### **Pre-SIT Clarification: Critical Questions for the Payment Module**

To: Project Team (Project Manager, Business Analysts, Development Leads, Architects)

From: QA Team

Date: August 3, 2025

Subject: Agenda for Pre-SIT Clarification Session - Payment Uploader (Payment Module)

**1. Introduction & Objective**

Team,

As we approach the formal System Integration Testing (SIT) for the Payment Module, the QA team has completed a deep-dive analysis of the FDD, TDD, and all associated process flows. This analysis has been incredibly helpful in building our test strategy.

To ensure our SIT phase is as efficient and effective as possible, we have identified several critical scenarios and potential gaps that are not explicitly detailed in the current documentation. The purpose of this session is to collaboratively discuss these points to align our understanding, mitigate risks, and confirm the system's designed behavior before we commit to the extensive SIT execution cycle.

**2. Agenda: Critical Questions for Discussion**

#### **Category A: Business Process & Operational Scenarios (The "What Ifs")**

These questions focus on real-world complexities that extend beyond the primary "happy path" workflow.

* **A1: On Failed Transaction Lifecycles**
  + **Question:** The documents define the "Balance Short" status. If a Standing Order fails due to insufficient funds, what is the defined system behavior for the *next* payment cycle? Does the system automatically suspend the Standing Order after a set number of consecutive failures, or does it attempt to debit indefinitely each month?
  + **Why it's critical:** This clarifies the long-term handling of problematic accounts, which directly impacts customer experience, operational workload, and system performance.
* **A2: On the "Manual Repair" Function**
  + **Question:** The FDD mentions a "Manual Repair" function. Is this purely a re-trigger mechanism for the existing data, or can an operator **correct underlying data** (e.g., an incorrect Billing ID that was mistakenly approved) as part of the repair process? If data can be corrected, what is the specific audit and approval workflow for that change?
  + **Why it's critical:** This defines whether "Repair" is a simple retry or a complex data correction tool, which has significant implications for operational procedures, security, and auditability.
* **A3: On Financial Reconciliation & Dispute Resolution**
  + **Question:** The documents detail the *transactional* reconciliation with the Biller Aggregator. What is the defined process for the *financial* reconciliation? How does the Accounting department reconcile funds settled into the "MD Account / Miscellaneous deposit account" against the transaction records in the Payment Uploader? Is there a specific report generated from the PU for this purpose?
  + **Why it's critical:** This probes the crucial link between technical transaction success and actual financial settlement, a key area for financial control and dispute management.

#### **Category B: Technical Resilience & State Management (Worker Service)**

These questions target the robustness of the automated Worker Payment Service and its ability to handle unexpected technical failures.

* **B1: On Atomic Operations (The "Point of No Return")**
  + **Question:** The worker's payment flow is: 1) Hold Amount, 2) Pay Biller, 3) Debit Customer. What is the system's exact recovery mechanism if a catastrophic failure occurs *after* the Biller Aggregator confirms payment but *before* the customer's account is debited? How do we guarantee we debit the customer exactly once and avoid financial loss?
  + **Why it's critical:** This is the most significant financial risk in the process. A gap here could lead to the bank paying on behalf of a customer without being reimbursed.
* **B2: On Idempotency of the Worker Service**
  + **Question:** If the Worker Payment Service job is accidentally triggered twice for the same day, how does the system prevent it from processing the same payment instruction multiple times and causing a double-debit?
  + **Why it's critical:** A non-idempotent worker could cause severe financial and reputational damage. We need to confirm the design prevents this at a fundamental level.
* **B3: On Concurrency Control**
  + **Question:** The system is deployed on OpenShift, which allows for multiple container instances. If we scale the Worker Payment Service to run in parallel, what is the database locking strategy (e.g., SELECT FOR UPDATE) on the ts\_payment\_status table to prevent two workers from processing the same transaction simultaneously?
  + **Why it's critical:** Without a clear concurrency strategy, scaling the application could introduce race conditions, leading to duplicate or failed payments.

#### **Category C: Biller Aggregator (SYB) Dependency Management**

These questions address the risks and ambiguities associated with our critical third-party partner.

* **C1: On Biller Error Code Handling**
  + **Question:** The FDD lists high-level statuses like "Payment Suspect." For our operations and development teams to build robust error handling, do we have a comprehensive data dictionary of *every* specific error code the SYB API can return, and a clear mapping of their codes to our internal system statuses?
  + **Why it's critical:** Without a detailed error code mapping, the PU can only handle failures generically, which limits our ability to automate retries intelligently or provide clear, actionable information to operators.
* **C2: On Onboarding New Billers**
  + **Question:** The timeline document shows a 45-day process for adding a new biller. From a technical perspective within the PU, what does this entail? Is it purely a data configuration change in the "Master Product" and "Master Charges" modules, or does onboarding a new biller from SYB require a new code deployment for the PU?
  + **Why it's critical:** This determines the agility of the platform. If adding a new biller requires a full development cycle, the business's ability to expand its service offering will be significantly slower and more costly than anticipated.

**3. Next Steps**

We believe that getting clarity on these scenarios is crucial for a successful SIT and a resilient production launch. We propose a 1-hour meeting to discuss these points and would like to invite the key stakeholders to align on the expected system behaviors.