REGULATIONS FOR SALES PAID BY CARD

UNATTENDED TERMINALS

(October 2015)

These regulations, the "Regulations for Unattended Terminals", apply to sales paid by Card using unattended terminals such as parking meters, vending machines and toll booths.

The Regulations comprise a supplement to the General Terms and Conditions for the Redemption of Card Transactions that have been entered between the Merchant and Bambora. In the event of discrepancies between the Master Document and the Regulations, the Regulations shall take precedence.

1. Types of Terminal for unattended environments

Type 1 is an unattended terminal where authorisation is always obtained online regardless of the amount and where verification is provided by PIN code, such as vending machines.

Type 2 is an unattended terminal where authorisation is always obtained online regardless of the amount but where verification cannot be provided by PIN code. Transactions via parking meters (MCC 7523) in such environments may not exceed EUR 50*. Transactions via vending machines (see definition below) in such environments may not exceed EUR 20*. In general, the transaction amount may never exceed EUR 100*.

* Or the equivalent in the local currency.

Type 3 This solution is only permitted for Toll roads (MCC 4784). Refers to Unattended Terminals that are only offline and lack functionality for verification by PIN code. Transactions in such environments may not exceed EUR 40 and the card must be checked against blacklists.

Special regulations apply to unattended petrol pumps (MCC 5542).

2. 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 Bambora a fee if the Merchant breaches the above. In such cases, under the Master Document the Merchant is obligated to compensate Bambora for such fees.

As of 1 January 2016, all newly installed terminals – regardless of type – at merchants that have not previously accepted Card payments must support contactless payments. This even applies to merchants that replace all of their card readers. As of 1 January 2020, all terminals must support contactless payments.

3. Customer receipt

Customer receipts shall always be provided and include the following information:

- The Merchant's name, location and corporate ID number.
- The date.
- The Card Number in truncated format (that is, only the last four (4) digits shall be shown with the initial digits represented by '*').

- The amount.
- Information on value added tax.
- Reference/tracing number (unique identifier for the Transaction).

4. Use of PIN

If the Terminal supports PIN codes, the Cardholder shall be given three (3) attempts to identify him- or herself by PIN code. If an incorrect PIN code is entered three (3) times in a row, if possible the equipment shall retain the card. Such cards are cut in two and sent to the appropriate card issuer. The Cardholder shall be able to cancel a Transaction instead of making further PIN code attempts.

If PIN codes are not permitted for the card type, the card cannot be used in self-service equipment with PIN code verification.

Transactions via vending machines refers to goods and services that can be sold using an unattended terminal with the exception of:

- Parking spaces, parking meters and garages (MCC 7523).
- Toll roads (MCC 4784).
- Petrol pumps (MCC 5542).
- All goods or services with statutory age limits on sales (such as gambling, tobacco and alcohol products).
- All goods or services that in accordance with other rules or regulations are subject to certain sales restrictions and require some type of customer or Cardholder verification (such as pharmaceuticals).

4. Collecting transactions

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 Terminal Type 1 and, in the case of parking meters (MCC 7523), via Terminal Type 2.

5. Reporting

5.1 Submitting payment transactions

Electronically collected payment transactions shall be transferred to Bambora within two (2) days of the date of payment. The "date of payment" is the date of authorisation.

5.2 Transaction Log

The Merchant shall keep a special log detailing all Transactions for which a Card 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 (in truncated format if supported by the Terminal);
- The transaction type (payment or return/credit) in plain text;

- Point of sale identifier;
- Control number as proof of authorisation;
- The amount to debit;
- Reference/tracing number; and
- Response code.

5.3 Storage
The Merchant shall for at least eighteen (18) months archive the Transaction Log in accordance with the applicable rules for PCI DSS (see section 6.1 below). If requested by Bambora, the Merchant shall be able to provide a receipt for an individual Transaction within five (5) days. This applies even if the Merchant's redemption agreement with Bambora has otherwise come to an end.

6. Security

6.1 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.

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

6.3 Special regulations for so-called Nodes and Payment Service Providers
If the Merchant uses a third party (a so-called node or 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.

6.4 Changes to equipment etc.
The Merchant shall inform Bambora prior to every installation, relocation or decommissioning of equipment that is technically connected to Bambora 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 Bambora's consent.

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

6.5 Special regulations for PoS systems with integrated card readers/Security Instructions
Merchants that use PoS systems with integrated card readers shall also ensure compliance with the Security Instructions issued by Bambora from time to time.

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

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

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 Bambora's request compensate Bambora for the costs of the Investigation.

7. Liability Shift

Bambora employs so-called Liability Shift. This means that the Merchant in its relation to Bambora 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.