FINANCIAL MARKETS DIVISION

National Payment Systems

GUIDELINES FOR QUICK RESPONSE (QR) CODE PAYMENTS IN ZIMBABWE

MARCH 2026

gm

TABLE OF CONTENTS

gm

1. INTRODUCTION

1.1 The Reserve Bank of Zimbabwe (Reserve Bank/RBZ) recognizes the growing role of digital payments in fostering financial inclusion, efficiency, and convenience in the payment ecosystem. In particular, the Reserve Bank notes the rapid acceleration and increasing usage of Quick Response (QR) code payments in Zimbabwe.

1.2 To build on this momentum, these Guidelines have been developed to modernize and standardize the use of QR code payments, while ensuring security, interoperability, and regulatory compliance across Zimbabwe's financial sector.

1.3 QR code payments offer an efficient, low-cost, and contactless payment solution, allowing consumers to make transactions using smartphone cameras or dedicated applications. The Guidelines provide a regulatory framework for financial institutions, payment service providers, merchants, consumers, and other stakeholders.

1.4 The issuance of these Guidelines is anchored in the Reserve Bank of Zimbabwe's mandate to promote the smooth operation of payment systems in terms of the Reserve Bank of Zimbabwe Act [Chapter 22:15] ("the Reserve Bank Act"), Banking Act [Chapter 24:20] and the National Payment Systems Act [Chapter 24:23] ("the NPS Act").

1.5 Payment, clearing, and settlement system providers, participants, and stakeholders of payment systems wishing to make use of QR codes in their systems are therefore expected to be familiar with the requirements of the existing legal framework, and additionally:

- Directives, guidelines, and circulars issued by the Reserve Bank.
- International Standards and best practices.
- Any other additional regulatory requirements governing payment systems as may come into effect from time to time.

2. GLOSSARY

2.1. "**Acquirer**" means a financial institution or payment service provider that enables merchants to accept payments. The acquirer processes payment transactions on behalf of the merchant by facilitating the transfer of funds from the payer's bank (issuer) to the merchant's account.

2.2. **"Cross-scheme**" means QR acceptance and processing that supports more than one recognized payment scheme within a single QR or merchant profile.

2.3. **"Closed Loop System"** means a system in which an entity onboards merchants and subsequently issues QR codes to them. Only the account holders of that entity can use these QR codes to make payments to the merchants.

2.4. **"EMV"** means Europay, Mastercard, and Visa, the organisations that jointly created the global standard for secure payment transactions.

2.5. **"EMVCo"** means the organization that manages and maintains the EMV® QR Code Payment Specification (EMV® QRCPS), which defines standards for QR code-based payment transactions. Available at: https://www.emvco.com/emv-technologies/qr-codes.

gm

2.6. **"Inter-provider (Inter-PSP")** means a transaction in which the issuer and acquirer belong to different licensed providers (banks, mobile money operators, or other PSPs), whether on the same scheme or across schemes.

2.7. **"Issuer"** means a financial institution that provides payment instruments (such as bank accounts, debit cards, mobile wallets, or QR-based payment solutions) to consumers. The issuer is responsible for authenticating and authorization of payments initiated by its customers and ensuring the funds are debited accordingly.

2.8. "**Merchant**" means any person that accepts retail payment instruments, including e-money, as payment for their goods and services.

2.9. **"Merchant Account Information"** means essential information for identifying the merchant, such as the scheme, merchant ID, acquirer details, and more. This is a crucial field within the QR code data objects and is typically issued by the scheme.

2.10. **"Open Loop System"** means a system governed by a framework in which various participants act as acquirers and issuers. In this system, acquirers issue QR codes in a standardized format that can be utilized by other participants.

2.11. "**Payment Service Provider (PSP)**" means an entity that provides services enabling funds to be deposited and withdrawn from an account or wallet; payment transactions involving transfers of funds; the issuance and/or acquisition of payment instruments such as cheques, e-money, credit cards, debit cards; remittances and other services central to the transfer of funds.

2.12. **"PSO/PSP"** means Payment System Operator/ Payment Service Provider.

2.13. "**QR Codes (Quick Response Codes**)" means two-dimensional machine-readable barcodes which store data both horizontally and vertically, consisting of squares arranged on a grid that can store URLs or other information as indicated below.

2.14. **QR Code Payments** means a contactless, digital payment method where transactions are completed by scanning a QR code using a smartphone camera or other dedicated applications.

2.15. **"QR repository"** means a centralized or federated database system that stores, manages, and distributes QR code templates, merchant payment identifiers, and related metadata used for QR-based payment transactions, facilitating standardisation, interoperability, and secure retrieval of QR codes by payment service providers and end-users across different platforms or networks.

2.16. **"Service providers"** means banks and non-bank payment service providers.

2.17. **"Scheme"** means entities that develop systems and rules, and they serve as a platform to enable QR Codes as a payment mechanism to their participants (acquirers and issuers). These schemes can be domestic or international.

gm

2.18. **"User"** means an individual or entity that utilizes QR code payment services. This includes anyone engaging in financial transactions by scanning QR codes to make or receive payments.

3. SCOPE

3.1. These guidelines apply to all financial institutions, payment system operators, payment service providers, merchants, issuers, acquirers, and other stakeholders involved in the issuance, acceptance, and processing of QR code payments in Zimbabwe.

3.2. The guideline covers:

3.2.1. QR code payment standards and interoperability;
3.2.2. Licensing and application requirements;
3.2.3. Consumer protection measures and security protocols;
3.2.4. Risk management and fraud prevention mechanisms; and
3.2.5. Regulatory oversight and compliance requirements.

4. OBJECTIVES

4.1. The guidelines aim to ensure the adoption of appropriate QR code standards for safe, inclusive, and efficient digital payment services.

4.2. Therefore, the key objectives of these guidelines is to:

4.2.1. Promote the adoption and safe use of QR Code Payments.

4.2.2. Establish a standardized and secure QR code payment system;

4.2.3. Promote financial inclusion by enabling widespread adoption of QR payments;

4.2.4. Foster interoperability among banks and payment service providers, including mobile money operators offering various payment schemes and channels;

4.2.5. Ensuring security, fraud prevention, efficiency, and consumer protection in digital payments;

4.2.6. Foster innovation while ensuring regulatory oversight and compliance;

4.2.7. Align with international standards while addressing Zimbabwe's context; and

4.2.8. Establish roles and responsibilities of participants in QR Payments.

5. LEGAL FRAMEWORK

5.1. The Reserve Bank Act and the National Payment Systems Act empower the Reserve Bank to recognize, oversee, supervise, and operate payment, clearing, and settlement systems in Zimbabwe.

5.2. The legal framework is also bolstered by other supporting statutes on payment systems issues including the Banking Act [Chapter 24:20] Exchange Control Act [Chapter 22:05], and Money Laundering and Proceeds of Crime Act [Chapter 9:24] Cyber and Data Protection Act [Chapter 12:07], the Consumer Protection Act [Chapter 14:14]and, the Banking (Money Transmission, Mobile Banking and Mobile Money Interoperability) Regulations,2020 (S.I 80 of 2020) as well as the Banking (Money Transmission, Mobile Banking and Mobile Money Interoperability) (Amendment) Regulations, 2025, S.I 17 of 2025.

5.3. The Reserve Bank subscribes to and will also be guided by international best practice, in particular the Bank for International Settlements (BIS) Principles for Financial Market Infrastructures (PFMIs).

6. APPLICATION TO OFFER QR CODE PAYMENTS

Applicants wishing to offer QR code payment services must obtain approval from the Reserve Bank.

6.1. Eligibility for Approval

The Reserve Bank will only approve an application to provide QR code payment services to:

6.1.2 Licensed financial institutions;

6.1.3 Licensed payment system providers, including mobile money operators, and

6.1.4 Other entities as approved by the Reserve Bank from time to time.

6.2. Application Requirements

6.2.1 Providers wishing to apply for approval to provide QR Code payment services shall be required to submit a formal application letter addressed to the Reserve Bank of Zimbabwe, National Payment Systems Department.

6.2.2 Applicants should be guided by the following guidelines or standards in their application:

6.2.2.1 **Minimum requirements for retail payment systems**
https://www.rbz.co.zw/index.php/financial-markets/national-payment-system/approval-requirements

6.2.2.2 **The Framework for the Recognition of Payment Systems in Zimbabwe**
https://www.rbz.co.zw/documents/nps/framework-for-the-recognition-of-payment-systems-in-zimbabwe---april-2016.pdf

6.2.2.3 **Guideline for Retail Payment Systems**-
https://www.rbz.co.zw/documents/nps/payment-systems-guidelines-august-2017.pdf

6.2.2.4 **Oversight Framework** guideline https://www.rbz.co.zw/documents/nps/framework-for-oversight-of-payments-systems-in-zimbabwe---april-2016.pdf

6.2.2.5 **Cybersecurity and Resilience Guideline**
Cybersecurity_and_Resilience_Guideline_-_August_2025.pdf.

6.2.2.6 **Consumer Protection Framework**
https://www.rbz.co.zw/documents/consumer_protection/consumer-protection-framework-26-june-2017.pdf

gm

7. INTEROPERABILITY

7.1. All QR code payment systems must be interoperable across banks, mobile money providers, and payment processors and providers as per the requirements of S.I. 80 of 2020.

7.2. As a default, inter-provider routing and clearing shall be facilitated through the National Switch, which also hosts the National QR Repository. On-us QR code transactions may be processed on-us by the originating provider, subject to mandatory reporting of authorisation, clearing, settlement, and transaction data to the Reserve Bank and, where necessary, to the National Switch, as specified by RBZ from time to time.

7.3. While the National Switch shall be a key enabler, the Reserve Bank may, on a case-by-case basis, authorise direct cross-scheme interconnections for specific use cases (e.g. regional integration, card scheme linkages, or specialized PSPs/fintech arrangements) provided that such interconnections demonstrate:

a) Equivalent or stronger levels of interoperability, settlement finality, and consumer protection.
b) Continuous data visibility and reporting access for RBZ.
c) No adverse impact on the integrity or competitiveness of the national payment system.

8. PARTICIPANTS IN QR CODE PAYMENTS

8.1. All participants shall comply with the minimum standards outlined in these guidelines, including but not limited to registration, system interoperability, security, and consumer protection.

8.2. Participants in QR Code Payment in Zimbabwe include:

a) Merchants
b) Customers
c) Issuers (Banks and Payment Service Providers (PSPs)
d) Acquirers (Banks, PSPs)

9. RESPONSIBILITIES OF PARTICIPANTS

9.1. **Schemes/Switches/Network**

a) To provide QR as a payment mechanism under their scheme(s), PSO/PSPs and other regulated entities shall contact the National Switch to avoid duplication of their Merchant Account Information IDs (MAI ID) (first two digits).

b) The plan, as well as the relevant scheme rules, including fraud mitigation and management, merchant services management, consumer protection, and dispute resolution mechanisms and any other requirements as guided by the Reserve Bank from time to time, must be submitted to the Reserve Bank.

gm

c) Once the PSO/PSP has been issued the MAI ID, it may proceed to enroll acquirers and issuers on its QR scheme.

d) Only entities licensed by RBZ as PSPs are permitted to enable QR Code offerings to their participants (acquirers and issuers) through a scheme.

e) The MAI (first two numerals) should be checked with the National Switch and then RBZ shall be advised thereafter.

f) Participants in the scheme are required to adhere to the MAI format and share it with the other participants.

g) The scheme/switch operator is also responsible for the development of the items that will be utilized in Scheme Specific Data objects for the scheme's acquirers and issuers, if necessary.

h) The National Switch, in collaboration with other PSPs, will issue additional details under System Rules and will establish, maintain, and administer the scheme through well-defined system/business rules, fraud management, consumer protection, and dispute resolution mechanisms.

9.2. **Merchants shall:**

a) Use QR Code payment applications provided by the issuer for the intended purpose without modifications, at merchant locations, websites, or applications.
b) Comply with service agreements executed with the acquirer.
c) Cooperate with the acquirer to investigate any reported fraudulent transactions.
d) Report suspicious use of QR Codes for payments to the acquirer.
e) Conform with the rules and regulations of the acquirer.
f) Follow the Reserve Bank Guidelines on Payment Systems, Charges, and other applicable financial regulations.
g) While merchants have operational responsibilities, the acquirers shall be accountable to the Reserve Bank for ensuring that their merchants comply with these guidelines.

9.3. **User:**

a) Use QR Code payment applications provided by the issuer for the intended purpose without modifications, at merchant locations, websites, or applications.
b) Adhere to all minimum-security guidelines as stipulated by the issuer.
c) Report inappropriate or unauthorized QR Code payment transactions to Banks and payment system providers on their accounts or wallets.

gm

9.4. **Issuers (Banks, Mobile Money Operators, and Other Institutions) shall:**

a) Develop their apps and portals to be aligned with the specifications mentioned in this document, ensuring they can read all QR Codes generated by the acquirers in compliance to the standards in this guideline, as a minimum in line with the EMVCo QR Code Payment Specification (QRCPS).
b) Provide QR Code Payment applications to customers upon request and activation by the customer.
c) Allow the customer to select between the schemes of the choice of the customer, for the merchant which has been onboarded on multiple schemes by an acquirer; to the extent that the scheme is recognized by the issuer.
d) Enable their apps / portals to read the QR as a picture (.jpg, .png etc) from storage media, besides enable the QR to be scanned through the camera or other mechanism.
e) Execute service agreements with their customers.
f) Comply with Scheme Rules.
g) Determine appropriate transaction limits with customers for QR Code Payments based on their customers' risk profile assessment.
h) Ensure appropriate configurations on QR Code Payment applications that use QR codes for payments, ensuring compliance with QR Code regulations.
i) Deploy necessary updates and patches on QR Code Payment applications and ensure customers cannot initiate transactions using outdated versions beyond 14 days of an update's availability
j) Where applicable, issuers may induce an automatic update of the customer's application.
k) Provide adequate training, support, and security guidelines to customers on the use of QR codes for payments.
l) Ensure the security of QR Code payment applications for QR Code payments.
m) Resolve customer disputes in accordance with the Reserve Bank Consumer Protection Guideline.
n) Be guided by the Reserve Bank Guidelines on Retail Payments Systems (2017) and SI 80 of 2020 on charges that have to be approved by the Reserve Bank by Banks and PSPs.

9.5. **Acquirers shall:**

a) Onboard with the local QR repository as a domestic payment scheme. However, they may also work with international payment schemes where feasible.
b) Start to generate QR codes for newly onboarded merchants and replace existing QR codes in compliance with the adopted standards.
c) Replace the QR codes at merchant locations with a unified and interoperable QR code using a multi-scheme template where an acquirer has onboarded or is onboarding the same merchant to an additional scheme.
d) Generate dynamic QRs through online portals /apps (for e-Commerce) or digital display screens (for in-store purchases).
e) Offer QR codes to the merchants under a scheme only. The acquirers working in a closed-loop model may continue to work after which all closed-loop QR Codes shall cease to exist and only scheme-based (open-loop) QR codes will be operational after the effective date as per this guideline.
f) Execute service agreements with merchants.
g) Determine appropriate transaction limits with merchants for accepting QR Code Payments based on the merchant's risk profile assessment.

gm

h) Ensure appropriate configurations and use of QR codes at merchant locations, websites, or applications in compliance with QR Scheme(s) and QR Code regulations.
i) Ensure that appropriate security protocols are applied.
j) Provide adequate training, support, and security guidelines to merchants on the use of QR codes for payments.
k) The Acquirer must ensure to undertake KYC and prescribed due diligence for all merchants onboarded.
l) Ensure that hardware, software, and protocols used for QR Code payments comply with QR Code payments guidelines.
m) Provide merchants with value for QR Code transactions within T+1 or as agreed with the merchant.
n) Be guided by the extant Reserve Bank Guidelines on Risk-Based Cyber Security Guideline, Retail Payment Systems, Guide to Charges, and other applicable guidelines as may be issued by the Reserve Bank from time to time.

9.6. The National Switch and other payment schemes must develop and implement operating guidelines for QR Code Payments, which should include the following minimum elements:

- Participant responsibilities.
- Settlement arrangements.
- Cybersecurity requirements.
- Complaints handling mechanisms.

10. CONFIDENTIALITY AND PROTECTION OF CUSTOMER DATA

10.1. To foster public trust and uphold operational integrity, all parties involved in QR code payments, including banks, payment service providers (PSPs), issuers, acquirers, scheme operators, processors, and authorized third parties, must strictly observe the confidentiality of all customer data accessed under this regulation.

10.2. Customer information must only be used for purposes expressly provided in these Guidelines. Its use for commercial, marketing, or behavioral profiling purposes is prohibited unless prior written consent is obtained from the customer or authorization is granted by the Reserve Bank.

10.3. Entities must adhere to prevailing legal frameworks governing banking secrecy and data protection.

10.4. Participating institutions shall implement appropriate technical and organizational controls, including:

a) End-to-end encryption of sensitive information both in transit and at rest.
b) Access controls based on roles and responsibilities.
c) Multi-factor authentication and activity monitoring.
d) Periodic risk assessments and third-party security audits.
e) Maintenance of tamper-evident audit trails to enable traceability of all data access or changes.

gm

11. CONSUMER PROTECTION AND SECURITY

To ensure user trust and confidence, the following consumer protection measures must be observed:

11.1. Transaction refund and reversal procedures shall be clearly outlined. The National Switch shall issue and maintain a minimum Dispute & Reversal Artefact Set, including required data elements and submission formats. All PSPs/Acquirers/Issuers shall align their internal procedures thereto.

11.2. A structured dispute resolution mechanism must be in place for handling complaints.

- Transaction reversal procedures to be clearly outlined.
- Dispute resolution must be completed within Fourteen (14) working days from customer lodgment, inclusive of the determination of liability.
- Where a refund/reversal is due, it must be processed within five (5) working days after the determination of liability. Customers shall receive interim updates at least every five (5) working days until closure.
- Refunds for erroneous, unauthorized, or fraudulent transactions must be processed within five (5) working days after determination of liability.
- Providers must not impose excessive fees or delays for legitimate consumer refund claims.

11.3. A 24/7 customer support channel should be availed for handling queries. Dispute channels must be accessible to users in rural areas and persons with disabilities.

11.4. Policies and mechanisms to prevent fraud and protect against cyber-attacks and protect personal data.

11.5. Disclosure and implementation of monthly and daily transaction limits to mitigate against money laundering and fraud risks.

11.6. Escalation procedures to the Reserve Bank or an independent, impartial person must be available.

11.7. Disclosure and Transparency on the key features, risks and terms of the products, fees, commissions or charges applicable. All promotional material should be accurate, honest, understandable and not misleading. All communication with consumers should be in plain, simple and comprehensible language.

11.8. Adhere to the Reserve Bank Consumer Protection Framework and any other guidelines as may be issued from time to time.

12. CUSTOMER EDUCATION AND AWARENESS

12.1. All participants should invest in earnest efforts to drive education and awareness campaigns for QR code payment adoption through intuitive print, electronic means, social media, and any other available platforms.

12.2. Issuers should endeavor to ensure that awareness and technical support are provided in multiple languages (at least in two local languages and English).

12.3. Consideration should be made to include interactive tutorials and community outreach sessions, especially in rural areas.

gm

13. ACCESSIBILITY AND USABILITY STANDARDS

13.1. PSPs and acquirers must ensure that QR platforms comply with accessibility standards, including:

a) Compatibility with screen readers for visually impaired users.

b) Scalable text and intuitive interfaces.

c) Alternative input methods for users with motor disabilities.

13.2. RBZ may issue further accessibility compliance guidance.

14. TRANSACTION LIMITS

Transaction limits will be as per other retail payment services, as guided from time to time by the Reserve Bank, through circulars and notifications.

15. MERCHANT REQUIREMENTS

15.1. Payment Service Providers must conduct thorough know your customer (KYC) checks on Merchants before onboarding them for use of QR Codes.

15.2. Payment Service Providers must guarantee that merchants have a valid Bank account or mobile money wallet and adhere to all requirements as stipulated in the law.

15.3. Merchants shall retain customer-facing and operational QR transaction records for a minimum of five (5) years. Acquirers/PSPs/Gateways shall retain complete transactional, reconciliation, and audit logs for at least Five (5) years, or longer where required by applicable law and Reserve Bank directives.

15.4. Merchants display certified QR decals at points of sale (POS).

15.5. Use certified POS terminals with QR scanners compliant with Provisions on Barcode and QR Code Payment Acceptance Terminal Standards.

16. RISK MANAGEMENT AND FRAUD PREVENTION

16.1. Service providers must implement real-time transaction monitoring and fraud detection tools.

16.2. In case of security breaches, providers must report incidents to the Reserve Bank within 3hours or as soon as the provider becomes aware of the breach.

16.3. Reports must follow the format outlined in Appendix 3 of the Cybersecurity and Resilience Guideline, which incorporates initial incident reports, update incident reports, and concluding incident reports.

16.4. Merchants must undergo anti-fraud training.

16.5. Payment System Providers must enforce strict KYC protocols.

16.6. Adhere to RBZ's Risk-Based Guideline on Cybersecurity, including regular penetration testing and incident reporting.

16.7. Providers must use traceable QR elements to support AML/CFT monitoring and reporting.

16.8. Integration with national AML/CFT systems is mandatory.

gm

17. NATIONAL QR CODE REPOSITORY

17.1. RBZ shall ensure the establishment of a centralized QR code repository at the National Switch accessible to all licensed issuers and acquirers.

17.2. The repository shall enable standardized onboarding and improve fraud mitigation.

17.3. The Repository shall maintain Merchant Account Information (MAI) issuer ranges and scheme templates, prevent duplication, and enable multi-scheme QR issuance.

17.4. Access, write permissions, and cryptographic controls shall follow the least-privilege principle, with independent audits submitted to RBZ.

18. COMPLIANCE AND REGULATORY OVERSIGHT

18.1. The RBZ will conduct periodic examinations and inspections of payment, clearing and settlement system providers, participants, and relevant stakeholders of payment systems making use of QR code payment systems.

18.2. Non-compliance with these guidelines will be dealt with as provided for in the existing legal framework.

18.3. Other actions of non-compliance in violation of any requirements for the provision of money transmission and mobile banking services will be dealt with in terms of the Banking (Money Transmission, Mobile Banking and Mobile Money Interoperability) Regulations,2020 (SI 80 of 2020).

18.4. Service providers must submit reports to the Reserve Bank as follows:

a) Periodic reports, i.e. weekly, monthly/Quarterly submission of transaction volumes, values, and subscriber information to the Reserve Bank.
b) Fraud and Security Incident Reports: reporting of fraud attempts, breaches, and anomalies within 24 hours of detection.
c) System Performance Monitoring Reports: Service providers must maintain uptime records and report any system downtimes exceeding 3 hours.

19. PENALTIES

19.1. All parties shall comply with the provisions of this guideline and other relevant guidelines issued by the Reserve Bank.

19.2. The Reserve Bank shall apply appropriate sanctions, including monetary fines, suspension/revocation of services, or other measures to any party that fails to comply accordingly.

19.3. Fines up to the Levels prescribed in terms of the relevant laws shall be applicable.

19.4. Entities that violate any requirements of this guideline and, having been notified, fail to rectify compliance issues within the days stipulated in the notice may have their licenses/approval revoked.

gm

20. TECHNICAL SPECIFICATIONS

20.1. All participants in the QR payment ecosystem shall adopt the EMVCo QR Code Standard to ensure efficiency, consistency, encryption, and global interoperability.

20.2. All Participants should be guided by the technical standards adopted and captured in **Annexure 1** for the technical standards adopted for Zimbabwe.

20.3. There shall be the use of multi-scheme QR Codes that can accommodate multiple payment schemes in a single QR code to prevent fragmentation and ensure ease of use for merchants and customers.

20.4. **Scan to Pay Code Data Specification**

The Reserve Bank of Zimbabwe (RBZ) has adopted the **EMV® QR Code Specification for Payment Systems (EMV QRCPS)** for merchant-presented QR codes to ensure **standardization and interoperability**. As new participants and payment rails are introduced, the EMV QR standard implemented by RBZ will be updated to incorporate **alternative payment acceptance methods** compatible with emerging payment rails.

20.5. **Specification Usage Column Fields**

- **Mandatory Fields**

Data Objects marked (M) in the *Presence* column in Annexure 1 must be present under the root of the QR Code. When Data Objects are marked (MC) it means the mandatory designation applies to transactions on the card rails only, as it is an EMVCo or Local industry requirement for card transactions.

- **Conditional**

Data Objects that are marked (C) in the Presence column in Annexure 1 shall be present under the root of the QR Code if the respective conditions are met.

20.6. **Use of Generic Information**

- **QR Code Payload**

The total length of the QR Code payload must not exceed 512 bytes.

21. GENERAL SPECIFICATIONS

21.1. PSPs shall offer merchant products that support QR Code Payments through multiple channels, including mobile applications, USSD, POS devices, and web platforms.

21.2. Ensure encryption for secure transaction processing. All Payment Service Providers (PSPs), Acquirers and Issuers shall ensure that sensitive identifiers within QR payloads, such as Primary Account Numbers (PANs), wallet IDs or account numbers, are not exposed in clear text. Such identifiers must be masked, encrypted, or tokenized in accordance with RBZ-issued Cyber Security Guidelines, among others.

21.3. The actual data contained in the QR codes may vary based on the specific use case and implementation.

gm

21.4. QR codes must contain essential payment information, including:

- Merchant identification details.
- Transaction details: e.g. date, time, currency, amount, and other details outlined in Annexure 1.

21.5. Payment network compatibility. Where QR transactions involve card-based instruments, PSPs shall additionally comply with the latest Payment Card Industry Data Security Standard (PCI DSS) requirements for data storage, processing, and transmission.

21.6. To enhance accessibility in low-connectivity areas, PSPs are encouraged to implement offline (store-and-forward) QR payment functionality, allowing transactions to be initiated when connectivity is unavailable and settled automatically once connectivity is restored. Such functionality shall conform to National Switch technical standards and include safeguards against double-spending and data tampering.

21.7. Static vs Dynamic QR Security/Other

a) Dynamic QR (or its equivalent or better in terms of security) shall be preferred for all forms of transactions. Merchants shall present a dynamic QR code generated for each transaction (embedding the amount, a one-time nonce, and an expiry value). Dynamic QRs may be displayed through POS terminals, merchant apps, or e-commerce checkout pages.

b) Static QR (or their equivalent in terms of security) shall be permitted only for low-value transactions below USD50 or local currency equivalent, provided the following controls are in place:
   - Certified decals with secure printing features (e.g. micro-text, UV markings, serialized QR).
   - Strong merchant KYC and terminal/store mapping (Tag 62-07 Terminal ID) with periodic verification.
   - Periodic QR refresh or re-issuance (recommended quarterly) and staff guidance on tamper detection.
   - Real-time risk analytics (velocity rules, geo/IP/device pattern checks).
   - Consumer confirmation screen showing merchant name and amount before authorisation.
   - The RBZ may review the above threshold periodically in line with inflation, exchange-rate developments, and risk assessments.

c) E-commerce and Remote Payments: Merchant-presented dynamic QRs (or secure deep links) shall be mandatory for all online, remote, or in-app transactions.

d) USSD Fallback: Where dynamic display is infeasible, acquirers shall provide an issuer-controlled amount entry and on-screen merchant verification before approval.

21.8. Each QR code shall clearly indicate its Point-of-Initiation Method in accordance with EMVCo v1.1 (or upgraded versions) specifications:

- Tag 01 = “11” for static QRs
- Tag 01 = “12” for dynamic QRs
- Each dynamic transaction shall include a unique nonce or reference identifier in Tag 62-05 to prevent replay attacks and ensure transaction uniqueness.

gm

22. EFFECTIVE DATE

These Guidelines shall take effect from 11 March 2026.

23. FEEDBACK AND CLARIFICATIONS

Questions relating to the Guidelines should be addressed to the Deputy Director, National Payment Systems, Reserve Bank of Zimbabwe.

24. CERTIFICATION AND APPROVAL OF THE GUIDELINES

The Reserve Bank of Zimbabwe official's signature placed hereinunder certifies the approval of these Guidelines.

PP

Dr. J. Mutepfa
Deputy Director
National Payment Systems Department

11 March 2026

Date

ANNEXURE 1:

Name	EMVCo Tag ID	Format	Length	Usage M/O/C	Description	Specific notes
Payload Format Indicator	00	N	02	M	Defines the version of the QR code release. Any increment to the version number would be jointly agreed between the participants (Cards & Network). The first version should be numbered 01".	
Point of initiation method	01	N	02	M	In this two digit field first character indicates the method by which the data is presented by the merchant. The second character indicates if the data is static or dynamic. 1st character : 1 = QR 2 = BLE 3 = NFC 4-9:Reserved for future use 2nd character : 1=static, 2=dynamic 3-9:Reserved for future use Example: "11" indicates QR static code "12" indicates QR dynamic code	
Merchant identifier as defined by network	02-03	AN	Variable as defined by the network	One of them Is mandatory, anything more than one is optional	Tag to be followed by length and data as defined by Network 1 -Visa	
	04-05				Tag to be followed by length and data as defined by Network 2 - Mastercard	
	06-08				Tag to be followed by length and data as defined by Network 3 - NPCI	
	09-10				Tag to be followed by length and data as defined by Network 4 - Discover	
	11-12				Tag to be followed by length and data as defined by Network 5 - Amex	
	13-14				Tag to be followed by length and data as defined by Network 6 - JCB	
	15-16				Tag to be followed by length and data as defined by Network 6 – UnionPay	
	17–25			O	Reserved by EMVCo. For additional Payment Networks	

gm

	26-51			O	To be allotted to existing/approved network/scheme operators considering present QR landscape and some tags will be reserved by the Reserve Bank of Zimbabwe and the National Switch.	
Merchant Category Code	52	N	04	MC	As defined by ISO 18245 Retail Services – Merchant Category Codes	
Transaction currency Code	53	N	03	MC	ISO 4217 –Zimbabwe = 924.	
Transaction Amount	54	ANS	Variable 13	O	This amount is expressed as how the value appears, amount "100.00" is defined as "100.00", or amount "99.85" is defined as "99.85", or amount "99.333" is defined as "99.333", or amount "99.3456" is defined as "99.3456"	
Tip or convenience indicator	55	N	02	O	01 : Prompt customer to add tip in payment 02 : Fixed Tip Amount in QR (tag 56) 03 : Indicates that merchant would charge a percentage convenience fee defined in Tag 57	TIP indicator will only be applicable in specific merchant categories that should be allowed by the scheme rules
Value of convenience fee fixed	56	ANS	Variable 13	C	Presence is dependent on the presence and value of tag Id 55 present if Id 55-Tip or Convenience Indicator present and with a value of 02 Note: 0 is not a valid value.	Any two of these IDs required if Tag 55 is populated
Value of convenience fee percentage	57	ANS	Variable 05	C	Presence is dependent on the presence and value of tag Id 55 present if Id 55-Tip or Convenience Indicator present and with a value of 03 Note: 0 or 100 is not a valid value.	
Country Code	58	AN	02	M	As defined by ISO 3166.	"ZW" Zimbabwe
Merchant Name	59	ANS	Variable up to 23	Mandatory	Should always be the "doing business as" name for the merchant.	
Merchant City	60	AN	Variable up to 15	Mandatory	City of operations for the merchant	
Postal Code	61	AN	Variable up to 10	Mandatory	Zip code or Pin code or Postal code of merchant	
Additional Data Field	62 (constructed Tag)	AN	Variable 99(up to the total length of the nested tags)	C	Additional information beyond that mentioned above may be required in certain cases. This information may be either presented by the merchant or acquirer or the Consumer may be prompted for entry on the app. For consumer prompt, the value field of Tag would be 3 asterisks i.e. ***. The acquirer / merchant should provide only	

gm

					minimum information in order to avoid making the size of data onerous. The length of each tag is variable up to 26 characters and overall it is not to exceed the maximum of 99 characters for the total size of the Additional Data Field.					
					Tag Value	Item	Format	Length	Usage	Description
					01	Bill number	ANS	Var. up to 25	O	Invoice number or bill number
					02	Mobile number	ANS	Var. up to 25	O	To be used for top-up or bill payment
					03	Store Label	ANS	Var. up to 25	O	A distinctive number associated to a Store
					04	Loyalty number	ANS	Var. up to 25	O	Typically a loyalty card number as provided by store or airline
					05	Reference ID	ANS	Var. up to 25	O	Any value as defined by merchant or acquirer in order to identify the transaction
					06	Customer ID	ANS	Var. up to 25	O	Typically a subscriber ID for subscription services or student enrolment number etc.
					07	Terminal ID	ANS	Var. up to 25	O	A distinctive number associated to a Terminal in the store. It will be mandatory value for all merchants on boarded for acceptance
					08	Purpose	ANS	Var. up to 25	O	Purpose of transaction like top-up for Mobile Top- Up use case- “Airtime”, “Data”, International Package”.
					09	Additional consumer data	ANS	Var. up to 25	O	
					10		ANS	Var. up to 25	O	
					11		ANS	Var. up to 25	O	
					12-49					Reserved for future use

gm

					50 - 99	Designated range of Identifiers that are dynamically allocable
CRC	63	AN	04	Mandatory	The checksum shall be calculated according to [ISO/IEC 13239] using the polynomial '1021' (hex) and initial value 'FFFF' (hex). The data over which the checksum is calculated shall cover all data objects, including their ID, Length and Value, to be included in the QR Code, in their respective order, as well as the ID and Length of the CRC itself (but excluding its Value).	
Merchant Information – Language Template	64	S	Var. up to 99	O	This allows the merchants information (name and city) to be populated in an alternative language	The information may use different Character set from the common Character set.
80-99	Unreserved Templates					

gm