Asima Service Level Agreement

Effective date: [Insert date]

Parties: This Service Level Agreement ("SLA") is between Wonderful Payments Limited, trading as and referred to as **Asima** ("Provider") and the **Client** ("Customer"), and forms part of the Master Services Agreement.

---

1. Introduction

This SLA defines the service standards and commitments for Asima's open banking infrastructure services, including **Account Information Services (AIS)**, **Payment Initiation Services (PIS)**, and related monitoring, support, and change-management processes.

Its purpose is to ensure clear expectations regarding availability, performance, incident handling, and remedies. This SLA applies for the duration of the Client's active subscription or contract term, unless superseded by a mutually agreed amendment.

---

2. Service scope

The services covered under this SLA include:

- **Account Information Services (AIS)** – secure retrieval of account data, balances, and transactions.

- **Payment Initiation Services (PIS)** – initiation of single immediate payments and variable recurring payments (VRP).

- **Service transparency** – public status page, real-time monitoring, incident history.

- **Customer support** – multi-channel support for technical and operational queries.

Excluded: Any third-party service not operated or controlled by Asima, including bank APIs, network infrastructure outside Asima's control, and customer-hosted systems.

---

3. Availability and performance

3.1 Availability target

- **API uptime:** 99.5% monthly, calculated across all production endpoints.

- Uptime excludes:

  - Scheduled maintenance (max 4 hours per month, notified at least 48 hours in advance)

  - Outages caused by upstream bank/API downtime

3.2 Performance targets

- Median response time for balance and transaction endpoints: **< 300 ms** under normal load.

- Peak load handling:

  - Sustained ≥ 500 requests/minute per endpoint.

  - ≥ 15,000 requests in any rolling 8-hour window.

---

4. Monitoring and reporting

- **Continuous monitoring:** 24/7 automated systems tracking availability, latency, and error rates.

- **Reporting:**

  - Client dashboard with real-time SLIs/SLOs.

  - Weekly and monthly performance summaries.

- **Alerts:** Real-time incident notifications to Provider's engineering team and Client's designated contacts when SLIs are breached.

---

5. Incident response

Severity	Definition	Response Target	Resolution Target	RCA Delivery
Sev 1	Full outage or complete loss of a critical function	15 minutes	4 hours	5 business days
Sev 2	Partial degradation, major performance issue	1 hour	1 business day	5 business days
Sev 3	Minor bug or non-critical defect	4 hours	5 business days	Provided if Client requests

Root cause analysis (RCA) will include incident summary, cause, resolution steps, and prevention plan.

---

6. Version and change management

- **Major endpoint changes:** Minimum 60 business days' notice.

- **Critical security patches:** Immediate deployment with notification.

- **Deprecation policy:** 90-day migration phase for deprecated versions unless a security risk requires shorter notice.

---

7. Support and service desk

- **Business hours:** Monday to Friday, 08:00–18:00 GMT (excluding UK public holidays).

- **Support channels:** Email, ticketing portal, and telephone.

Response targets:

- Critical issue: ≤ 2 business hours.

- General enquiry: ≤ 1 business day.

---

8. Remedies and service credits

If monthly uptime falls below:

- **99.0% but ≥ 98.0%** → 10% service credit

- **< 98.0%** → 25% service credit

Credits are capped at 50% of the monthly fee and applied against future invoices. Requests for credit must be made in writing within 30 days of the reported breach.

---

9. Review and revision

This SLA will be reviewed **biannually** or upon major regulatory, operational, or technical change. Any amendments require written agreement by both parties.

---

10. Glossary and definitions

- **Availability:** The percentage of time production endpoints return a successful 200-series HTTP status.

- **SLA period:** One calendar month.

- **SLI:** Service Level Indicator – a specific metric (e.g., uptime percentage).

- **SLO:** Service Level Objective – the target value or range for an SLI.

- **Severities:** Defined in Section 5.

- **Scheduled maintenance:** Pre-announced maintenance windows that may cause downtime.

Annex A – Severity definitions and examples

This annex forms part of the Asima Service Level Agreement. It defines the classification of incidents, their operational impact, and examples for consistent application.

Severity 1 – Critical outage

Definition:

A complete loss of service for one or more critical functions, with no available workaround. Incident prevents the Client from using a production service in a manner that meets their business-critical requirements.

Examples:

- All API endpoints unavailable.

- Payment initiation requests failing at 100% across all banks.

- Balance and transaction data retrieval completely failing across all connections.

- Security breach requiring immediate service shutdown.

Operational impact:

Immediate, sustained disruption to the Client's ability to process live transactions or access live data.

Severity 2 – Major degradation

Definition:

A partial loss of service or significant performance degradation affecting a critical function, but where some functionality remains available and workarounds are possible. The impact is material but does not completely halt business operations.

Examples:

- Payment initiation failing for a specific bank group but functioning for others.

- Significant latency increase (e.g., > 2 seconds) on balance or transaction endpoints, affecting > 50% of requests.

- VRP payments intermittently failing during authorisation.

- High error rates (≥ 20%) in a major endpoint under normal load.

Operational impact:

The Client's operations are impaired, potentially causing delays or manual intervention, but service remains partially functional.

Severity 3 – Minor issue / bug

Definition:

A defect, anomaly, or localised issue causing minimal operational impact, with a viable workaround available. The incident does not significantly affect core business processes or SLAs.

Examples:

- Incorrect error message text or metadata field.

- Latency spikes under very high load, within stress-test tolerance.

- Inaccurate data in a non-critical field that does not affect transaction integrity.

- Dashboard display issue not impacting API performance.

Operational impact:

Minimal impact, typically cosmetic or affecting only a small subset of operations.

Incident classification notes

1. **Upstream dependencies:** Issues caused by third-party bank APIs or external networks will be classified according to their impact on Asima's services, but may not

be eligible for service credits if outside Asima's control.

2. **Reclassification:** If new information emerges, Asima reserves the right to reclassify an incident's severity after initial triage, with written notification to the Client.

3. **Multiple clients affected:** If the same incident impacts multiple clients, it will be classified based on the highest severity impact observed.