

PRD - Personal Cards: User Account

Status	Aligned	Author(s)	Fernando Barros
Last Updated	Mar 20, 2026	Approver(s)	João Caetano (Caetano) Manuella Valença
Created	Mar 20, 2026	Channel	#team-b2b #faststore

Introduction

The B2B Buyer Portal introduces a distinction between personal payment cards, owned exclusively by the individual shopper, and shared cards owned by a contract or organizational unit. Currently, the User Account lacks a dedicated "My Cards" area, forcing all card management to occur within the Checkout flow. This gap prevents the enforcement of this distinction, leading to a lack of governance over personal payment methods and operational risks for organizations.

This PRD defines the business rules governing how the User Account handles personal cards and shared cards, how access is gated by user type and role, and what actions are permitted under each condition. It does not cover Checkout behavior, platform card validations, PCI/GDPR compliance, or mobile design. The goal of this document is to align product, design, and engineering stakeholders on the intended long-term behavior of the User Account Personal Cards area.

TL;DR: Enforce role-based access for B2B buyers to manage personal payment cards in the User Account and protect shared organization cards as read-only.

Product/Area: B2B Buyer Portal / User Account

Focus Task: Define and enforce access rules for personal payment cards in the User Account, with clear separation from shared organization cards

Persona: B2B Buyer (individual shopper, with or without a Unit/Contract association)

Working title/Commercial Name: Personal Cards – User Account

Value headline: B2B buyers gain controlled, role-aware access to manage personal payment cards from the User Account, with a clear and enforced boundary between personal and shared organization cards.

Mini-Press Release: B2B buyers can now manage their personal payment cards directly from the User Account, with full control over adding, and deleting. Buyers associated with a Unit or Contract see only the card management capabilities they are authorized to use, based on roles assigned by their organization. Shared cards remain visible as a read-only reference but are fully protected from accidental modification in the User Account.

Context

Problem 1: All Buyers Lack a Dedicated Card Management Area in the User Account (My Cards)

The User Account currently lacks a dedicated area (My Cards) for buyers to manage their payment cards, forcing all card management operations (view, add, edit, delete) to be performed exclusively within the Checkout flow. This restriction applies universally to all buyers, regardless of their association with an Organizational Unit/Contract (B2B) or their status as an unaffiliated shopper (B2C). This deficiency limits the buyer's ability to control their saved payment methods, creates a dependency on transactional contexts, and undermines the expected self-service capabilities of the User Account.

In practice, this includes:

- A buyer cannot view or manage their saved personal cards until they enter the transactional context of the Checkout flow.
- A buyer (B2B or B2C) must wait until a purchase attempts to add and delete a saved payment card.

Business impact:

- Buyer friction and churn increase due to the inability to manage essential profile data (payment methods) in a dedicated, non-transactional area.
- Self-service is undermined, as buyers must engage with the high-context Checkout flow for simple card administration.
- The platform experience for managing saved data is inconsistent for both B2B and B2C buyers.

Out of scope

- Checkout payment method selection, card prioritization, or any payment behavior at the time of purchase
- Platform card validations (CVV, tokenization, expiry rules, fraud signals)
- Organization Account card management — creation, editing, or deletion of shared (contract/unit) cards
- Buyer Portal conversion flow and ConvertProspect integration
- Status history or audit log for card management actions
- Interim UI surfaces prior to a full MyCards implementation in the User Account
- There is no edit / modify existing cards.

Requirements

Phase 1 : Access Governance and Card Type Separation

Value delivered: The User Account enforces a clear, role-aware boundary between personal and shared cards, allowing authorized buyers to manage their personal payment methods while protecting shared contract cards from unauthorized modification.

Must have ▾

[REQ-1] Personal Card Ownership Isolation

I, as a B2B buyer, want my personal cards to be exclusively owned by my User Account and invisible as editable resources to Organization Account administrators, so that my personal payment data is private and distinct from shared contract payment methods.

Acceptance criteria:

- The system must treat personal cards as exclusively owned by the individual shopper's User Account.
- The system must not expose personal cards as editable or viewable resources in the Organization Account.
- The system must not allow Organization Account administrators to view, edit, or delete a user's personal cards.

[REQ-2] User Type Detection and Access Gate

I, as a B2B buyer associated with a Unit or Contract, want the Personal Cards area to be accessible only if my assigned roles include the useAdHocCard permission, so that my organization's payment governance policies are enforced by the platform without requiring manual controls.

Acceptance criteria:

- The system must detect Unit/Contract association by the presence of a unitId field in the user's session token.
- The system must hide or disable the Personal Cards menu entry for users who have a unitId but do not hold the useAdHocCard permission.
- The system must grant access to the Personal Cards area for users who hold the useAdHocCard permission, regardless of Unit association.
- The system must allow users without a unitId (unaffiliated buyers) to access the Personal Cards area without any additional permission requirement.

[REQ-3] Full Personal Card Management for Eligible Users

I, as a B2B buyer with access to the Personal Cards area, want to view, add, and delete the personal card, so that I can manage my personal payment methods independently and without administrative intervention.

Acceptance criteria:

- The system must allow eligible users to view all personal cards saved to their User Account.
- The system must allow eligible users to add a new personal card to their User Account.
- The system must allow eligible users to delete a personal card from their User Account.

[REQ-4] Shared Card Read-Only Visibility

I, as a B2B buyer, want to see which shared cards are available to me as a read-only reference in the User Account, so that I understand my available payment options without the risk of accidentally modifying shared payment methods.

Acceptance criteria:

- The system must display shared cards available to the user in the User Account as read-only records.
- The system must not allow edit or delete actions on shared cards from the User Account.
- The system must surface a descriptive business-level message when a user attempts to edit or delete a shared card: "Shared cards can only be managed from the Organization Account."

[REQ-5] Visual and Behavioral Distinction Between Card Types

I, as a B2B buyer, want personal cards and shared cards to be clearly identifiable as distinct types in any User Account view that lists both, so that I do not confuse my personal payment methods with contract-managed payment methods.

Acceptance criteria:

- The system must visually distinguish personal cards from shared cards in any combined listing within the User Account (for example, through a label, badge, or icon).
- The system must ensure the shared card area, when present, is presented in a read-only state with no edit or delete affordances available.

[REQ-6] Access Denial for Ineligible Unit-Affiliated Users

I, as a Buyer Portal administrator, want the Personal Cards area to be hidden from users who belong to a Unit but do not hold the useAdHocCard permission, so that payment method governance is enforced at the platform level without requiring manual intervention.

Acceptance criteria:

- The system must hide the Personal Cards menu entry or area for users who have a unitId in their session token and do not hold the useAdHocCard permission.
- The system must not surface a generic error to ineligible users — the Personal Cards area must simply not be accessible or visible to them.

[REQ-7] Personal Card Data Protection (PCI/GDPR Alignment)

I, as a platform, want to ensure that all personal card data stored and processed within the User Account is handled in compliance with applicable security and privacy standards, such as PCI DSS and GDPR, so that we maintain certification and protect customer data integrity.

Acceptance criteria:

- The system must ensure that the storage, processing, and transmission of personal card data adhere to the latest PCI DSS requirements.
- The system must ensure that the collection and management of personal payment data complies with relevant privacy regulations, including GDPR principles (e.g., data minimization, purpose limitation).
- The User Account card management area must only display masked Personal Account Numbers (PANs), consistent with PCI DSS display requirements (e.g., first six and last four digits).

Unsolved Questions / Discovery Areas

FAQs

What problem does this PRD solve?

This PRD solves the lack of a dedicated card management area in the User Account, which currently forces buyers to manage payment methods exclusively during Checkout. By introducing the "My Cards" interface, the platform can finally enforce the necessary distinction and governance between personal and shared cards, ensuring that individual shoppers can manage their own data while protecting organizational payment methods from unauthorized modification.

Does this PRD change how buyers select payment methods at checkout?

No. This PRD is scoped exclusively to the User Account; the buyer's personal profile area. Checkout payment method selection, card prioritization, and any payment behavior at the time of purchase are explicitly out of scope and will be addressed in separate product work.

What is the useAdHocCard permission and who manages it?

useAdHocCard is the platform permission that grants access to personal card management for users associated with a Unit or Contract. If a unit-affiliated buyer does not hold this permission, the Personal Cards area is not visible or accessible in the User Account. The permission is assigned

and managed by Buyer Portal administrators through platform roles (for example, Personal Cards User) and the platform API.

Why are buyers without a Unit treated differently from unit-affiliated users?

Buyers without a Unit association are individual shoppers not governed by an organizational contract. For these users, personal card management is equivalent to standard consumer card management. No organizational policy applies, no unitId is present in their session token, and no additional permission is required to access the Personal Cards area.

Appendix

Related Assets

 [User Roles & Permissions](#)