APPROVED by
Resolution of
the Supervisory Board of JSC NSPC
(minutes No. 13 dated 1 October, 2015)

MIR PAYMENT SYSTEM

REGULATIONS

APPENDIX 4

TRANSACTION RULES

The official language of the Mir Payment System Regulations (Version 1.0, Moscow 2015) is Russian and in case of any discrepancies between the original Regulations and the English version of the Regulations, the Russian version prevails.

Version 1.0

Moscow. 2015

CONTENTS

1. General Transactions Procedure

The System provides for the following Transactions:

- with presentation of the Card when the Cardholder is present during a Transaction (assisted (attended) by personnel of a merchant or an Acquirer/not assisted (attended) by personnel of a merchant or an Acquirer).

In order to reduce the risk of transactions conducted without the Cardholder's consent, including but not limited to those conducted using a Card by a person other than the Cardholder, using a counterfeit Card and unlawfully using card details (fraudulent transactions), Acquirers should ensure that Transactions with presentation of the Card in the Acquirer's Network of Devices are carried out using the Card microprocessor.

In the case of a Transaction using the magnetic stripe or manual entry of Card details, which is further found fraudulent, responsibility for the risks associated with such a fraudulent transaction will be borne by the Acquirer.

In the case of a Transaction using the Card microprocessor, responsibility for the risks associated with such a Transaction will rest with the Issuer, if the performance of the Transaction and its submission for clearing by the Acquirer complied with the System's Regulations and Standards.

- without presentation of the Card when the Cardholder is absent during a Transaction (an employee of a merchant or an Acquirer has no physical access to the Card).

In order to reduce the risk of fraudulent transactions, Issuers and Acquirers should ensure that Transactions without presentation of the Card use a reliable authentication technology designed to enhance security of Transactions on the Internet. The procedure for Transactions using the reliable authentication technology is the System's Standard and is posted on the System's Information Resource.

If a Transaction is conducted without reliable authentication and is further found fraudulent, responsibility for the risks associated with such a Transaction will be borne by:

- the Acquirer, provided that the Issuer maintains the reliable authentication technology;
- the Issuer, provided that the Acquirer maintains the reliable authentication technology;
- the Acquirer, provided that neither the Issuer nor the Acquirer maintains the reliable authentication technology;

In the case of a Transaction using the reliable authentication technology, responsibility for the risks associated with such a Transaction will rest with the Issuer, if the performance of the Transaction and its submission for clearing by the Acquirer complied with the System's Regulations and Standards.

In the case of a Cash Advance Transaction with manual entry of Card details, using the codes and passwords provided by the Issuer, responsibility for the risks associated with such a Transaction will rest with the Issuer, if the performance of the Transaction and orders thereon given by the Acquirer complied with the System's Regulations and Standards.

Transaction amount

Participants may not set the minimum Transaction amount. The Operator may set the maximum amount for one Transaction per Transaction type.

Authorisation

All Transactions in the System require the Issuer's Authorisation, including those for and on behalf of the Issuer, using the Backup Authorisation Service.

The Issuer and the Acquirer must ensure 24-hour Authorisation, independently and/or using the Backup Authorisation Service.

The System provides for Authorisation:

- in the on-line mode when Authorisation requested from the Issuer in real time, with an Authorisation Request made to the Operating Centre (On-line Transaction);
- in the off-line mode when Authorisation is provided by the Card's payments application without submitting an Authorisation Request to the Operating Centre (Off-line Transaction).

Both Authorisation types are equal and considered in equal measure to be a legally competent expression of the Issuer's stand on carrying out the relevant Transaction in the Acquirer's Network.

Transactions using the magnetic stripe or manual entry of Card details must be conducted with Authorisation in the On-line mode only.

Transactions using the Card microprocessor is only admissible with Authorisation in On-line and Off-line modes.

Off-line Transactions are conducted under authorisations specified by the Issuer in the Card payments application.

In the case of an Off-line Transaction, the Acquirer must ensure that the Card Off-line limit must be verified. If the amount of such a Transaction exceeds the Card Off-line limit, Authorisation must be effected in the On-line mode.

In the case of an Off-line Transaction, the Acquirer must ensure that the Card use limits is verified against the current Stop List.

If a Transaction is denied, the Cardholder must be provided with information on such Transaction denial and reasons therefor.

Card verification when conducting Transactions at merchants and CAOs with attendance of personnel

In the case of Card Transactions at merchants or CAOs, the designated employee should make sure there are no marks of forgery or damage (mechanical damage in the area of the microprocessor pad, magnetic stripe, Cardholder's signature panel, System hologram; marks of regluing the microprocessor pad, magnetic stripe, Cardholder's signature panel, System hologram; changes/erasures in the Card number, last four digits thereof, CVV2, Cardholder's signature etc.)

In the case of a Transaction using the Card magnetic stripe, the designated employee should additionally perform the following steps:

1. make sure that the Card has a microprocessor, System hologram, System trademark or Logo, Cardholder's signature panel or the Cardholder's signature photographic image;
2. pay attention to the Card expiry date on the Card face. If the Card has expired, a Transaction can be conducted upon Authorisation by the Issuer;

   Transaction using the Card can be carried out until the last day of the month indicated on the Card (expiry is shown in the month/year format);
3. compare the first six BIN digits of the Card number with the six digits printed in small type below the Card number on the Card face. They should coincide;
4. compare the last four digits of the Card number on the Cardholder's signature panel (Card's reverse) with the last four digits of the Card number on the Card face. They should coincide;
5. if a Card has the Cardholder's photo, compare it with the Cardholder's face;

6. make sure that there is the Cardholder's signature on the Cardholder's signature panel
7. if a Card has the Cardholder's signature photographic image, compare the Cardholder's details on the Card face with those typed below the Cardholder's signature photographic image.
8. if there are doubts as to the Cardholder's personality, ask him/her to produce the ID document. Compare the last and first names with the Cardholder's details on the Card face, the signatures on the document and on the Card, and the photo;
9. if there is no signature of the lawful Cardholder on the Cardholder's signature panel, the company's representative should ask the Cardholder to show his/her ID document for identification and require that the Cardholder should sign the Card in the presence of the employee. The employee should not complete the Transaction until the Cardholder has signed on the Cardholder's signature panel.

The employee may refuse to service the Card of a Cardholder and/or to allow a Transaction in the following instances:

- if a visual inspection finds the Card to have forgery or mechanical damage marks or to lack at least one of the following elements: microprocessor, System hologram, trademark or Logo, Cardholder's signature panel;
- the first six BIN digits of the Card number do not coincide with the six digits printed in small type below the Card number on the Card face.
- the last four digits of the Card number on the Card face do not coincide with the last four digits on the Cardholder's signature panel;
- the Cardholder's details on the Card face do not coincide with those typed below the Cardholder's signature photographic image;
- if the Cardholder's first and last names indicated on the Card used for a Transaction do not coincide with those indicated in the Cardholder's ID document or if the Cardholder refuses to produce the ID document;
- if there are suspicions that the Card has been used for fraudulent purposes.

Additional commission fee

Acquirers may charge an additional commission fee directly from Cardholders for the following types of Transactions:

- ATM cash advance in foreign currencies
- Cash withdrawals in roubles and foreign currencies at CAO
- Transfer from the Card to cards of other payment systems in all devices of the Acquirer's Network of Devices;
- Payment for goods (works, services) only for the following MCCs – 4900, 9211, 9222, 9223 and 9399.

When charging a commission fee, the Acquirer must inform the Cardholder, before he/she carries out a Card Transaction, about the commission fee amount charged from the Cardholder for carrying out a Transaction. The Cardholder should be allowed to refuse to carry out a Card Transaction after being informed about the commission fee amount charged by the Acquirer. The commission fee amount must be specified in the primary document issued to the Cardholder.

The Acquirer may not charge an additional commission fee from Cardholders, which exceeds the amount of the additional commission fee charged on similar types of transactions conducted with cards of other payment systems.

Charging an additional commission fee from Cardholder on other Transaction types is prohibited.

Chargeback Transaction

The Chargeback Transaction is carried out at a merchant outlet when a Cardholder returns a product (refuses to accept works/services) that he/she has earlier bought at this merchant outlet using the Card (Card details). It is a merchant that makes a decision on refunding cash to the Cardholder.

The Chargeback Transaction may only be carried out with the Card that has been used to pay for the returned product (work, service) at a merchant outlet. In the Chargeback Transaction carried out at a merchant outlet the chargeback amount must not exceed the amount paid for the product (work, service).

The Chargeback Transaction must be processed by the Acquirer and submitted for clearing within seven (7) calendar days of the Chargeback Transaction date.

Cash must be refunded by the Issuer to the Cardholder within fifteen (15) calendar days of the Refund Transaction processing date.

2. Payment for goods (works, services)

The period for the Acquirer to submit the Transaction for clearing is seven (7) calendar days of the Transaction date.

2.1. In a public infrastructure (directly at the service delivery place in Point-of-Sale Terminals (merchants), ATMs and Payment Kiosks)

2.1.1. Using the Card contact microprocessor

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. EMV-compatible Point-of-Sale Terminal/PIN pad 2. EMV-compatible ATM/ Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk
		Point-of-sale terminal at merchant outlets
	Authorisation by Card payments application (Off-line Transaction)	Point-of-sale terminal at merchant outlet*
		Payment kiosk*

* provided that the Card payment application settings specified by the Issuer permit such an Authorisation mechanism.

Cardholder authentication	Authorisation mechanism	Device type
Cardholder's handwritten signature on receipt or device screen	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at merchant outlet
	Authorisation by Card payments application (Off-line Transaction)	Point-of-sale terminal at merchant outlets*

2.1.2. Using the card magnetic stripe **

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. Point-of-sale terminal/PIN pad 2. ATM/Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk
		Point-of-sale terminal at merchant outlet

* provided that the Card payment application settings specified by the Issuer permit such an Authorisation mechanism.

** if for some reasons the Card and/or Card receiving device failed to perform a Transaction using the card microprocessor.

Cardholder authentication	Authorisation mechanism	Device type
Cardholder's handwritten signature on receipt or device screen	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at merchant outlet

2.1.3. With manual entry of card details

- full Card number typed on the Card

Service device's specifications
1. Point-of-sale terminal/PIN pad

Cardholder authentication	Authorisation mechanism	Device type
Cardholder's handwritten signature on receipt or device screen	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at merchant outlet

2.2. e- and m-commerce

2.2.1. With manual entry of card details

- full card number typed on the card, Card Verification Value 2 (CVV2) is shown on the card reverse;
- virtual card, the card has full card number and card Verification Value 2 (CVV2).

Service device's specifications
1. personal communication tool (smartphone, telephone, tablet, minicomputer etc.)

Cardholder authentication	Authorisation mechanism	Device type
CVV2 and using reliable authentication technology	Authorisation by Issuer (On-Line Transaction)	personal communication tool
CVV2	Authorisation by Issuer (On-Line Transaction)	personal communication tool

2.3. Particular Transaction types with manual entry of Card details

Description of the procedure for conducting the Transactions listed below, including periods for submitting Transactions for clearing (the procedure is available in the System Standards):

- ordering goods (services) via telephone, post or internet;
- regular payments;
- hotel reservations and car rentals (with/without prepayment);
- hotel and car rental payments;
- additional hotel and car rental billing.

3. Cash advance on card

The period for the Acquirer to submit the Transaction for clearing is seven (7) calendar days of the Transaction date.

3.1. In a public infrastructure (directly at the service delivery place in Point-of-SaleTerminals (CAO) and ATMs)

3.1.1. Using the card contact microprocessor

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. EMV-compatible Point-of-Sale Terminal/PIN pad 2. EMV-compatible ATM

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO
		ATM
Cardholder's handwritten signature on receipt or device screen	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO

*3.1.2. Using the card magnetic stripe***

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. Point-of-sale terminal/PIN pad 2. ATM

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO
		ATM
Cardholder's handwritten signature on receipt or device screen	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO

3.1.3. With manual entry of Card details

Service device's specifications
1. ATM

Cardholder authentication	Authorisation mechanism	Device type
codes and passwords provided by Issuer	Authorisation by Issuer (On-Line Transaction)	ATM

4. Account crediting with cash

The period for the Acquirer to submit the Account Credit Transaction for clearing is 24 hours from the Authorisation time.

The Issuer must make tools available to the Cardholder immediately after Authorisation.

Authorisation of the Account Credit Transaction and the Account Credit Transaction may not be cancelled.

The Issuer may initiate a request to the Operator regarding the Acquirer's failure to meet the deadline for submitting a Transaction for clearing, but not earlier than 3 working days after the Authorisation day.

4.1. In a public infrastructure (directly at the service delivery place in ATMs and Payment Kiosks)

4.1.1. Using the card contact microprocessor:

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. EMV-compatible ATM/ Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

4.1.2. Using the card magnetic stripe[**]

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. ATM/Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

[**] if for some reasons the Card and/or Card receiving device failed to perform a Transaction using the card microprocessor.

5. Card-to-Card Transfer

The period for the Acquirer to submit the Card-to-Card Transfer Transaction for clearing, in a format meeting all the requirements of the System Standards, is 24 hours from the Authorisation time.

The Issuer of the Cardholder-Transfer Recipient (Recipient's Issuer) must make tools available to the Cardholder immediately after Authorisation.

A Transaction Authorisation cancelling message may be sent by the Acquirer not later than 24 hours from the Authorisation time, but till the time when the Acquirer submits the Card-to-Card Transfer Transaction for clearing. The Issuer may decline an Authorisation Request for cancelling a Transaction.

It is not allowed to cancel the Card-to-Card Transfer Transaction submitted for clearing.

The Recipient's Issuer may initiate a request to the Operator regarding the Acquirer's failure to meet the deadline for submitting a Transaction for clearing, but not earlier than 3 working days after the Authorisation day.

5.1. In a public infrastructure (directly at the service delivery place in ATMs and Payment Kiosks)

5.1.1. Using the card contact microprocessor

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. EMV-compatible ATM/ Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

5.1.2. Using the card magnetic stripe[**]

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. ATM/Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

[**] if for some reasons the Card and/or Card receiving device failed to perform a Transaction using the microprocessor.

5.2. e- and m-commerce

5.2.1. With manual entry of card details

- full card number typed on the card, Card Verification Value 2 (CVV2) is shown on the card reverse;
- virtual Card, the Card has full Card number and CVV2.

Service device's specifications
1. via personal communication tool (smartphone, telephone, tablet, minicomputer etc.)

Cardholder authentication	Authorisation mechanism	Device type
CVV2 and using reliable authentication technology	Authorisation by Issuer (On-Line Transaction)	personal communication tool
CVV2	Authorisation by Issuer (On-Line Transaction)	personal communication tool

6. Balance enquiry

6.1. In a public infrastructure (directly at the service delivery place in Point-of-SaleTerminals (CAO), ATMs and Payment Kiosks)

6.1.1. Using the card contact microprocessor

- Microprocessor contact Card with magnetic stripe

Service device's specifications
1. EMV-compatible Point-of-Sale Terminal/PIN pad 2. EMV-compatible ATM/ Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO
		ATM
		Payment kiosk

6.1.2. Using the card magnetic stripe[**]

- Microprocessor contact card with magnetic stripe

Service device's specifications
1. Point-of-sale terminal/PIN pad 2. ATM/Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	Point-of-sale terminal at CAO
		ATM
		Payment kiosk

7. PIN code change

7.1. In a public infrastructure (directly at the service delivery place in ATMs and Payment Kiosks)

7.1.1. Using a contact interface

- Microprocessor contact Card with magnetic stripe

[**] if for some reasons the Card and/or Card receiving device failed to perform a Transaction using the Card microprocessor

Service device's specifications
1. EMV-compatible ATM/ Payment Kiosk

Cardholder authentication	Authorisation mechanism	Device type
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

7.1.2. Using the card magnetic stripe[**]

- Microprocessor contact card with magnetic stripe

Service device's specifications		
1. ATM/Payment Kiosk		
Cardholder authentication	**Authorisation mechanism**	**Device type**
PIN code entry	Authorisation by Issuer (On-Line Transaction)	ATM
		Payment kiosk

[**] if for some reasons the card and/or card receiving device failed to perform a Transaction using the Card microprocessor