**Tanzanian Mobile Financial Services**

**Bulk Payments (BP)**

**Interoperability Standards**

Published Version 1

17 September 2015

Contents

2 Document Control 6

3 Acceptance of these Standards 7

3.1 List of participants 8

4 Introduction 9

4.1 Effects 10

4.2 Governing Laws 10

4.3 Inconsistencies 10

5 Governance 11

5.1 Effective Date 11

5.2 Amendments & Waivers 11

5.2.1 Amendment to these Standards 11

5.3 Good Faith Co-operation 11

6 Participation in the BP Service 12

7 Services & Service Architecture 13

7.1 Services 13

7.2 Functional Flows 13

7.3 Subscriber Verification 13

8 Business model 15

9 Clearing and Prefunding 17

9.1 General Principles of Clearing 17

9.1.1 Provision of Information 17

9.1.2 Obligation to Credit 17

9.1.3 Returned Transactions 17

9.1.4 Responsibility for Transactional Errors 17

9.2 General Principles of Prefunding 17

9.3 Prefunding & Clearing Architecture 18

10 General Operational Considerations 19

10.1 Testing 19

10.2 System Support 19

10.3 Security 19

10.4 Money Laundering 19

10.5 Know Your Customer (KYC) 19

10.6 Reporting 20

10.6.1 Fraud Reporting 20

10.7 Service Levels 20

10.8 Retention of Records 20

10.9 Business Continuity Planning 21

10.10 Subscriber Support & Investigations 21

10.11 Bulk File Data Integrity 21

10.12 Mobile Number Portability 21

11 Principles for the Management of Subscriber Disputes 22

11.1 General Standards 22

11.1.1 Applicable Laws & Jurisdiction 22

11.1.2 Electronic Media As Evidence 22

11.1.3 Recipient MFS Opt-Out & Non-MFS Accounts 22

11.1.4 Reversals, Roll-Backs & Refunds 22

11.1.5 No Disintermediation 22

11.1.6 Subscriber Communications 22

11.1.7 Location Data 23

11.1.8 General Principles For The Recovery of Disputed Value: 23

11.1.9 General Process To Report & Resolve Subscriber Disputes 23

11.1.10 Fraudulent Disputes 24

11.1.11 Good Faith 24

11.1.12 Time Frames For Dispute Response 24

11.1.13 Grey-Listing Of MFS Accounts 24

11.1.14 Network Delays 25

11.2 Specific Examples 25

11.2.1 Money sent to the wrong user (“*error in personam*”) 25

11.2.2 Recipient Sent More Value Than Intended 25

11.2.3 Transaction Not Received by the Recipient’s MFSP 26

11.2.4 Technical Issues With The Sending Entity’s MFSP 26

11.2.5 Technical Issues With The Recipient Payee’s MFSP 26

11.2.6 e-Value Only Partially Credited 27

11.2.7 Bulk Payment Notification Messages Not Received 27

12 Risk management 28

13 General Standards of Compliance 29

13.1 Exemptions 29

13.2 Disclosure of Non-Compliance 29

13.3 Audit 29

13.4 Suspension & Termination 29

13.5 Notices 29

13.6 Liability for owned & controlled entities 29

13.7 Disclosures & Confidentiality 29

14 Appendix A – Governing Laws 30

Telecommunications-related oversight of MFS 30

Anti-money laundering laws, guidelines, circulars & regulations 30

Competition & consumer protection 30

Financial regulation 30

Auditing & Accounting regulation 30

15 Appendix B - Operational Requirements 31

15.1 Testing 31

15.2 Operational and Security Standards 31

15.3 Data Security 31

15.4 Prevention of Money-laundering 32

15.5 Reporting 32

16 Appendix C - Compliance 33

16.1 Exemptions & Waivers 33

16.1.1 Waivers from the Standards 33

16.1.2 Application for an Exemption 33

16.1.3 Determination of an Application for an Exemption 33

16.2 Disclosure of Non-Compliance 34

16.3 Audits 34

16.4 Suspension & Termination 34

16.4.1 Immediate Suspension 34

16.4.2 Other reasons for Suspension 35

16.4.3 Effect of Suspension 35

16.4.4 Withdrawal of Participants 35

16.4.5 Obligations of Cessation 35

16.4.6 Compliance with these Standards 35

16.5 Liability for owned & controlled entities 35

16.6 Disclosures 36

16.7 Confidentiality 36

17 Appendix D - Arbitration 37

18 Appendix E - Warranties 38

19 Appendix F – Application for Exemption 39

20 Appendix G –Interpretation 40

# Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version No.** | **Author** | **Comments** |
| 13 March 2015 | Draft 1 | MFSPs in Tanzania assisted by the IFC Team | First draft for Industry review. |
| 29 April 2015 | Draft 2 | MFSPs in Tanzania assisted by the IFC Team | Second draft for Industry review. |
| 17 September 2015 | Published 1 | MFSPs in Tanzania assisted by the IFC Team | Finalised following Industry review. |

# Acceptance of these Standards

By signing this document, each signatory binds itself to apply these Standards in all Commercial Bilateral agreements with each of the other signatories of these Standards, including any signatory which signs this document after the date of signature hereof by such first mentioned signatory, for the provision of Mobile Financial Interoperability Bulk Payments (MFSi BP) in the United Republic of Tanzania.

## List of participants

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company Name** | **Company Registration Number** | **Address of Registered Office** | **Address for Correspondence** | **Fax Number** | **Signatures** |
|  |  |  |  |  | 1) |
| 2) |
|  |  |  |  |  | 1) |
| 2) |
|  |  |  |  |  | 1) |
| 2) |
|  |  |  |  |  | 1) |
| 2) |
|  |  |  |  |  | 1) |
| 2) |
|  |  |  |  |  | 1) |
| 2) |

# Introduction

This document introduces the framework of Standards that are being developed to guide all entities that participate in the delivery of Mobile Financial Services (MFS) in the United Republic of Tanzania. This seamless delivery of MFS across all Mobile Financial Service Providers (MFSPs) is referred to as “Interoperability”.

The following Standards cover Bulk Payment transactions. A Bulk Payment transaction is the process by which an MFSP credits multiple Subscribers’ Financial Services accounts, held on e-Money platforms, with e-Value (referred to as “BP”).

Other services may be added from time to time with the agreement of MFSPs and will be covered in separate Standards documents applicable to the respective services.

In this document, we follow the GSM Association’s (GSMA’s) definition of Mobile financial services as: the use of a mobile phone to access financial services and execute financial transactions. This includes both transactional and non-transactional services, such as viewing financial information on a user’s mobile phone. Mobile money, mobile insurance, mobile credit and mobile savings are all mobile financial services.

The overriding vision is to achieve a nationally used and internationally recognised payments system.

## Effects

Becoming a signatory of these Standards will have the effect of compelling the signatories to apply; and each MFSP will acknowledge that it is bound to:

1. apply all the Standards in bilateral agreements with other members;
2. fulfil every obligation and duty required of it by the Standards in its bilateral agreements with other members; and
3. unless the parties have made applied for exemption and or made disclosure of such non-compliance.

As MFS Providers (MFSPs) put in place bilateral commercial agreements with signatories to these Standards, then those bilateral agreements should invoke these Standards.

If an MFSP wishes to put in place a commercial bilateral agreement with an MFSP that is not a signatory to these Standards, then such a commercial relationship need not invoke these Standards, but these Standards may be used by the non-signatory with the non-signatory having no right to vote on changes to these Standards.

If two MFSPs put in place a commercial bilateral agreement and both MFSPs do not wish to comply with certain aspects of these Standards, then areas of non-compliance should be recorded in the bi-lateral agreements and the BoT should be notified along with a compliance date if applicable.

## Governing Laws

The Constitution of the United Republic of Tanzania and various Acts of Parliament should be taken into consideration when executing MFSi. The main Acts are noted in Appendix A.

## Inconsistencies

If a provision in these Standards is inconsistent with a provision of the Constitution of the United Republic of Tanzania, the provision of the Constitution prevails.

If a provision of these Standards is inconsistent with a provision in the Laws named in Appendix A, the provision of Law prevails.

If a provision of these Standards is inconsistent with a provision of an MFSP’s internal rules for MFSi, the provision of these Standards prevails.

If a provision of these Standards is inconsistent with a provision of a bilateral agreement between the parties the provision of the bilateral agreement prevails.

# Governance

The MFSi BP Standards are owned and administered by a BP Governing Body (BPGB) on behalf of, and in the interests of, all organisations participating in BP MFSi (Participation criteria are defined in Section 6, below). The BPGB, taking a vote of all participating MFSPs, may make changes to these Standards, each MFSP having a single vote, irrespective of the size and transaction volume of the MFSP. A 75% majority is needed to make a change to these Standards.

The BPGB must be composed of representatives of MFSPs participating in BP. The MFSPs will elect representatives. The Chairman will serve for a one-year period and other representatives will serve a two-year period.

The BPGB should keep an up-to-date list of MFSPs and a primary and secondary contact person at each and so facilitate communication between MFSPs.

## Effective Date

The MFSi BP Standards will become effective and applicable upon signature.

## Amendments & Waivers

### Amendment to these Standards

The BPGB may amend these Standards at any time via circulars or any other means and following due process. The BPGB circular must specify the effective date of any change to these Standards.

Participating MFSPs may apply to the BPGB for a waiver from all or part of these Standards, unless a non-compliance disclosure has been made to the BPGB.

## Good Faith Co-operation

Each MFSP must:

1. perform its obligations under these Standards in good faith; and
2. use its best endeavours to co-operate with each other MFSP and the BPGB with respect to these Standards, and any subsidiary rule or documents.

# Participation in the BP Service

Any provider of Mobile Financial Services (MFS):

* Issuing e-money;
* Holding an e-money issuer license from the Bank of Tanzania as per the 2015 National Payments Systems Act;
* With a commercial agreement for interoperable BP service on the Receiver Pays Business model with at least 75% incumbent participants;
* Holding a current National Application Service License issued by the telecommunications regulator, the Tanzania Communications Regulatory Authority (TCRA).

may participate in the BP service will be known as an “MFSP”. The National Payments Act and Mobile Payments Regulations will guide the participation criteria and these Standards.

# Services & Service Architecture

## Services

The service described in this document is:

* Bulk Payments (“BP”).

## Functional Flows

The following page contains a generalised functional flow diagram for BP under the Service Architecture preferred by most MFSPs. These Standards recommend that:

* The BP file should go through two levels of internal approval by two different members of the Sending MFSP’s staff before the BP file is released for processing; and,
* The BP file should be encrypted by the Sending Entity using agreed encryption methods before being provided to the Sending MFSP for processing.

## Subscriber Verification

MFSPs will verify Subscribers against the counterparty MFSP database before final commitment of each transaction.



# Business model

* 1. **BPGB Costs**

In relation to the running and management of the BPGB each party is to carry its own direct costs and its share of any joint costs as agreed with the other participating parties.

* 1. **Mobile Interchange Structure**

The business model is a Receiver Pays Business Model with mobile interchange rates negotiated and agreed through bilateral agreements between participants. The following diagram shows an illustrative example of the Receiver Pays model:



* + 1. **Guiding principles:**

1. The business model and the mobile Bulk Payment (BP) Interchange will aim to achieve effective interoperability. Effective interoperability means:
2. Commercial rules and agreements are in place to enable interoperability
3. The inter-party pricing and fees agreed by participants, and are at a level that do not dis-incentivise any participant (MFSPs, sending entities, subscribers) from making or supporting cross network interoperable transactions.
4. Technical capability exists to enable transactions in real or near real time.
5. No surcharging is allowed for off-net transactions with an interoperability agreement where surcharging is the adding of a premium to the price of a transaction.
6. Mobile BP interchange will be used where necessary to achieve the balanced economics required to ensure that interoperability can be achieved. This may lead to different interchange rates for different use cases.
7. The BP interoperable business model is a “Receiver Pays” model. The receiving MFSP will pay the BP interchange to the sending MFSP (see diagram above).
8. Mobile BP interchange rates will be agreed between parties via a series of bilateral agreements between MFSPs.
9. MFSPs will calculate mobile BP interchange amounts due to/from each other periodically (daily, weekly, monthly) and bill/pay each other according to their bilateral agreements.
10. Subscriber and Sending Entity pricing remains the preserve of MFSPs, including the discretion to differentiate the Sending Entity send fee pricing between on and off network transactions.
11. The business model and the setting of mobile interchange rates will be compliant with all prevailing regulations.
12. Mobile BP interchange will be based on the net of all interoperable BP flows. Following the interchange calculation from this and from other use cases (e.g. P2P) interchange amounts due to/from participants can be netted off across multiple use cases with the agreement of the counterparty MFSP.
    * 1. **Fees for Failed and/or Disputed Transactions**

Fees may optionally be levied against Sending Entities, Receiving Subscribers, and/or other MFSPs as the case may be for recovery of disputed value.

Any Sending Entity or subscriber fees that may be charged for failed transactions or for the reversal of disputed transactions are at the MFSP’s discretion.

Where applicable and as may be agreed, these fees could be apportioned between the two MFSPs that participated in the interoperable transaction (sender and receiver MFSPs).

# Clearing and Prefunding

## General Principles of Clearing

### Provision of Information

Each MFSP agrees to provide all other MFSPs with sufficient and accurate information to allow all parties to clear and prefund MFSi transactions.

### Obligation to Credit

An MFSP is obliged to credit the account of the intended Subscriber when a valid BP transaction is received from a MFSP where the MFSP has provided sufficient liquidity to fund the transaction from the MFSP’s disbursal account on the Subscriber’s MFSP platform.

Minimum replenishment thresholds and alerts on the MFSP disbursal account must be maintained by the MFSP that owns the disbursal account.

### Returned Transactions

A Subscriber’s MFSP is obliged to return received e-Value to the MFSP sending the e-Value if the Subscriber’s MFSP is for any reason unable to credit the identified Subscriber’s account. Such a return should not take longer than 30 minutes.

### Responsibility for Transactional Errors

In the event of error by the MFSP sending e-Value, the onus to rectify the error is on the MFSP sending e-Value, but the Subscriber’s MFSP must endeavour to assist the MFSP sending e-Value to do so.

In the event of error by the Subscriber’s MFSP, the onus is on the Subscriber’s MFSP to rectify the error.

## General Principles of Prefunding

Due to the pre-funded model, MFSPs do not hold each other liable for post settlement obligations.

Each MFSP should ensure that they adequately prefund their disbursement account to cover all outbound cross-net transactions.

## Prefunding & Clearing Architecture



**Transaction steps and associated Account Transfers**

|  |  |
| --- | --- |
| 1 | Debit "A" Corporate eWallet Account |
| 2 | Credit "A" Collection Account |
| 3 | Send a Bulk Payment (Direct Credit) Message via API Interface |
| 4 | Debit “A" Disbursement Account on Platform “B” |
| 5 | Credit "B" Subscriber Account |
| 6 | Settle |

# General Operational Considerations

This chapter contains an overview of the Standards that govern the day-to-day operations of the MFSi service in Tanzania. Additional information is contained in Appendix B.

## Testing

All MFSPs participating in MFSi are expected to demonstrate due diligence and to test their respective systems so that the systems have:

* Integrity;
* Reliability;
* Consistency; and
* Scalability.

Note: MFSPs must develop technical test scripts once process and systems architecture have been finalised.

## System Support

All MFSPs should have in place tested processes for supporting the MFSi service once it has gone live. This should include the ability to trouble-shoot and fix network, hardware and software problems.

## Security

All MFSPs, without exception, are expected to take all reasonable steps to guarantee the security of MFS transactions and data.

As a matter of best practice, any BP data provided by Sending Entities to an MFSP should be encrypted using PKI keys or similar methodology.

## Money Laundering

All MFSPs must take reasonable steps specifically to combat Money Laundering and to detect suspicious activities such as smurfing and layering through the MFSi service (including the enforcement of transaction limits and velocity checks) and to comply with all current Legislation.

An annual Anti-Money Laundering self-audit of MFSi activity should be completed by MFSPs and submitted to the BoT on a schedule to be established by BoT.

The identity of all entities sending and receiving e-Value through the MFSi service must be checked by each MFSP using their own customer data before a transaction completes specifically for Anti-Money Laundering purposes. This will also increase efficiencies by reducing disputes and give a consistent Subscriber experience.

MFSPs should undertake regular Customer Due Diligence (CDD) to ensure that the MFSi BP facilities are not being used for ‘smurfing’ ML purposes.

## Know Your Customer (KYC)

Agents, Master Agents and MFSPs must take all reasonable steps to perform KYC checks on MFSi transactions in accordance with BoT directives and international best practice.

Sending Entities using any MFSI BP facilities to send e-Value should as a matter of best practice have a valid Tax ID Number.

To reduce the risk of MFSi transactions being disputed, MFSPs should to try to harmonise their KYC rules and processes unless doing so would contravene current legislation.

The MFSP sending e-Value should check the Subscriber MFSP’s Subscriber database before sending the transaction. The details held in the Subscriber MFSP’s Subscriber database would allow the MFSP sending e-Value to determine that the transaction was above the Subscriber’s limit and also other aspects of the Subscriber’s profile, if so desired. The MFSP would not then send the transaction, if it breached the Subscriber’s transaction and/or account limits but would refuse to accept it and would reply to the Sending Entity with an appropriate message whilst respecting the Subscriber’s confidentiality.

The Subscriber’s MFSP should check their Subscriber database before accepting the transaction. The details held in the Subscriber database would allow the Subscriber’s MFSP to determine that the transaction was above the Subscriber’s limit and also other aspects of the Subscriber’s profile, if so desired. The Subscriber’s MFSP would not accept the transaction if it breached the Subscriber’s KYC limit(s) but would refuse to accept it and would reply to the MFSP sending e-Value with an appropriate message whilst respecting the Subscriber’s confidentiality.

## Reporting

There will be three levels of reporting:

1. Internal reporting that an MFSP, Sending Entity, Super Agent or Master Agent produces for its own use;
2. Reporting required by BoT; and,
3. Ad hoc reporting.

### Fraud Reporting

Where there are patterns and particular modus operandi of fraudulent transactions detected in MFSi transactions, MFSPs must provide reports to BoT to a schedule defined by BoT.

If particular Sending Entities, Subscribers and/or Agents have been found by one MFSP to be regularly engaging in fraudulent activity or AML smurfing, the MFSPs may provide details of these activities to the BPGB and the BoT, in the framework allowed by the law. Such reporting would be over and above their legal obligations for AML Suspicious Activity Reports.

## Service Levels

MFSPs agree to maximise uptime, minimise latency, and notify counterparties in advance of foreseeable risks/issues.

## Retention of Records

All MFSPs must retain all records generated and/or obtained during the course of the operation and administration of MFSi for a period of at least ten years (or such other period as may be prescribed by an Act of Parliament or in any other applicable legislation) as from the date of each particular record.

## Business Continuity Planning

Each MFSP will make sure that it develops, introduces and maintains an effective and practical business continuity plan, relevant to MFSi systems and procedures, records, audit trails, recovery procedures and human resources, in order to ensure the effective continuity of its participation in the MFSi.

## Subscriber Support & Investigations

All MFSPs must have designated personnel and processes to undertake timely investigations of any complaints or queries raised by Sending Entities and Subscribers as well as by MFSi counterparties and the BoT.

Details of these designated personnel and Subscriber support processes must be updated as necessary and communicated to the BPGB.

## Bulk File Data Integrity

The Sending MFSPs should ensure that any Bulk Payment data provided to them by the Sending Entity is suitably formatted, encrypted and validated.

## Mobile Number Portability

In the case of Mobile Number Portability (MNP), and in the absence of a CSD containing ported numbers, it is also incumbent on the Sending Entity to ensure that the correct Recipient MFSP for each Recipient’s mobile phone number is entered into the database provided to the Sending Entity’s MFSP.

# Principles for the Management of Subscriber Disputes

## General Standards

The rules describing the Arbitration process for disputes between MFSPs are contained in a bilateral agreement.

Formal Arbitration should only begin after all avenues of amicable dispute resolution have been exhausted.

For the purposes of this section relating to Bulk Payment disputes, the entity sending e-Value may be an Enterprise or Small, Micro or Medium-sized Enterprise (SMME) (hereafter “Sending Entity”), who as part of a Bulk Payment process sends a payment to an individual Subscriber acting as a validated and authorised payee (hereafter “Recipient Payee”) using MFSi.

The Sending Entity initiating Bulk Payments through a Sending Entity’s MFSP must provide a properly formatted database to a Sending Entity’s MFSP that contains correct and updated Recipient mobile phone numbers and the appropriate Recipient’s MFSP details, as well as payment values confirmed for a particular Bulk Payment sending session. The Sending Entity MFSPs should ensure that any Bulk Payment data provided to them by the Sending Entity is suitably formatted, encrypted and validated.

### Applicable Laws & Jurisdiction

All processes and principles below are subject to, and may be superseded by, all applicable laws, regulations, circulars, and orders, in particular those outlined in Appendix A.

### Electronic Media As Evidence

In all cases MFSPs agree to accept audited electronic evidence in cases of disputes.

If a dispute arises over the electronic evidence itself and the parties cannot come to an agreement, then the PGB may call upon the services of an independent third party specialist auditor.

### Recipient MFS Opt-Out & Non-MFS Accounts

If value is sent to someone who, for whatever reason, does not have a MFS account, for the purposes of these Standards the transaction will not be considered as a Bulk Payment transaction.

### Reversals, Roll-Backs & Refunds

In cases where a transaction has to be reversed, rolled back, or refunded, the MFSPs must, where applicable, re-align their Collection and Disbursement Accounts and individual Sending Entity and Recipient accounts to reflect the values and fees. Such re-alignment should be completed in a timely manner.

### No Disintermediation

No MFSP may directly contact the Subscriber of another MFSP regarding a disputed transaction unless both MFSPs have pre-agreed to such contact.

### Subscriber Communications

In all cases of dispute, the MFSPs must maintain clear, accurate, timely and consistent communications to their Subscribers in both Swahili and English.

### Location Data

In the case of any dispute, location data of the transaction participants must be shared on request. This must be done in a timely manner so as to mitigate the risk of fraud and/or mistake.

### General Principles For The Recovery of Disputed Value:

A Recipient’s MFSP may, subject to the conditions below, generally attempt to recover any value that is subject to a dispute if the value in dispute has not been withdrawn from the Recipient’s MFS account.

Disputed values should be debited from Recipient’s account and be no longer visible, and similarly not available, to the Recipient. The disputed value should be held frozen or placed in a Suspense Account until the investigation into the dispute completes, whereupon the values are credited to the Recipient’s account or credited to the Sending Entity’s account, as the case may be.

Fees for the recovery of disputed values may be levied against Sending Entities, Recipients, and/or other MFSPs, as the case may be, at the discretion of the respective MFSP.

Where the dispute arose because of a system error, any applicable transaction fees shall be refunded to any affected parties.

### General Process To Report & Resolve Subscriber Disputes

The following is a general procedure that must be followed by MFSPs with respect to resolving disputes.

It is noted that any process for recovery of disputed values recognizes the relatively limited investigative capabilities MFSPs may have to inspect the merits of any disputes. As such, MFSPs should apply best efforts in attempting to resolve Bulk Payment disputes. The resolution process may however be modified according to whether there is a *prima facie* case of fraud, or where the Receiving MFSP has been ordered by an appropriate Authority or court to freeze and/or refund disputed values.

The process described below must be clearly explained in the T&Cs provided to Sending Entities and Recipient Payees.

Step 1: The Sending Entity calls their MFSP.

Step 2: Within 30 minutes of the dispute being raised by the Sending Entity, the Sending Entity’s MFSP contacts the Recipient’s MFSP. If both MFSPs agree, electronic messages may be used in place of telephone calls.

Step 3: The two MSFPs discuss the disputed transaction and if the funds are still in the Recipient’s account, the Recipient’s MFSP may freeze the disputed value from being used.

Step 4: The Recipient’s MFSP calls the Recipient and asks permission to initiate a transaction reversal and refund.

Step 5: If the Recipient agrees to the reversal, a reversal and refund process is executed and the Sending Entity is notified by the Sending Entity’s MFSP.

The Recipient’s MFSP proceeds to Step 6 if the Recipient does not agree to the reversal.

Step 6: The funds, if frozen in the Recipient’s account, are released by the Recipient’s MFSP once proper verification of the need for a reversal has been done by the Recipient’s MFSP.

Step 7: The Recipient’s MFSP contacts the Sending Entity’s MFSP to tell them that the funds cannot be recovered, and the reason why.

Step 8: The Sending Entity’s MFSP calls the Sending Entity to tell them that the funds cannot be recovered, providing the reason given to the Sending Entity’s MFSP by the Recipient’s MFSP.

Step 9: The Sending Entity may take separate steps such as legal action to recover the funds.

### Fraudulent Disputes

MFSPs must take all reasonable steps to make sure that transactions are not being disputed fraudulently. Only once an MFSP has determined to the best of their ability that a disputed transaction is genuine, may an attempt be made to recover the disputed value.

In all other cases, MFS accounts and values sent and/or received may be subject to being grey-listed, suspended, or transactions reversed, as the case may be, where directed by a court of law.

### Good Faith

The legal principle of Good Faith is used in banking law and will be generally applied to MFSi transactions.

This principle generally protects those who have received value in good faith from a Sending Entity who was originally not entitled to that value. The Sending Entity in this case may be an individual Subscriber who has, for whatever reason, incorrectly received value as part of a Bulk Payment processed and sent by a Sending Entity but meant for an authorised Recipient payee.

In such cases, the value received by a Recipient who was unaware of the origins of the value received should be frozen if still in the Recipient’s account and should not be automatically reversed by the Recipient’s MFSP without an investigation first having been conducted.

However, if it is suspected that fraud/collusion/bad faith has occurred, an MFS account may be suspended, or grey-listed, or the value received blocked from use while a legal investigation is conducted, and/or a court of law directs that this should be done and how it should be done.

### Time Frames For Dispute Response

MFSPs will allocate any reported disputes to appropriate personnel for immediate investigation and will endeavour to respond to disputes within 10 working days.

### Grey-Listing Of MFS Accounts

Grey-Listing is an MFSP process of only allowing certain transactions and/or use of value to take place on an MFS account. Generally this means that a grey-listed MFS account will only be able to accept in-bound transactions, and/or that specific values subject to a dispute may not be transacted by the holder of the MFS account.

Where there is a dispute regarding received value, the Recipient’s MFSP will apply their best judgement as to whether to grey-list the account of a Recipient.

Where there is *prima facie* evidence of fraud or other malpractices by a Sending Entity, MFSPs also have the option to grey-list the account of that Sending Entity.

### Network Delays

To avoid disputes arising from network delays, the two MFSP systems should exchange electronic handshakes. A ‘handshake’ is a term used to describe the process of one computer establishing or confirming a connection with another computer.

If the handshake is replied to, then the transaction will go though at a system level.

If the handshake is not replied to within an agreed number of seconds, then the handshake may be repeated an agreed number of times.

If all handshake attempts fail, then the MFSP system detecting the failure of a handshake should generate an error message and the transaction should automatically be reversed. In this case, the Sending Entity should not be charged a transaction fee.

All MFSPs agree that a problem ‘ticket’ should be created so that the root cause of the issue may be discovered and fixed.

All parties agree to resolve any technical issues as quickly as reasonably possible and to allocate resources 24 hours per day, 7 days per week to the resolution of technical issues.

## Specific Examples

This Section describes some of the areas for disputes for BP transactions in an MFSi environment and suggests processes for handling the dispute in each such case.

The following list is not exhaustive and further examples may be added from time to time:

### Money sent to the wrong user (“*error in personam*”)

There may be circumstances where a Sending Entity has sent value to an incorrect mobile phone number.

This may arise because the Sending Entity was initially provided with an incorrect mobile phone number by the payee (as the intended and authorised Recipient Payee). Or the mobile phone number initially provided by the Recipient Payee has since “churned” and is now allocated to a new MFSP Subscriber Or, the mobile phone number within a Bulk Payment database was incorrectly inputted by the Sending Entity despite it having been given the correct phone number by the Recipient Payee, and where the Sending Entity may have done so despite being given the opportunity to validate the Recipient’s details as provided by a CSD (if applicable).

Once the Sending Entity becomes aware of the error, a dispute may be initiated according to the process set out in clause **11.1.9** above.

### Recipient Sent More Value Than Intended

There may be circumstances where a Recipient Payee has been sent more value than the Sending Entity intended to send.

Once the Sending Entity becomes aware of the error, a dispute may be initiated according to the process set out in clause **11.1.9**, above.

### Transaction Not Received by the Recipient’s MFSP

There may be incidents where a Sending Entity has received confirmation from the Sending MFSP that the value and transaction fee have been debited from the Sending Entity’s MFS account, but it is found that the intended Recipient Payee has not received the value or part of the value.

Once the Sending Entity becomes aware of the error, a dispute may be initiated by the Sending Entity using the process set out in clause **11.1.9** above.

Appropriate remedies at an MFSP level will depend on where the fault lies. That is, either with the Sending Entity or Recipient MFSP, or with both MFSPs.

### Technical Issues With The Sending Entity’s MFSP

The Sending Entity’s MFSP should check logs of the Sending Entity’s transaction history via the Sending Entity MFSP’s Bulk Payment interface to determine if the transaction was successfully processed in the Sending Entity MFSP’s system and that the transaction data was sent to the Recipients MFSP’s system.

If the Sending Entity MFSP’s transaction logs indicate that the value was sent to the Recipient’s MFSP, then the Sending Entity’s MFSP should contact the Recipient’s MFSP to track the transaction.

If the transaction data was never received by the intended Recipient’s MFSP, then the Sending Entity’s MFSP should apply the following:

* Validate that the sending account was debited and locate the relevant credit in the applicable Suspense Account
* Reverse the transaction in the Sending Entity's MFS account by crediting the Sending Entity’s MFS account for the full value sent, as well as for the full transaction fee charged to the Sending Entity for that transaction, and
* Generate an error ticket with the technical team to inspect the relevant APIs and initiate testing so as to trace the transaction failure, and if needed, remedy any errors or deficiencies in the system to prevent any future similar occurrences. Inspection and remedy should take place within a reasonable period of time.

### Technical Issues With The Recipient Payee’s MFSP

If it is found that the Recipient’s MFSP’s system received the transaction data from the Sending Entity MFSP and that the Recipient Payee has a valid MFS account able to receive the full value, but for technical and/or operational reasons the Recipient Payee’s MFSP did not credit the value received to the Recipient’s MFS account, then the Recipient’s MFSP should apply the following:

* Immediately release the value and post the value to the Recipient’s account, notifying the Recipient thereof, and
* Notify the Sending Entity’s MFSP that the Recipient’s MFS account has been credited with the full, sent value.
* Generate an error ticket with the technical team to inspect the relevant APIs and initiate testing so as to trace the transaction failure, and if needed, remedy any errors or deficiencies in the system to prevent any future similar occurrences. Inspection and remedy should take place within a reasonable period of time.

### e-Value Only Partially Credited

Circumstances may arise when a Recipient does not receive the full e-Value expected from the Bulk Payment process. This may be, for example, the result of system issues and/or unauthorised charges.

If the full, correct values are not in the Recipient Payee’s account, the Sending Entity’s MFSP must be contacted so as to report the issue and to initiate an investigation.

The Sending Entity’s MFSP should generate an error ticket with their technical personnel to inspect the relevant APIs and initiate testing so as to trace the issue if needed, remedy any errors or deficiencies in the system so as to prevent any future similar occurrences. The time frame for such inspection and technical remedy should be less than 24 hours.

The time frame reverting to the Sending Entity and concluding the remedy related to incorrect e-Value should be less than 24 hours.

### Bulk Payment Notification Messages Not Received

Where a Bulk Payment Recipient/Payee has not received a usual SMS notification that confirms a payment from a Bulk Payment transaction, both the Sending Entity and Recipient Payee should immediately check their respective balances and last sets of transactions. The Recipient Payee should also be advised to check, and if needed clear, their Phone and/or SIM card memory to ensure that new SMSs can be received.

If the balances reflect the recent Bulk Payment, the Recipient Payee can wait to receive the delayed SMS notification of the Bulk Payment. The Recipient Payee should however contact their MFSP to report a delayed SMS notification.

The time frame for the MFSP reverting to the Recipient with any explanations or a resultant confirmatory SMS, or error ticket numbers, as the case may be, should be less than 24 hours.

# Risk management

All MFSPs in MFS should be aware of the risks they face and must take appropriate mitigating action for each and every risk.

To reduce the risk of MFSi transactions being disputed, MFSPs should to try to harmonise the wording of their Subscriber Terms & Conditions and wording used to report errors to Subscribers, unless doing so would contravene current anti-competition legislation.

Interparty settlement risk is mitigated to a large extent by the pre-funded nature of the business model.

All MFSPs should formally review the risks they face in MFSi at least every 6 months.

# General Standards of Compliance

All MFSPs will make reasonable efforts to comply with these Standards.

Detailed rules of Compliance are set out in **Appendix C**.

## Exemptions

Any MFSP may apply to the BPGB for an exemption from part of these rules if they feel that they have a valid reason.

To be fair and consistent, these Standards set out the procedures that all MFSPs should follow to apply for an Exemption as well as the procedures that must be followed when evaluating a request for an Exemption.

## Disclosure of Non-Compliance

If an MFSP that has signed this Standards document chooses not to comply with one or more of these Standards, the non-compliant MFSP will disclose its non-compliance to the BPGB who can then take impartial and appropriate steps to inform the Bank of Tanzania about the non-compliance and, if necessary, other MFSPs.

## Audit

MFSPs participating in BP will add MFSi to their existing statutory and internal audit process.

## Suspension & Termination

In the event of a termination of bilateral agreements, a participant may no longer qualify for participation in interoperable BP and would thus be terminated from this agreement.

In addition, an MFSP may voluntarily withdraw from participation in MFSi in accordance with Appendix C.

## Notices

The BPGB has to notify MFSPs of a change in these Standards in a timely, even-handed and consistent manner.

## Liability for owned & controlled entities

If an MFSP owns a subsidiary company that participates in MFS in Tanzania, then the MFSP is responsible for the actions of its subsidiary.

## Disclosures & Confidentiality

All MFSPs and the BPGB have an obligation of confidentiality to all other MFSPs. A statement of Confidentiality is in the Appendices.

# Appendix A – Governing Laws

The Constitution of the United Republic of Tanzania and the following Acts of Parliament should be taken into consideration when executing MFS:

### Telecommunications-related oversight of MFS

1. Tanzania Communications Regulatory Authority Act 12 of 2003
2. Electronic And Postal Communications Act of 2010

### Anti-money laundering laws, guidelines, circulars & regulations

1. Anti-Money Laundering and Proceeds of Crime (Amendment) Act, 10 of 2009 – for Tanzania Zanzibar - AMLPOCA (Consolidated version)
2. Written Laws (Miscellaneous Amendment) Act 12 of 2011 - for Tanzania Zanzibar
   * 1. including Amendment of the Anti-Money Laundering and Proceeds of Crime Act 10 of 2009
3. Anti-Money Laundering and Proceeds of Crime Act 10 of 2009 - for Tanzania Zanzibar (AMLPOCA)
4. Anti-Money Laundering Act, Cap. 423 of 2006 - for Tanzania Mainland (AMLA)
5. Anti-Money Laundering Amendment Act of 2012 [FIU]

### Competition & consumer protection

1. Fair Competition Act 8 of 2003 (FCA)

### Financial regulation

1. National Payment Systems Act of 2015
2. Bank of Tanzania Act 4 of 2006
3. Banking and Financial Institutions Act 5 of 2006

### Auditing & Accounting regulation

1. The Auditors and Accountants (Registration) Act No. 33 of 1972, as amended by Act No. 2 of 1995; and
2. The Companies Act of 2002

Participants should familiarise themselves with these Acts and with the other Guidelines, Circulars & Regulations issued by the competent authorities from time to time.

# Appendix B - Operational Requirements

## Testing

On behalf of the Participants, the BPGB may from time to time require one or more MFSPs to test their ability to comply with these Standards

The Participant must:

1. comply with the BPGB’s requirements; and
2. co-operate with the other Participant(s) involved.

Whenever practicable in the circumstances the BPGB will:

1. consult with the affected Participant as to the scheduling of any testing requirement; and/or
2. give the affected Participant reasonable notice of any testing requirement.

## Operational and Security Standards

The BPGB may, from time to time with the agreement of and on behalf of all Participants issue and amend Standards applicable to the technical, operational and security aspects of:

1. MFS Transactions;
2. MFS Interoperability activities;
3. any other matter covered by these Standards;
4. any other matter related or incidental to these matters.

To assist in interpretation of, supplement or provide processes for implementation of matters contained in these Standards the BPGB may from time to time issue (and update) Guidelines. Participants must comply with Guidelines and ensure that their Service Providers do so also.

## Data Security

A Participant that receives Data in respect of a Subscriber of another Participant while participating in an MFSi Transaction must:

1. only use that Data to comply with its obligations under these Standards and/or the Operational and Security Standards;
2. treat that Data as Confidential Information;
3. take all reasonable measures to ensure that Data is protected against loss and unauthorised:
4. access;
5. use;
6. disclosure; or
7. modification; and

(v) ensure that any person who is given access to the Data is made aware of, and undertakes to comply with, the obligations in this clause.

## Prevention of Money-laundering

The movement of money through the MFS Interoperability service which is or which forms part of the proceeds of any crime or which is intended to facilitate, aid or finance the commission of any crime is expressly prohibited.

Participants must ensure that all their staff responsible for the MFSi services comply and are up to date with all Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) laws, regulations, standards or directives in force from time to time, including any guidelines, policies and procedures to that effect as may be issued by the Bank of Tanzania.

Participants will monitor and report any suspicious activity in relation to MFSi services under these rules to its Money Laundering Reporting Officer (MLRO) who may eventually escalate the suspicious activity to the relevant law enforcement authority.

A Participant shall be entitled to terminate their participation in the MFSi service in the event that they or another Participant reasonably and in good faith determines that there has been a breach of AML obligations set out in these Standards.

## Reporting

All reporting will comply with BoT reporting requirements.

# Appendix C - Compliance

## Exemptions & Waivers

### Waivers from the Standards

Participants may request a variance to allow non-compliance with a provision of the MFSi Standards, provided that it does not endanger the overall application of the Standards for other Participants. A variance will only be considered where there are special circumstances, which make such variance appropriate for the Participant requesting it, but not for Participants in general.

A request for a waiver must be submitted in writing to the BPGB, together with a statement of the reasons for the request and any appropriate evidence.

If the waiver is granted, the applicable Participant must advise the BPGB if the waiver is no longer required. The BPGB may also modify or cancel the variance, with a reasonable period of notice.

### Application for an Exemption

A Participant may apply for an exemption from a requirement in these rules.

An application for an exemption must include the following:

1. the period for which the exemption is sought;
2. the date of the original exemption (if seeking an extension of an existing exemption);
3. the section(s) and requirement(s) of these Standards from which the Participant seeks an exemption;
4. a statement of the reason(s) for non-compliance;
5. a risk rating applicable to the non-compliance;
6. a full description of any compensating controls that are offered as justification for the exemption; and
7. details of the Participant’s action plan to achieve compliance, including the expected date of achieving compliance.

Upon receipt of an application for an exemption, the BPGB may require the Participant to provide additional information or evidence before it determines the application.

### Determination of an Application for an Exemption

The BPGB will determine an application for an exemption as soon as possible and will notify the applicant in writing of the outcome.

The BPGB may grant an exemption:

1. for a limited period of time; and/or
2. subject to conditions on the applying Participant’s activities pursuant, or related, to these Standards.

If the BPGB grants an exemption, subject to compliance with any time period or conditions imposed, the Participant receiving the exemption is not required to comply with the relevant section(s) and requirement(s) of these Standards.

In determining an application for an exemption, the BPGB will have regard to the reputation, integrity, security, reliability and stability of MFS Transactions, MFS Interoperability activities and/or the settlement resulting from them.

The BPGB may, at any time, withdraw an exemption if in the BPGB’s opinion the exemption poses a risk to the reputation, integrity, security, reliability and stability of MFS Transactions, MFS Interoperability activities and/or the settlement and clearing resulting from them.

Prior to making a decision to refuse an application for an exemption, to grant an exemption subject to conditions or to withdraw an exemption, the BPGB must comply with the procedures set out in these Standards.

Any decision of the BPGB in respect of an application for an exemption is final and binding.

## Disclosure of Non-Compliance

Each Participant must disclose by notice in writing to the BPGB:

1. each and every instance of non-compliance with these Standards; and
2. its inability to comply with any section(s) or requirement(s) of the Standards, within 7 days of the Participant becoming aware of the non-compliance or its inability to comply.

## Audits

Participants are required to use their annual statutory and internal audit processes to ensure compliance with these Standards, particularly with regard to security, business processes, operations and fraud.

A copy of the annual audit report as it relates to Interoperable MFS is to be provided to the Bank of Tanzania.

## Suspension & Termination

### Immediate Suspension

A Participant is suspended immediately upon:

1. becoming insolvent or making an arrangement or composition with creditors generally;
2. being wound up, dissolved or otherwise ceasing to exist;
3. failing to settle for the obligations it has incurred under these Standards;

Suspension under this clause will continue until the Participant ceases to be a Participant; or

the BPGB is satisfied that:

1. the Participant is solvent and capable of settling for the obligations it incurs under these Standards on an on-going basis and the Participant has settled all outstanding obligations which it has incurred under these Standards; and
2. if capable of rectification, the Participant has rectified any breach of these Standards associated with its suspension.

### Other reasons for Suspension

The BPGB may suspend a Participant if:

1. the Participant fails to comply with, or is incapable of complying with these Standards unless that MFSP has made the necessary application for waiver and or disclosure of non-compliance or
2. the Participant no longer satisfies the applicable requirements for membership set out in these Standards;
3. the Participant was admitted and then there is in the BPGB’s opinion a material change in the Participant’s circumstances and such change requires the suspension of the Participant to preserve the reputation, integrity, security, reliability and stability MFS Transactions, MFS Interchange Activities and/or the settlement resulting from them;
4. the Participant requests that it be suspended;
5. the Participant fails to pay any fees due to the BPGB or another Participant.

Suspension will continue until the BPGB is satisfied that the Participant has addressed the circumstance(s) that caused the suspension.

### Effect of Suspension

While suspended a Participant is not entitled to:

1. Vote on any matter tabled for BPGB Decision
2. Participate in BPGB discussions

### Withdrawal of Participants

A Participant is allowed to withdraw as a Participant by giving the BPGB 90 calendar days written notice.

### Obligations of Cessation

If a Participant is suspended, expelled or withdrawn, the Participant will nevertheless remain liable for all its accrued and accruing obligations under these rules. There are no limits to this.

### Compliance with these Standards

Any termination of a Participant will not affect any right or liability arising under these Standards prior to the date such termination takes effect or arising in respect of any act, matter or thing occurring prior to that date, including obligations to comply with any requirements relating to its ceasing to be a Participant.

## Liability for owned & controlled entities

An MFSP that owns or controls, is owned or controlled by, or is under common ownership or control of another entity is liable to all other MFSPs for all of that entity’s obligations under these membership rules and for all of the entity’s activities related to MFS Interoperability.

It is the responsibility of each Participant to assure the onward connection from the MFS Interoperability Service to any other entity or third parties for completing the transaction cycle.

## Disclosures

Unless required to do so by law, no Participant may disclose, fully or partially, to any third party, any documentation, related to the fees and any other statistical information related to the operation of the MFS Interoperability Service.

For these purposes, confidential information shall include, but not be limited to, Transaction volumes, charges, fees and any other statistical information related to the operation of the Interoperability Service.

Information not previously disclosed to the public concerning any Participant or Service that is under consideration for inclusion in the operation of the Interoperability Service.

## Confidentiality

The BPGB on behalf of the MFSi Participants maintains these Standards. These standards should be in the public domain and there should be encouragement to apply these standards in all exchanges of e-Value not only those where the parties are signatory to these guidelines.

Confidential information shall include Transaction volumes and any other statistical information related to the operation of the Interoperability Service.

# Appendix D - Arbitration

Formal Arbitration should only begin after all avenues of amicable dispute resolution have been exhausted.

In the event that any dispute has arisen and the Participants have not been able to settle the same, within thirty days (30), then any Participant involved in the dispute may elect to go to arbitration. Each Participant shall appoint one arbitrator and the Participants involved in the dispute shall jointly appoint a chairperson. The three-person panel shall conduct the arbitration. The appointment of Arbitrators and other conditions of Arbitration will be defined in the bilateral agreements.

To the extent permissible by Law, the determination of the majority Arbitrators shall be final, conclusive and binding upon the Participants.

Pending final settlement or determination of a dispute, the Participants shall continue to perform their subsisting obligations under these Standards.

Nothing in this Clause shall prevent or delay a Participants seeking urgent injunctive relief in a court having jurisdiction.

# Appendix E - Warranties

At all times each Participant represents and warrants to all other Participants and the BPGB that:

(i) it has the power to observe its obligations under these Standards; and

(ii) it performs its obligations in good faith;

(iii) except as contained in these Standards, it has not relied on any representation made by any other Participant or the BPGB to induce it to become a Participant or otherwise act in accordance with these Standards; and/or

(iv) it has made (without reliance on any other Participant or the BPGB) its own independent assessment of these Standards as being appropriate for its needs and requirements; and

(v) its obligations under these Standards are valid and binding on it.

# Appendix F – Application for Exemption

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Exemption Application Form** | | | | | | | | | | | | | | |
| Date of Request |  | |  | |  | |  | |  | |  | |  | |
|  |  | |  | |  | |  | |  | |  | |  | |
| Section number of requirement | Requirement for which Participant is not in compliance | | Reason for non-compliance | | Risk (Potential impact) | | Risk (Likelihood) | | Mitigating actions | | Residual risk | | Action to be taken and timeframe | |
| *Section from the Standards or the Technical Operational and Security Standards* | *Type in the actual wording of the Requirement with which you are not complying* | | *Describe the situation, including when and why out-of-compliance occurred.* | | *Describe the risks the out-of-compliance situation poses & its possible impact in terms of "Low", "Medium", "High".* | | *Describe the risks the out-of-compliance situation poses & how likely it is to happen in terms of "Low", "Medium", "High".* | | *List the compensating controls that reduce the risk* | | "Low", "Medium", "High". | | *List what you are doing to correct the non-compliance. For extension requests Indicate the reason for seeking an extension and give a promised date of correction.* | |
|  |  | |  | |  | |  | |  | |  | |  | |
|  |  | |  | |  | |  | |  | |  | |  | |
| Agreement to Disclosure: Where applicable I authorise the BP Governing Body to provide the Bank of Tanzania (BoT) with a copy of this exemption request. | | | | | | | | | | | | | | |
|  | |  | |  | |  | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |  | |  | |
| Name: | |  | | Position: | |  | | Signature: | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |  | |  | |

# Appendix G –Interpretation

Terms used in these Standards have the meaning given to them in the Constitution of the Republic of Tanzania or any applicable laws in the Republic of Tanzania. Where there is more than one meaning to a term in any applicable laws, the meaning in the most recent law will prevail.

The words in the Standards’ Glossary are commonly used in discussing MFS interoperability and have the meanings shown in the Glossary when used in these Standards, unless the contrary intention appears.