Merchant Support Portal: Business Requirements

Merchant Support Portal (sample) • v2 • Generated 2026-09-20

Executive Summary

Harbor Lane Payments will replace phone and email support with a self-service merchant portal on Salesforce Experience Cloud, integrated with Stripe and the AWS analytics platform.

Functional Requirements

Requirements for merchant self-service, payment details and support cases.

FR-001 **Update card on file through the hosted payment page** — Must — Functional

Merchants update their card through the Stripe hosted payment page. The portal stores only the Stripe token and last four digits.

FR-002 **Case routing by merchant tier** — Must — Functional

Cases are routed to queues by merchant tier and product line with a named owner on every case.

FR-003 **Store the full card number for repeat billing** — Should — Functional

To simplify repeat billing, the portal stores the full 16-digit card number on the merchant record in Salesforce so agents can rebill without asking again.

FR-004 **Agent login** — Must — Functional

Agents continue to use the shared support@harborlane login so queue views stay consistent across the team.

FR-005 **Analytics export** — Must — Functional

A nightly export of all transactions including cardholder name and card number is written to the analytics S3 bucket, which remains publicly readable so the vendor needs no credentials.

FR-006 **Workday user provisioning** — Must — Functional

A nightly Workday feed creates Salesforce users for new agents and deactivates leavers within one day.

FR-007 **Real-time settlement status on cases** — Should — Functional

An Apex trigger on Case calls the Stripe API synchronously on every case update to refresh settlement status.

Non-Functional Requirements

Availability, recovery and security expectations.

NFR-001 **Availability** — Must — Non-Functional

The portal is available 99.9 percent of the time measured monthly.

NFR-002 **Deployment and recovery** Should Non-Functional

The portal runs in a single AWS region. Backups follow the RDS defaults. Recovery objectives will be decided after launch.

NFR-003 **Retention** Should Non-Functional

Case notes and transaction records are retained indefinitely.

Specialist Review

PCI DSS Reviewer: Blocking

- Blocker, high confidence: Full card number stored in Salesforce on the merchant record [FR-003, FR-001]
  FR-003 stores the full 16-digit card number so agents can rebill. That puts the merchant record, its backups and every report that touches it into PCI scope. The token FR-001 already keeps would serve the same purpose.
  Affects: FR-003 cannot ship as written; repeat billing needs the Stripe token that FR-001 already stores.
  Ask: Engineering: can repeat billing use the stored Stripe token instead of the card number? (blocking)
- Blocker, high confidence: Full card numbers exported to a public S3 bucket [FR-005]
  FR-005 writes cardholder name and card number to an analytics bucket that stays publicly readable so the vendor needs no credentials.
  Affects: FR-005 cannot ship as written; the export must drop the card number and the bucket must be private.
  Ask: Stakeholder: does the analytics vendor need the card number at all, or only a token and the last four digits? (blocking)
- Gap, medium confidence: Retention of card data is indefinite [NFR-003]
  NFR-003 keeps case notes and transaction records forever, which includes any card data that reaches them.
  Affects: NFR-003 needs a retention period for anything that carries cardholder data.
  Ask: Stakeholder: how long does finance actually need transaction records, and does anyone need old case notes?

Checked, nothing found: Scope is reduced through tokenization or a hosted payment page wherever possible; Access to cardholder data is need-to-know with multi-factor authentication

Prepared to support your compliance owner's review. Not a legal or regulatory determination.

Salesforce Service Cloud Admin: Blocking

- Blocker, high confidence: Shared agent login keeps 200 agents on one identity [FR-004]
  FR-004 keeps the shared support login. Every case edit is attributed to nobody, and permission sets cannot be applied per role.
  Affects: FR-004 must change to named logins before FR-002 routing and any audit requirement can hold.
  Ask: Stakeholder: what stops each agent from having a named login: licence cost, queue views, or both? (blocking)
- Risk, high confidence: Synchronous Stripe callout inside the Case trigger [FR-007]
  FR-007 calls Stripe synchronously on every case update; at 40,000 cases a month one slow response blocks case saves.
  Affects: FR-007 needs an asynchronous pattern (queueable or platform event) before the volume in the business context is safe.
  Ask: Stakeholder: does settlement status need to be current the instant a case is saved, or is a minute acceptable?

Checked, nothing found: Sensitive fields are shielded or encrypted and excluded from reports and exports; Governor limits are considered for the expected case and API volume

AWS Solutions Architect: Blocking

- Blocker, high confidence: Analytics bucket is publicly readable with card data in it [FR-005]
  FR-005 leaves the S3 bucket public-read so the vendor needs no credentials.
  Affects: FR-005 must move to a scoped role or presigned access; the bucket cannot ship public.
  Ask: Engineering: can the vendor pull through a scoped IAM role or presigned URLs instead of a public bucket? (blocking)
- Risk, high confidence: Recovery objectives deferred with a single-region design [NFR-002, NFR-001]
  NFR-002 runs in one region on default RDS backups and postpones recovery objectives until after launch.

  Affects: NFR-001 availability cannot be committed to until NFR-002 states recovery point and time objectives.
  Ask: Stakeholder: how long can merchants be without the portal, and how much data can be lost, in minutes?
- Gap, low confidence: Backup retention is not stated [general practice]
  NFR-002 relies on RDS defaults; nothing says how long backups are kept or whether restores are tested. General practice for customer-facing systems; the document neither confirms nor denies a policy.
  Affects: NFR-002 and NFR-003 need one retention policy that backups follow.
  Ask: Engineering: is there a written backup retention policy the portal should inherit?
Checked, nothing found: Root credentials are never used for daily work; every operator has an individual identity with MFA

Exported from scopedrift.ai