**QCB Simulated Regulatory Circular:**

**Digital Consumer Protection & AML/KYC**

**Circular Ref:** QCB-FINTECH-2025-003 **Effective Date:** 2025-10-20 **Applicable Entity Type:** Digital Payment Service Providers and P2P Lending Platforms (Fintech Category 3)

**SECTION 1: ANTI-MONEY LAUNDERING (AML) & KYC REQUIREMENTS**

**Article 1.1: Customer Due Diligence (CDD)**

1.1.1. **Mandatory Verification:** All regulated Fintech entities must implement enhanced Customer Due Diligence (CDD) procedures for any user transacting more than **QAR 10,000** per calendar month. 1.1.2. **Source of Funds:** For high-risk customers or transactions exceeding **QAR 50,000**, the entity must obtain and maintain records documenting the verified source of funds and source of wealth. 1.1.3. **KYC Documentation:** A minimum of two forms of government-issued identification must be verified using digital and non-editable means. **Proof of Residency** must be obtained for all international users. 1.1.4. **Policy Document:** The entity must submit a written, Board-approved Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Policy, clearly outlining transaction monitoring rules.

**Article 1.2: Transaction Monitoring**

1.2.1. **Suspicious Activity:** The entity must deploy an automated transaction monitoring system capable of identifying and flagging suspicious activity based on patterns, velocity, and deviation from typical customer behavior. 1.2.2. **Reporting:** All Suspicious Transaction Reports (STRs) must be filed with the relevant Qatari authorities within **48 hours** of detection.

**SECTION 2: DIGITAL CONSUMER PROTECTION & DATA GOVERNANCE**

**Article 2.1: Data Protection and Residency**

2.1.1. **Data Residency:** All customer personal identifiable information (PII) and transactional data related to Qatari citizens and residents **must be stored on servers physically located within the State of Qatar.** 2.1.2. **Consent:** Explicit, informed consent must be obtained from the customer for the sharing of any data with third-party service providers (including cloud providers).

**Article 2.2: Corporate Governance and Audit**

2.2.1. **Compliance Officer:** The entity must appoint a designated, independent **Compliance Officer** whose CV and credentials must be submitted to the QCB for approval prior to licensing. 2.2.2. **Annual Audit:** An annual external audit of all technology systems and compliance policies is mandatory.