REGULATIONS FOR IN-STORE CASH WITHDRAWALS BY CARD

IN-STORE CASH WITHDRAWALS

(May 2015)

These regulations, the "Cash Withdrawal Regulations", apply to in-store cash withdrawals by Card through the use of a Terminal (MCC 6010).

The Cash Withdrawal Regulations comprise a supplement to the general terms and conditions that apply to the agreement on the Redemption of Card Transactions (the "Master Document") that has been entered between the Merchant and Embracy. *In the event of discrepancies between the Master Document and the Cash Withdrawal Regulations, the Cash Withdrawal Regulations shall take precedence.*

1. Checks

In conjunction with cash withdrawals, the Merchant shall conduct the checks specified below.

1.1 The Card

In cases where (i) the information on the Card is read without the involvement of the Merchant and (ii) the Cardholder signs the Transaction with a PIN code, the checks specified in section 1.1 below need not be conducted. The same applies if the information on the Card is read without the involvement of the Merchant and the type of Card does not require any further action/acknowledgement of the Transaction than the actual reading of the information.

The Merchant shall visually inspect the card to check that:

- The Card has been signed by the Cardholder;
- The Card bears no sign of alteration;
- The Valid thru date specified on the Card has not expired;
- When identification is presented, the name embossed on the Card is the same as the name on the identification;
- The Card is adorned with a brand, compare with section 1 ("Cards") of the Master Document, that is covered by the Agreement; and
- Under the Card Number are four printed digits and these digits are identical to the first four digits of the Card Number.

Should any of the above conditions not be met, the Card may not be accepted.

1.2 Identification check

An identification check shall always be performed for in-store cash withdrawals and the identification number shall be noted on the Merchant's receipt.

1.3 Signature

The Merchant shall compare the Cardholder's signature on the Merchant's receipt with those on the Card and the identification. If the different signatures do not match the Card may not be accepted.

The Merchant need not check the signature if the Cardholder signs the Transaction by PIN code (see section 3 below).

1.4 Authorisation and blacklist checks

Authorisation checks shall always be made in conjunction with payment, regardless of the purchase sum. If authorisation and blacklist checks are not conducted electronically from the Terminal, the Merchant shall contact Embracy over the phone for approval before processing the transaction. Embracy provides approval in the form of a control number that must be noted on the Merchant's receipt. Cards on which names and/or numbers are not embossed (such as Cards branded Maestro and Electron), however, require that authorisation is always provided electronically. If when authorising the transaction the Merchant receives the response that the Card is blacklisted, or if it is apparent that the Card is being used by an unauthorised person, if possible the Merchant shall retain the card. The Merchant shall then cut the Card in two and send it to Embracy.

1.5 Cash withdrawal limit

Card issuers have different rules concerning the limits that apply to their card products as regards the size and number of cash withdrawals that can be made within a certain period. If these limits are reached, this may be why authorisation is rejected and the transaction cannot be processed.

1.6 Chip and PIN Terminals

Terminals that are used to process Card transactions shall support magnetic stripe reader and EMV chip technology. MasterCard/VISA may charge Embracy a fee if the Merchant breaches the above. In such cases, according to sections 6.3 and 6.4 of the Master Document the Merchant is obligated to compensate Embracy for such fees.

2. Receipts

2.1 Content of the Merchant's receipt

The Merchant's copy of the signature receipt shall include the following information:

- The Merchant's name, location and corporate ID number;
- The Merchant's customer number at Embracy;
- The date and time of the Transaction;
- The Card Number (in truncated format if supported by the Terminal);
- The transaction type (withdrawal) in plain text;
- Control number (proof of authorisation);
- The amount of the Transaction;
- The text: "Authorised to debit my account as specified above" (this does not apply when a PIN code is used);
- Space for the Cardholder's signature (this does not apply when a PIN code is used);
- Number and type of identification (this does not apply when a PIN code is used);
- Reference/tracing number (unique identifier for the Transaction); and
- The four digits referenced in section 1.1 above, under item 6 (which shall be handwritten).

2.2 The Cardholder's copy

The Cardholder shall receive a copy of the signature receipt that includes the same information as the Merchant's copy of the signature receipt. However, the following differences apply to the Cardholder's copy:

- The Card Number shall be in truncated format (that is, only the last four (4) digits shall be shown with the initial digits represented by '*');
- The text "card payment" need not be specified (this is only required if the copy of the signature receipt comprises an extended point of sale receipt);
- The text "PIN code" need not be specified (this is only required when a PIN code is used);
- The text "Authorised to debit my account as specified above" need not be specified.

2.3 Storage

The Merchant shall archive the Merchant's receipt for at least eighteen (18) months. If requested by Embracy, the Merchant shall be able to provide a signature receipt for an individual Transaction within five (5) days. This applies even if the Merchant's redemption agreement with Embracy has otherwise come to an end.

3. Use of PIN

The amount shall be known to the Cardholder when the PIN code is entered. The entering of the PIN code comprises the Cardholder's authorisation for the transaction to be charged to the Cardholder's account. In certain environments, following special agreement Embracy can approve another procedure.

The Cardholder shall be given three (3) attempts to provide the correct PIN code. The Cardholder shall be able to cancel a Transaction instead of making further PIN code attempts. In a manual processing environment, the Cardholder shall have the right to refrain from using his or her PIN code to instead sign a signature receipt (on the condition that PIN code transactions are not obligatory for the concerned Card).

In the scenarios presented below, a written signature must be provided and as such the Cardholder may not be asked to use his or her PIN code:

- Authorisation cannot be granted electronically;
- Use of a PIN code, in accordance with Embracy's Instructions, is not permitted for the concerned Card; or
- The Card Number has been registered manually, that is, the Card could not be read by machine.

4. Collecting transactions

4.1 Collecting in general

The collecting of payment transactions made using Cards on which the name and/or number is not embossed (such as Cards branded Maestro and Electron) may only take place via a Terminal.

4.2 *Terminal*

The Card shall be read by machine in the Terminal. If this is not possible due to a problem with the Card, Embracy can provide special permission to register the Card Number and

Valid thru date manually. In such situations the Merchant must be able to prove that the Card was present in conjunction with the transaction, such as with an imprint or photocopy of the Card. The photocopy or other proof shall be kept together with the corresponding signature receipt. However, manual registration is never permitted for a Card on which the name and/or number is not embossed (such as Cards branded Maestro and Electron).

5. Reporting

5.1 Submitting payment transactions

Electronically collected payment transactions shall be transferred to Embracy within two (2) days of the date of the transaction. Paper copies shall be received by Embracy, or the party designated by Embracy, within five (5) days of the date of the transaction. The "date of the transaction" is the date of authorisation.

5.2 PIN code log

The Merchant shall keep a special log detailing all Transactions for which a PIN code was used, that is, both processed and cancelled Transactions. This log shall show:

- How the Transaction was processed;
- The Merchant's name (trading name), location and corporate ID number;
- The date and time;
- The Card Number and Valid thru date;
- The transaction method (see section 2.1 above);
- The transaction type (withdrawal or return/credit) in plain text;
- Point of sale identifier;
- Control number as proof of authorisation;
- The amount to debit;
- Reference/tracing number;
- Processing code (see the Instructions);
- Identification method (see the Instructions);
- Status code (see the Instructions);
- Transaction authentication code (see the Instructions); and
- Response code.

6. Returns

Returns are not permitted for in-store cash withdrawals.

7. Security

7.1 Processing Cardholder Data

In order to on the one hand maintain a high level of security in global card payment systems and on the other strengthen trust in Cards as a means of payment, it is of the utmost importance that everyone who processes Cardholder Data does so in a secure manner. "Cardholder Data" refers to such information that is embossed or printed on the front and back of the Card, including information that is stored in the Card's magnetic stripe and chip. For these reasons, the card industry has agreed to a common standard for processing Cardholder Data. The standard is called the Payment Card Industry (PCI) Data Security

Standard (DSS) and has been established by the international payment card networks Visa and MasterCard.

The Merchant agrees to comply with the PCI DSS as currently published at www.pcisecuritystandards.org.

7.2 System approval
Terminals that deliver Transactions to Embracy shall be approved by Embracy, or by a third party designated by Embracy. Embracy can require special audits concerning the security of sensitive components.

7.3 Special regulations for Payment Service Providers
If the Merchant uses a third party (a so-called Payment Service Provider) as part of its payment solution for processing Transactions, the Merchant must ensure that said third party complies with all of the requirements of PCI DSS.

7.4 Changes to equipment etc.
The Merchant shall inform Embracy prior to every installation, relocation or decommissioning of equipment that is technically connected to Embracy or another collector of Transactions that acts on behalf of the Merchant within the framework of this agreement.

Changes to Terminals affecting the conditions that applied at the time of approval may not be implemented without Embracy's consent.

Before transactions are transferred to Embracy, the Merchant shall conduct a test specified by Embracy on said Merchant's connection to Embracy's receiving system.

7.5 Hacking and IT forensic investigation
If Embracy suspects that the Merchant's point of sale, computer or other system has been subject to hacking, manipulation or the like that, in Embracy's assessment, in some way affects the Parties' cooperation under this Agreement, Embracy has the right to conduct a so-called IT forensic investigation of the concerned equipment. The Investigation may be conducted by Embracy or an IT forensic company engaged by Embracy.

The time, and related issues/procedures connected to the implementation of the Investigation, shall, unless Embracy deems it inappropriate, as far as possible be agreed between the Parties. If, however, Embracy deems it more appropriate, Embracy may visit the Merchant and conduct the Investigation without previously informing the Merchant.

It falls to the Merchant to participate in the Investigation to a reasonable extent and facilitate its implementation so that the purpose of the Investigation, which is to determine whether hacking/manipulation has taken place, can be achieved.

In cases where the Investigation determines that the Merchant's point of sale, computer or other system has been subject to hacking, manipulation or the like, the Merchant is obligated to at Embracy's request compensate Embracy for the costs of the Investigation.

8. Liability Shift

Embracy employs so-called Liability Shift. This means that the Merchant in its relation to Embracy under the Agreement is liable for all losses attributable to Transactions made by magnetic stripe with fraudulently manufactured cards where the legitimate Card, that is, the Card issued by the authorised/licensed card issuer, with the same card number as the fraudulent card is equipped with a so-called EMV chip.