacy-compliant model for reuse, merchants resort to identity-based loyalty programs to extract value from transaction data. These programs require customers to acquire a merchant-branded loyalty card or share their email/mobile number with the merchant during registration.



Identity-based loyalty programs increase the amount of personal information merchants must collect and protect, increasing privacy and security exposure.



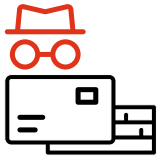
Most loyalty systems do not bind customer reviews to reusable, verified line-item transaction attributes.

Solution: PCX-based Loyalty Program



Protects

Personal and confidential information of customers

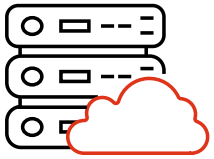


Allows

Customers to join participating loyalty programs pseudonymously

PCX

Privacy-Compliant eXtensible



Stores

Line-item customer transaction records without personal identifiers



Unlocks

Cross-merchant spending insight

Note:

1. The PCX panel above links to the PCX White Paper, which describes the protocol in full. The underlying tokenization technology and the PCX-based loyalty program are documented in more detail on the ValiDeck website.
2. The core token pipeline is protected by patents granted in the United States (US12125054B2 and US12749086B2), Australia, and India. The newer U.S. continuation claims a PoS-linked contextual review-form workflow. Related applications remain under examination in Canada, Europe and China; separate U.S. and European record-architecture applications filed in 2026 remain pending.

Joining the PCX-based Loyalty Program

01

GENERATE KEY PAIR



Customer generates a cryptographic public-private key pair on their personal device.

02

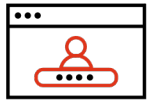
REQUEST KEY ATTESTATION



Customer requests their card issuer to attest the public key against its KYC records.

03

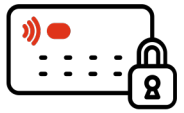
SUBMIT ATTESTED KEY



Customer submits the attested public key to the PCX Platform. The PCX Platform creates a customer account using the attested key.

04

REQUEST & REGISTER TOKEN



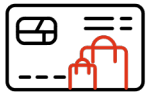
Customer requests their card issuers to generate a token number for each issued card. Customer registers the tokens in their PCX Platform account.

Note: The PCX Platform does not require the customer to disclose personal or confidential information during account creation. No email addresses, phone numbers, or payment card details are shared with the PCX Platform.

Running the PCX-based Loyalty Program

01

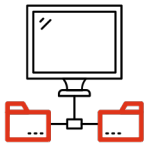
ACCEPT PAYMENT



Customer makes payment using any tokenized card. No loyalty card, app, or personal identifier is required at the point of sale.

02

TRANSFORM CUSTOMER TRANSACTION



Merchant PoS links the token to the transaction record and sends both to the PCX Platform, which creates the domain-specific records.

03

RECORD CUSTOMER TRANSACTION



The PCX Platform stores each domain record separately. Customer identity is not combined with reusable transaction history. Card tokens map to pseudonyms, not direct identifiers.

04

REWARD CUSTOMERS

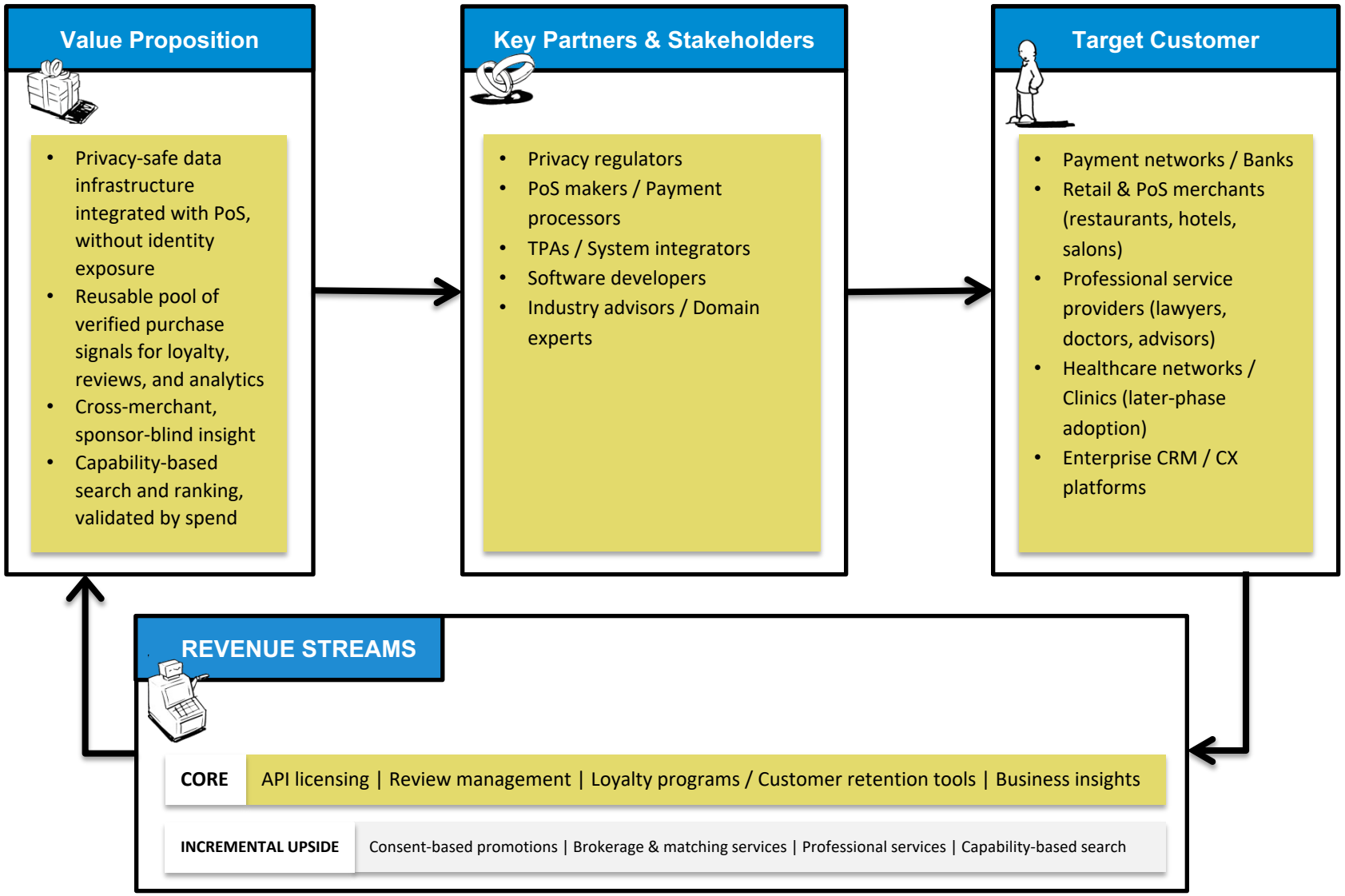


Enrolled merchants reward on their own and partner-network sales. Cross-merchant, sponsor-blind rewards run on synthetic records.

Competitive Advantage

Feature	Fetch Rewards	Ibotta	Fidel API	ValiDeck
Pseudonymous Enrollment Note: A platform qualifies for the pseudonymous enrollment label if a customer can enroll and transact without disclosing personal identifiers (name, email, phone, or card number) with records linked to a customer-controlled pseudonym that persists across merchants rather than to a real-world identity.	No	No	No	Designed
Customer-controlled Data Aggregation Note: When a customer joins a merchant loyalty program, the transaction records are stored on the merchant's platform. A platform qualifies for this label only if the customer's copy of the record is under their control: portable, deletable, and not monetized without consent. Receipt-scanning apps that hold and monetize the customer's copy without that control do not qualify.	No	No	No	Designed
Sponsor-Blind Cross-Merchant Rewards Note: A merchant in a loyalty program sees a customer's spending only at its own store, or within a partner network. A platform qualifies for the sponsor-blind cross-merchant rewards label if a sponsor can reward purchases made at unaffiliated merchants, without ever seeing or singling out the customer.	No	No	No	Designed
Line-item Transaction Details Captured Directly from PoS Note: To understand exact spending behavior (e.g., $100 on Nike sneakers), line-item transaction details must be available. A platform qualifies for this feature when granular transaction details are captured directly from the merchant transaction flow and can be aggregated without receipt scanning or manual entry.	No	No	No	Designed

Business Model



Note: Information on revenue streams is described in more detail in the product development strategy.

Team & Ask

Founder

Alok Narula – Product, IP, and System Architecture
LinkedIn: https://www.linkedin.com/in/aloknarula

Support

- IP Education and Funding: Intellectual Property Ontario (IPON)
- Talent Search, Networking Events, and IP Strategy: Communitech

Seeking: US$1M Pre-Seed Round, deployed in staged tranches over 24 months to validate the PCX architecture and produce independently reviewable evidence:

- $700K – Engineering & Product Build
- $200K – Partner Integration & Testing
- $100K – Compliance & Operations

Outcome: Independently reviewable PCX prototype and partner-ready evidence package within 24 months → prepared for Phase II live partner integration and controlled commercial pilots.

Non-Dilutive Funding: IPON Tier 2 client, eligible for up to **CAD $300K lifetime** in cost-shared IP funding for patent prosecution, approved per statement of work.
SR&ED Potential: Canadian R&D activities will be documented for potential SR&ED tax-credit claims, subject to eligibility.

Roadmap & Milestones (Phase I)

1-6 Months

Platform Design

- Translate the patented architecture into an implementation design
- Build a virtual PoS Simulator for multi-merchant testing
- Implement secure enclave for privacy-preserving transaction processing

6-9 Months

Backend Development

- Implement Loyalty Server backend linking tokens with transaction records
- Automate encryption validation and performance benchmarking
- Prepare SR&ED technical narrative and evidence documentation

9-12 Months

Analytics & Compliance

- Deploy BI dashboard for cross-merchant analytics
- Prepare PIPEDA / GDPR privacy-readiness memo and independent audit plan

12-24 Months

Reference Integration

- Finalize UI/UX, investor demo, and independent privacy/security review
- Build PoS SDK and reference connector, validated against the transaction simulator
- Demonstrate tokenized reference integration designed for GDPR readiness