PCX — Because Privacy and Commerce Must Coexist

A privacy-compliant protocol for identity-decoupled records

In brief: PCX is a proposed open protocol for representing completed commercial transactions in a form that can be stored, linked, and reused for loyalty, analytics, and search without carrying the identity of the person behind them. It is intended to replace today's forced choice between deleting data to protect privacy and retaining identity-bearing records that create liability. This paper sets out why the current model fails, what a solution must do, what changes once the record is decoupled from identity, and how ValiDeck intends to demonstrate it, beginning with customer-transaction records (PCX-CTR).

When you buy a prescription, a train ticket, groceries, insurance, or a service, the evidence of that purchase is often stored across systems you do not control. These traces of your real-world activity live in silent archives: banks, merchants, loyalty systems, insurers, inbox receipts. Each fragment may be linked to your identity, yet you do not possess a complete record of the transactions associated with you. Instead, portions of that information can be aggregated by institutions and data intermediaries to reconstruct and commercialize your purchasing behavior.

This quiet asymmetry has become one of the defining paradoxes of modern commerce. The more digital and efficient the economy becomes, the less control individuals have over the records generated by their participation in it. Privacy becomes a luxury; usability becomes a compromise; and personal data becomes both a liability and a bargaining chip. This situation was never the product of a deliberate decision. It persists because no widely adopted protocol unites privacy, utility, and analytical value at the foundational layer of data representation.

PCX, **the Privacy-Compliant eXtensible protocol**, is a proposed method for capturing real-world activity in structured records that preserve utility without embedding identity. It redesigns the structure of the record itself, ensuring that continuity, analysis, and reuse do not require surveillance, correlation, or trust in institutional restraint.

Why the Current Model Is Failing

The modern financial and retail ecosystem attempts to protect privacy by withholding detail, by deleting information, limiting retention, and prohibiting storage when identity might be inferred. This is not privacy-by-design; it is privacy achieved through strategic blindness. The system throws away value because it cannot encode it safely. What remains is an ecosystem that constantly asks individuals to trust institutions, to permit data collection, to "consent" to tracking, or to negotiate against systems they did not build and cannot influence.

Meanwhile, businesses stand in a contradictory position. To understand customer behavior, prevent fraud, tailor offers, or operate efficiently, they often rely on personal identifiers, not because they prefer surveillance, but because identity remains the dominant bridge between events. Loyalty programs, data brokers, clean rooms, and cross-merchant tracking all exist for the same reason: without a safe alternative, identity becomes the glue that binds the digital economy together.

Attempts to mitigate risk (hashed identifiers, token vaults, clean rooms, encrypted silos) can shift exposure from one surface to another. However, the dependency remains intact. Identity continues

to serve as the connective tissue of the system, and regulatory liability scales with every retained record.

When detail must be deleted to preserve privacy, the economy is forced to operate with artificially constrained visibility. Planning, procurement, forecasting, and logistics must then proceed with incomplete evidence, not because the data does not exist, but because it cannot be reused safely.

The deeper issue is that the current system externalizes the cost of its own limitations. Individuals lose agency over the records that describe their lives, governments must regulate behavior they cannot observe, and businesses spend substantial resources reconstructing patterns that already exist somewhere in fragmented form. These inefficiencies are not accidental; they are structural consequences of binding continuity to identity. At some point, this contradiction must be resolved.

The history of digital standards such as HTTPS, EMV, and TCP/IP shows that when structural tension becomes costly enough, common standards can emerge. **A protocol for identity-decoupled records is therefore more than a theoretical improvement; it is a plausible infrastructural requirement.**

What a Protocol Must Solve

To succeed, a protocol must eliminate the contradiction at its root. It must make it possible to store, link, and reuse records without embedding direct identity or a platform-visible mapping back to the person. In PCX, records carry pseudonymous continuity identifiers rather than direct personal identifiers: a record can be stored, linked, and reused without revealing, on its own, the person behind it.

Such a protocol must allow a person to accumulate years of records across domains without revealing themselves. It must allow a small business to understand demand without assembling behavioral profiles. It must allow regulators to enforce compliance without penetrating the lives of citizens. Most importantly, it must reflect real-world activity as it actually unfolds: fluidly, continuously, and across domains.

How PCX-CTR does this, concretely: PCX separates the customer's identity from the transaction record before the record enters the PCX environment. When a customer makes a payment, the customer's card number and identity do not become a part of the transaction record held by the PCX Platform. Instead, the payment card issuer represents the card account using a token — a substitute value that can be used to process and associate the transaction without exposing the underlying card number. PCX uses this protected reference to associate the completed transaction with a persistent pseudonymous customer reference.

The transaction record is therefore linked to a pseudonym rather than to the customer's name, email address, or other direct identity. The bank retains the relationship between the payment account and the customer, while the PCX Platform holds the transaction record against the pseudonymous reference. Neither side, acting alone, has both the customer's identity and the corresponding PCX transaction history; reconnecting the two would require an authorized process involving both sides.

This separation also supports loyalty without creating a conventional identity-based customer profile. When a customer joins a merchant's loyalty program, the merchant can recognize and reward that customer based on transactions with that merchant, without gaining access to purchases made elsewhere. PCX is also being developed to support cross-merchant programs through separate customer, merchant, and synthetic transaction records. In that model, a rewards sponsor can define a

policy that is evaluated against privacy-preserving transaction data, while the customer's identity and broader transaction history remain undisclosed.

PCX is therefore not a single schema but a family of cross-domain formats, each representing a different domain of real-world activity in the same identity-decoupled structure. ValiDeck's initial implementation targets only PCX-CTR; the others form a staged, longer-term roadmap rather than parallel builds:

- **PCX-CTR** — customer transactions: line-item records of what was bought, where, and at what price
- **PCX-AUTO** — automotive lifecycle events: purchase, servicing, ownership, and resale history
- **PCX-HLTH** — healthcare and pharmacy events: prescriptions, procedures, and dispensing records
- **PCX-TRAVEL** — travel and mobility events: bookings, itineraries, and journeys
- **PCX-INSURANCE** — insurance policy and claims events: coverage, premiums, and settlements

People do not live within institutional silos. A medical event may affect insurance; travel reshapes consumption; a vehicle's history affects its resale value; and a single purchase can touch several of these at once. A protocol that hopes to represent real-world activity faithfully must model these interdependencies, not reinforce the artificial divisions of legacy systems.

These properties define PCX not merely as a data format but as a constitutional framework for long-term privacy, neutrality, and interoperability. They ensure that PCX remains resistant to commercial capture, adaptable across decades of technological change, and stable enough to serve as an infrastructural foundation.

A protocol intended to serve as the substrate of the digital economy must also remain durable over time. Authentication will change; payment instruments will evolve; regulatory expectations will adapt, but the representation of an event must remain stable. **PCX treats these records not as data exhaust but as long-lived, reusable assets whose value compounds with continuity**.

The technologies underlying PCX — cryptographic tooling, tokenization, trusted execution, and privacy regulation — have existed in different forms for decades. What has changed is their maturity and convergence. PCX is possible now because these capabilities can be combined into an implementable privacy-preserving architecture in a way that was far less practical a decade ago.

What Changes Once the Record Is Decoupled from Identity

Decoupling identity from the record does more than improve privacy; it restructures the informational logic of the entire economy. Trust shifts from institutional assurances to structural guarantees embedded directly in the record. Privacy need no longer be traded off against utility. Data becomes far less of a liability. Continuity no longer requires exposure.

Businesses gain the ability to understand customers without watching them. Governments gain mechanisms for oversight without intrusion. Healthcare systems can measure outcomes without reconstructing patient lives. Merchants can evaluate demand without building surveillance-driven behavioral models. Citizens gain the ability to possess, reuse, and transmit the history they generate everywhere they go.

The competitive landscape also changes. When identity is decoupled from the record, the advantage accumulated by incumbents through proprietary behavioral profiling can be reduced. Small firms can

gain more equal access to verified signals; competition shifts from data extraction to service quality, relevance, and design.

Perhaps the most subtle transformation is cultural. When privacy is preserved by design, people stop interacting with the digital economy defensively. Participation need not expose them in the same way. Trust becomes a structural feature, not a negotiated concession. A privacy-compliant economy is not only more efficient; it is more human.

By restoring the ability to reuse transaction data without exposing the person, **PCX turns transaction records from a compliance liability into a reusable information asset.** Recorded consumption becomes a reliable signal rather than a by-product, allowing production, pricing, inventory, and capital deployment to follow what the economy is actually doing instead of what models predict.

From Implementation to Standardization

ValiDeck is building a reference implementation of the PCX protocol, beginning with PCX-CTR. In this architecture, pseudonymous PCX-CTR records would be stored in a logically centralized repository under regulatory oversight rather than corporate ownership, with control designed to remain distributed across lawful custodians, so that centralization does not become data capture and the repository can serve as a public good.

Standardization will not occur through mandate alone, but through demonstration. As PCX-based systems show that privacy and utility can reinforce one another, adoption becomes a rational choice rather than a regulatory obligation. Merchants benefit from accurate analytics that do not expose customers. Regulators gain trustworthy, non-intrusive auditability. Developers gain a neutral substrate upon which to innovate.

Such a system was not feasible in the past. Only with the alignment of regulatory frameworks, cryptographic tooling, and distributed governance models has identity-decoupled continuity become operationally viable at scale. As PCX matures and early implementations demonstrate real-world value, its role shifts from a technical innovation to an institutional framework. The approach has been specified at the architectural level, and the patents already granted protect the token-based capture-and-aggregation pipeline. The privacy-preserving record architecture that builds on that pipeline, the decomposition into customer, merchant, and synthetic records described before, is the subject of separate applications now pending. This creates the conditions for PCX to evolve from an architectural insight into a public infrastructure layer.

The structure of the economy is shaped by the structure of its records. If those records depend on identity, surveillance pressure becomes difficult to avoid. If they do not, privacy becomes the foundation upon which intelligence, competition, and innovation can grow. PCX proposes a future in which data derived from real-world activity is both useful and low-risk, a future in which the digital economy can be efficient without being extractive, and innovative without being intrusive.

The PCX protocol itself is not yet a ratified industry standard, but it is a proposed interoperability layer designed to demonstrate that privacy-compliant record reuse can be achieved with today's technology. As adoption grows, regulatory cooperation may crystallize it into a recognized standard across jurisdictions. ValiDeck is developing a companion PCX Architecture document that expands these principles into the Custodian, Platform, and Governance layers and describes the operational and cryptographic design required for implementation.