Terms and Conditions for eBanking

(Version 0.1., Date: 06.12.2021)

1. Services Offered

1.1

The holder of an account/securities account can process banking transactions via eBanking, to the extent offered by the Neo-Microfinance. Furthermore, he/she can access information from the Neo-Microfinance via eBanking. Using eBanking, the Customer additionally has the right to make use of a payment initiation service provider in accordance with regulations in order to issue a payment order and to request account information using an account information service provider in accordance with regulations.

1.2

Account/securities account holders and authorised persons shall hereinafter be referred to as "Participants". Accounts and securities accounts shall hereinafter be referred to as "Accounts".

1.3

With regard to the usage of eBanking, the credit limits agreed separately with the Neo-Microfinance shall apply.

2. Conditions for the Use of eBanking

In order to be able to process banking transactions via eBanking, the Participant requires the Personalised Security Features and Authentication Instruments agreed with the Bank in order to prove to the Neo-Microfinance his/her identity as a legitimate Participant (see Section 3) and in order to authorise orders (see Section 4). Instead of a Personalised Security Feature, a biometric feature can be agreed for the purpose of authentication or authorisation. This process shall be named Authentication Process.

2.1 Personalised Security Features

Personalised Security Features are personalised features which the Neo-Microfinance provides to the Participant for the purpose of Authentication. Biometric features or Personalised Security Features, which can also be alphanumerical, are, e.g.::

- the unique combination of email address and a password, which the Participant sets upon opening the account itself, with which he/she can log in to the end Customer interfaces,
- as well as the PIN, with which the Participant can release payment transactions on request. The end Customer can assign this PIN him/herself using the procedures described in the MIQO Support Center.

2.2 Authentication Instruments

The combination of a smartphone that is initially associated with the Participant's account and a personalised security feature serves as an Authentication Instrument. Only with this combination can the Participant release payment transactions. For more information on linking smartphones and their cancellation, visit the MIQO Support Center.

3 Access to eBanking

Participants are provided with access to eBanking

- after having transmitted the account number or the individualized Customer identifier and the PIN or electronic signature or the biometric feature,
- when the verification of these data by the Bank has shown that the Participant is authorised to access eBanking, and
- provided that access is not blocked (see Sections 8.1 and 9).

Once access to eBanking has been granted, the Participant will be able to retrieve information or to place orders. Sentences 1 and 2 equally apply if the Participant issues payment orders via a payment initiation service provider or requests account information via an account information service provider (see Section 1.1 Sentence 2).

4 eBanking Orders

4.1 Placement of orders and authorisation

In order for eBanking orders (e.g. bank transfers) to be valid, the Participants have to authorise them with the provided Personalised Security Feature or with a comparable agreed biometric security feature, and transmit them to the Neo-Microfinance via eBanking. The Neo-Microfinance confirms receipt of the order via eBanking. Sentences 1 and 2 equally apply if the Participant issues and transmits a payment order via a payment initiation service provider (see Section 1.1 Sentence 2).

4.2 Withdrawal of orders

Whether an eBanking order can be withdrawn depends on the special terms applicable to the relevant type of order (for instance, terms for Neo-Microfinance transfers). Orders can only be withdrawn outside the eBanking system, except if the Bank expressly offers a withdrawal option within the eBanking system.

5 Processing of eBanking Orders by the Neo-Microfinance

5.1

eBanking orders are processed on the business days specified for the processing of the relevant type of order (e.g. bank transfer) on the Neo-Microfinance's eBanking site or in the List of Prices and Services, within the framework of regular work processes. If the order is received after the time specified on the Neo-Microfinance's eBanking site or set out in the "List of Prices and Services" (receipt deadline), or, if the time of receipt is not a business day in accordance with the Neo-Microfinance's "List of Prices and Services", such orders shall be deemed to have been received on the following business day. Processing will only commence on this day.

5.2

The Neo-Microfinance will execute the order if the following conditions are

fulfilled: ● The Participant authorises the order;

- the Participant has proven his/her identity by means of the Personalised Security Feature;
- the authorisation for the Participant for the relevant type of order (e.g. securities order) has been issued;
- the eBanking data format is being complied with;
- the separately agreed eBanking credit limit is not being exceeded;
- the additionnal processing conditions according to the special terms applicable to the relevant type of order (e.g. sufficient deposit on the account, in accordance with the terms for bank transfers) are being fulfilled.

If the processing conditions under Sentence 1 are fulfilled, the Neo-Microfinance will process the eBanking orders in accordance with the provisions of the special terms applicable to the relevant type of order (e.g. terms for bank transfers).

5.3

If the processing conditions under Paragraph 2 Sentence 1 are not fulfilled, the Neo-Microfinance will not process the eBanking order, and will provide the Participant with information via eBanking regarding the fact that the order will not be processed and, if possible, of the reasons for this decision and the options of correcting the mistake which led to the rejection.

6 Information for the Account Holder on eBanking Transactions

The Neo-Microfinance will inform the Account Holder at least once per month of the transactions made via eBanking, via the means of communication agreed for account information.

7 Participant's Diligence Obligations

7.1 Technical connection to eBanking

The Participant is obligated to only technically connect to eBanking via the eBanking access channels (e.g. internet address) provided separately by the Neo-Microfinance. The Participant may also establish a technical connection to eBanking via a payment initiation service provider for issuing payment orders or via an account information service provider for requesting account information (see Section 1.1 Sentence 2).

7.2 Confidentiality of Personalised Security Features and secure storage of Authentication Instruments

(1) The Participant shall be obligated

- to keep confidential his/her Personalised Security Features (see Section 2.1), and
- to store his/her Authentication Instrument (see Section 2.2) secured against access by third parties. The reason for this is that any person who is in possession of the Authentication Instrument can, in combination with the associated Personalised Security Feature, use the eBanking procedure in an abusive manner. For eBanking, the obligation to confidentiality concerning the Personal Security Features according to Sentence 1 is not breached if the Participant transmits the Personal Security Features to issue a payment order or to request information on Participant's payment account to the payment initiation service provider or to the account information service provider of Participant's choice.

(2) The following will in particular have to be observed in order to protect the Personalised Security Feature and the Authentication Instrument:

- The Personalised Security Feature must not be stored electronically in an unsecured way outside of the permitted Authentication process (e.g. on a terminal device or in the Customer system).
- When entering the Personalised Security Feature, it must be ensured that other persons cannot spy out such features.
- The Personal Security Feature must only be entered within the Authentication processes permitted by the Neo-Microfinance - this also applies when the Participant uses a payment initiation service provider or an account information service provider.
- The Personalised Security Feature must not be forwarded outside the eBanking procedure, i.e. for instance not by e-mail.
- The password and the PIN for releasing transactions may not be stored together with the Authentication Instrument.

- To increase the security of your Personal Data the combination of your email address and your password (used for the MIQO app) must not be used for any other service.

7.3 Safety instructions by the Neo-Microfinance

The Participant must comply with the safety instructions on the Neo-Microfinance's internet pages relating to eBanking, in particular the measures for the protection of the hardware and software used (Customer System).

7.4

Verification of order data with the data displayed by the Bank In as far as the Bank displays data from an eBanking order (e.g. amount, recipient's account number, securities ID) in the Customer System or via another device used by the Participant (e.g. mobile telephone, chip card reader with display) to the Participant for confirmation, the Participant shall be obligated to verify prior to confirming such data that the displayed data correspond to the data required for the transaction. 8 Notification and Information Obligations

8.1 Blocking notification

(1) Should the Participant detect

- the loss or theft of the Authentication Instrument,
- an improper use or
- otherwise unauthorised use of his/her Authentication Instrument, the Participant shall inform the Neo-Microfinance thereof immediately (blocking notification). The Participant can issue a blocking notification to the Neo-Microfinance at any time, also via the contact data provided separately to him/her.

(2) The Participant shall immediately report any theft or improper use to the police.

(3) Should the Participant suspect that another person

- is in possession of his/her Authentication Instrument or has knowledge
- of his/her Personalised Security Feature, or
- uses the Authentication Instrument or the Personalised Security Feature without authorisation, he/she shall also issue a blocking notification.

8.2 Information on unauthorised or incorrectly processed orders

The Account/Securities Account Holder shall inform the Neo-Microfinance immediately should he/she detect that an order was processed without authorisation or incorrectly.

9 Blocking

9.1 Blocking upon the Participant's request

The Neo-Microfinance, upon a request by the Participant, in particular in the event of a blocking notification pursuant to Section 8.1, will block

- eBanking access for him/her or all participants, or
- his/her Authentication Instrument.

9.2 Blocking upon the Neo-Microfinance's initiative

The Neo-Microfinance may block eBanking access for a Participant if

- it has the right to terminate the eBanking contract for cause,

- this is justified due to objective reasons in connection with the security of the Authentication Instrument or the Personalised Security Feature, or
- there is a suspicion that the Authentication Instrument is being used in an unauthorised or abusive manner.

The Neo-Microfinance will inform the Account/Securities Account Holder of such blocking, including the reasons for such blocking, prior to, or at the latest immediately after the blocking.

9.3 Lifting of Blocking

The Neo-Microfinance will lift the blocking or exchange the Personalised Security Feature or Authentication Instrument when the reasons for the blocking have ceased to apply. It shall inform the Account/Securities Account Holder thereof without delay.

9.4 Automatic blocking of a chip-based Authentication Instrument

The chip card with signature function will block itself automatically if the user code for the electronic signature is entered incorrectly three times in a row.

The Authentication Instruments specified in Sentence 1 above can no longer be used for eBanking. The Participant will have to contact the Neo-Microfinance in order to reinstate the possibility of using eBanking.

10 Liability

10.1 The Neo-Microfinance's liability for unauthorised eBanking transactions and eBanking transactions which are not carried out, not carried out correctly or carried out late

The Neo-Microfinance's liability for unauthorised eBanking transactions and eBanking transactions not carried out, not carried out correctly or carried out late shall be governed by the special terms agreed for the relevant type of order (e.g. terms for bank transfer transactions, terms for securities transactions).

10.2 Account Holder's liability in the event of an abuse of a biometric feature or a Personalised Security Feature or of an Authentication Instrument

10.2.1 Account Holder's liability for unauthorised payment transactions prior to the blocking notification

(1) If unauthorised payment transactions prior to the blocking notification are due to the usage of an Authentication Instrument which has been lost, stolen or has otherwise disappeared or to any other misappropriation of an Authentication Instrument,, the Account Holder will be liable to the Neo-Microfinance for any damage caused to the Neo-Microfinance, up to an amount of 35000FCFA, irrespective of the Participant's responsibility.

(2) The Account Holder is not obligated to reimburse damage under Paragraph 1, if

- it was not possible for the Account Holder to notice the loss, theft, any other disappearance or any other misappropriation of Account Holder's Authentication Instrument prior to the unauthorised payment transaction, or
- the loss of the Authentication Instrument was caused by an employee, an agent, a subsidiary of a payment service provider or any other entity to which the payment service provider has outsourced its activities.

(3) If unauthorised payment transactions occur prior to the blocking notification, and if the Participant has acted with fraudulent intent or has intentionally or in a grossly negligent manner failed to fulfil the notification and diligence obligations under

these Terms and Conditions, the Account Holder shall bear the full damage incurred by way of derogation from Paragraphs 1 and 2. The Participant may in particular be deemed to have acted in a grossly negligent manner if he/she

- has failed to inform the Neo-Microfinance of the loss or theft of the Authentication Instrument or the misappropriation of the Authentication Instrument or the Personalised Security Feature immediately after obtaining knowledge thereof (see Section 8.1 Paragraph 1),
- has stored the Personalised Security Feature electronically in an unsecure way (see Section 7.2 Paragraph 2 item 1)
- Has not kept the Personalised Security Features confidential, and if the abuse was caused by this (see Section 7.2 Paragraph 1 item 1),
- has forwarded the Personalised Security Feature outside the eBanking procedure, e.g. via email (see Section 7.2 Paragraph 2 item 4),
- has stored the Personalised Security Feature on the Authentication Instrument, or has stored it together with the Authentication Instrument (see Section 7.2 Paragraph 2 item 5),

(4) By derogation from Paragraphs 1 and 3, the Account Holder is not liable for damages if the Neo-Microfinance has not required a strong customer authentication in accordance with regulations although the Neo-Microfinance was obligated to require a strong customer authentication according to regulations. A strong customer authentication requires in particular the usage of two independent elements from the categories knowledge (something only the Participant knows, e.g. PIN), possession (something only the user possesses, e.g. TAN-generator) or inherence (something the user is, e.g. finger print).

(5) The liability for damage caused during the period for which the credit limit applies shall be limited to the agreed credit limit.

(6) The Account Holder is not liable for damages in accordance with Paragraph 1 and 3, if the Participant could not give the blocking notification in accordance with Section 8.1 because the Neo-Microfinance had not secured the possibility of receiving the card blocking notice.

(7) Paragraphs 2 and 4 - 6 do not apply if the Participant has acted with fraudulent intent.

(8) If the Account Holder is not a consumer, the following applies additionally:

- The Account Holder is liable for damages caused by unauthorised payment transactions beyond the liability limit of 35000FCFA under Paragraphs 1 and 3 if the Participant has intentionally or in a negligent manner failed to fulfil the notification and diligence obligations under these Terms and Conditions.
- The limitation of liability according to Paragraph 2, item 1) does not apply.

10.2.2 Liability for unauthorised securities transactions prior to the blocking notification

If unauthorised securities transactions prior to the blocking notification are due to the use of a lost or stolen Authentication Instrument or a different misappropriation of the Personalised Security Feature or of the Authentication Instrument, and if the Neo-Microfinance has incurred damage due to this, the Securities Account Holder and the Neo-Microfinance shall be liable in accordance with the statutory principles of contributory negligence.

10.2.3 Neo-Microfinance's liability after blocking notification

As soon as the Neo-Microfinance has received a blocking notification from a Participant, the Neo-Microfinance shall assume any damage incurred after this time due to unauthorised eBanking transactions. This shall not apply if the Participant has acted with fraudulent intentions.

10.2.4 Exclusion of liability

Liability claims shall be excluded if the circumstances which give rise to a claim are due to unusual and unforeseeable events which the Party invoking such event cannot influence, and the consequences of which could not have been avoided even if the required level of diligence had been applied