INSTRUCTIONS FOR SALES PAID BY CARD
Card Not Present
(August 2019)

These Instructions, the "Card Not Present Instructions", apply to sales paid by Card where the Card is not present in connection with payment. The Sales Methods covered by the Card Not Present Instructions include, for example, sales over internet, sales by mail and telephone order, mobile payments, recurring payments and other MIT's.

The Card Not Present Instructions comprise a supplement to the General Terms and Conditions that apply to the agreement on the Acquiring of Card Transactions (the "Master Document") that has been entered between the Merchant and Bambora. In the event of discrepancies between the Master Document and these Card Not Present Instructions, the Card Not Present Instructions shall take precedence.

1. Definitions

Words that begin with an upper case letter are words that, if not defined in these Instructions, have been assigned special definitions in the Master Document and such words shall have the same meaning in these Instructions as in the Master Document.

"**3D Secure**" means a messaging protocol developed by EMVCo to enable Cardholders to authenticate themselves with their card issuer when making Card Not Present purchases over the internet. The Card Schemes may use different names for their 3D Secure solutions from time to time, for example Verified by Visa, MasterCard SecureCode, Protect By and SafeKey.

"**MIT**" means merchant initiated transactions, where the Cardholder has given a mandate authorizing the Merchant to initiate a Transaction or a series of Transactions with the Cardholder's Card Information, and where such mandate is based on an agreement between the Cardholder and that Merchant.

"**MOTO**" means mail and telephone order and refers to Card payments where the Cardholder provides their Card Information to the Merchant over the phone or on a mail order form. The Merchant then enters the Card Information into a virtual payment solution.

"**Recurring Payments**" means a series of recurring Transactions to the same amount, from the same Cardholder to the same Merchant, where such mandate is based on an agreement between the Cardholder and that Merchant.

"**SCA**" means strong customer authentication; an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

2. Special conditions for Card Not Present environments

The Merchant agrees to:

- On the order form or internet website clearly inform the Cardholder, prior to the payment, about in which country the Transaction will be processed and in which country the Merchant pays value added tax;
- On the website not include information or links to websites with illegal and/or in Bambora's assessment unethical activities or to activities that on objective grounds can be considered to damage Bambora's reputation;
- Immediately inform Bambora if the website on which the Merchant's sales are made changes web address (URL) and/or if new web addresses are introduced that the Merchant uses for sales paid by Card.

3. Checks

Before debiting the Cardholder, the Merchant shall conduct the checks specified below.

3.1 Authorisation

Authorisation shall always be made in conjunction with payment, regardless of the purchase amount, except where the purchase amount is below the floor limit as determined from time to time by a Card Scheme. The authorisation shall be coded with the correct Sales Method.

When validating the status of the Cardholder's Card (card status control) a so-called "account verification" shall always be used. Such verification shall never include authorisation of any amounts.

3.2 Identification of the Cardholder

3.2.1 Internet

Identification of the Cardholder for Transactions over the internet shall be made in accordance with Chapter 4 below.

3.2.2 MOTO

In the case of MOTO, the Merchant cannot confirm the Cardholder's identity. For this reason, the Merchant is always liable for the risk associated with all Transactions made by MOTO. This means that Bambora has the right to reclaim any amounts for which Cardholders claim refunds (Chargebacks) from the Merchant. This applies regardless of whether the Cardholder's claim is legitimate.

3.2.3 Mail order

The Merchant shall request that mail order forms be sent in a sealed envelope and the form shall include:

- The Merchant's name, location and corporate ID number;
- The Cardholder's name;

- The Cardholder's address (delivery address);
- The Cardholder's telephone number;
- The name of the card issuer;
- The number of the Card;
- The Card's valid thru date;
- The order date;
- The total amount of the order;
- Information on value added tax;
- A description of the goods ordered; and
- The Cardholder's signature.

3.2.4 Storage

The Merchant shall for at least eighteen (18) months archive the order form/order documentation in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). If requested by Bambora, the Merchant shall provide the order forms/order documentation for individual Transactions within five (5) bank days.

3.3 Delivery confirmation

For the delivery of physically deliverable goods or tickets, the recommended delivery methods include, for example, parcel or letter with signed delivery confirmation that includes an identity check upon collection. For the delivery of high risk goods, however, such delivery confirmation is a requirement, see Section 6.1. If the Cardholder files a complaint and delivery confirmation was used, the subsequent investigation is better facilitated. However, such investigation may still result in that Bambora has the right to a Chargeback for a processed Transaction in accordance with the conditions of the Master Document.

4. Strong Customer Authentication

SCA shall be applied for identification of the Cardholder in conjunction with payment, unless any of the exemptions in Section 4.1 below are applicable. The methods accepted by Bambora for SCA in Card Not Present environments are limited to 3D Secure. Other methods for SCA may only be accepted by Bambora if and as separately agreed between Bambora and the Merchant.

4.1 Exemptions from SCA

SCA is not required in Card Not Present environments under the following circumstances:

- If the Card is issued by a card issuer outside of the EEA,
- For MOTO,
- For MIT's (although never for the first of such Transactions which shall always be subject to SCA).

Furthermore, exemptions from SCA in Card Not Present environments may be granted by the card issuer under the following circumstances:

- If the Cardholder has whitelisted the Merchant as a trusted beneficiary with the card issuer,
- In respect of secure corporate payments, which are only made available to Cardholders who are not consumers,
- For payments where the purchase amount is EUR thirty (30) or below, and where the payment from the same Cardholder is not the fifth payment in a row or has reached a total value of EUR 100 (one hundred euro),
- For Recurring Payments (although never for the first of such Transactions which shall always be subject to SCA).

Bambora cannot guarantee that any exemption will be finally accepted, as it is always the card issuer who will have the mandate to accept or decline the use of an exemption.

5. Collecting Transactions

5.1 Collecting in general

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. For environments such as hotels where so-called preliminary authorisation is used, Transactions shall be submitted to Bambora within thirty (30) days.

6. Reporting

6.1 Transaction information

The Merchant shall upon delivery of goods or services provide the Cardholder with a customer receipt via e-mail or together with the goods/services upon delivery. The customer receipt shall include the following information:

- The word "receipt" in the title;
- The Merchant's name. The name shall be the same as that specified in the Agreement with Bambora and that is thus specified on the Cardholder's account statement;
- Telephone number and e-mail address of the Merchant's customer service;
- In appropriate cases, the Merchant's website (web address);
- Truncated card number;
- The amount of the card payment together with the transaction currency;
- The date and time of the Transaction;
- Unique transaction number/order number identifying the Transaction;
- The control number received in the authorisation process;
- In applicable cases, information that it concerns a Transaction over the internet;
- The type of Transaction (purchase or refund/return);
- A description of the goods or services ordered;
- Return and refund rules;
- Other information in accordance with currently applicable legislation;
- For telephone orders, on the Cardholder's receipt the Merchant shall write "TO" or "Telephone Order"; and
- For mail orders, the Merchant shall write "MO" or "Mail Order".

In cases where a physical receipt for a processed and reported Transaction is not available, such as for certain types of internet commerce, the Merchant shall establish and save a Transaction log and at Bambora's request provide the following information:

- The Merchant's name;
- The Merchant's reporting number at Bambora;
- In appropriate cases, the Merchant's website (web address);
- A description of the goods or services;
- The recipient's name and delivery address and, in applicable cases, the recipient's method for authenticating him- or herself, such as 3D Secure code;
- Truncated card number;
- The amount of the Card payment together with the transaction currency and VAT;
- The date and time of the Transaction;
- Unique transaction number/order number identifying the Transaction;
- The control number received in the authorisation process;
- The type of Transaction (purchase or refund/return);
- Indicator for electronic commerce; and
- The IP address of the device from where the Transaction originates.

The Transaction log shall fulfil the requirements of PCI DSS.

The Merchant shall at Bambora's request provide information about Transactions from the system that processes 3D Secure. If this system is managed by a PSP, the Merchant shall ensure that the PSP can present this information on behalf of the Merchant. This also applies to requests for information about Transactions in the Transaction log.

7. Merchant’s website

The Merchant's website must include at least the following information:

- The Merchant's name. The name shall be the same as that provided to Bambora in the Agreement and that is thus specified on the Cardholder's account statement;
- The country in which the Merchant is registered;
- A description of the goods or services offered;
- Prices;
- Transaction currency;
- Taxes and other government levies;
- Rules for returns and refunds, as well as delivery terms and conditions;
- Shipping costs;
- Customer service contact, e-mail address and telephone number;
- The Merchant's street address;
- Any export restrictions;
- Logos for Cards that the Merchant accepts;
- In applicable cases, logos from Card Schemes; and
- Other information in accordance with current legislation applicable to the Merchant;

The Merchant agrees to provide correct information and to regularly update the information on the website regarding the above matters.

8. Special obligations regarding Recurring Payments and other MIT's for sales over the internet

- When the Merchant registers a new Cardholder for recurring payments and no debit is due at the time of registration, a so-called status check shall be conducted on the Cardholder's Card, that is, a so-called "account verification". Such verification shall never include authorisation of any amounts.
- When the Merchant registers a new Cardholder who is to pay by Card, the Merchant sends the first debit transaction with SCA.
- For subsequent recurring card payments (debits), the Merchant bears all risk, unless otherwise agreed.
- When a Cardholder registers for and enters an agreement on recurring card payments, the Cardholder shall receive confirmation by e-mail. This confirmation shall include the text "recurring card payment" and information about the amount, how often it is debited and the duration of the agreement. It shall also specify whether the amount is fixed or variable.
- When a Cardholder pays for goods and/or services from a Merchant, the Merchant may not register the Cardholder for Recurring Payments without this being clearly stated and accepted by the Cardholder.
- The Cardholder shall receive an e-mail prior to each debit.
- Cardholders shall receive an e-mail before the expiration of any "free periods" or other types of introductory offers.
- Cardholders shall regularly be informed by e-mail about any changes to the debits, such as changes in the amount or date of the debits.
- The Cardholder shall be able to cancel a recurring card payment with immediate effect.
- The Merchant may not save the Card number and/or other Card Information in its systems unless security validation and, in applicable cases, certification in accordance with the Industry requirements (PCI DSS) have been implemented and approved.
- The Merchant shall be able to present documentation from software that processes 3D Secure and customer receipts as regards the Cardholder's choice of debit frequency and the period for which Recurring Payments have been permitted by the Cardholder.
- Transactions shall include information about Recurring Payments. The Merchant is responsible for establishing requirements for PSPs so that the Transaction content is in line with the Master Document, Regulations and Instructions.
- Transactions shall always be checked via authorisation prior to every debit. If authorisation is rejected, the debit may not be processed.
- The amount that in accordance with the agreement with the Cardholder is to be debited may not be altered without the Cardholder's consent.

9. Security

9.1 System approval
Systems 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. This audit or scan is conducted by a party chosen in consultation with Bambora.

9.2 Special regulations for PSP's
If the Merchant uses a third party service provider, PSP, for part or the whole of its Card Not Present sales, the Merchant must ensure that said third party complies with all of the requirements of PCI DSS.

10. General technical requirements

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

Before any Transaction may be sent to Bambora, the Merchant shall conduct a test specified by Bambora on said Merchant's connection to Bambora's receiving system. 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.

11. Liability

The Merchant always bears all risks associated with Chargebacks for captured Transactions under the Master Document if the Cardholder disputes that goods or services have been received, regardless of how the Cardholder was identified in accordance with Chapter 4 of these Instructions.

11.1 Risk reduction
The Merchant receives a so-called risk reduction for using 3D Secure on Card Not Present Transactions, which means that the card issuer cannot normally make any claims for fraudulent Transactions.

Bambora is not responsible for informing the Merchant about card types and countries of issue or for warnings and/or checks on whether Cards are covered by the risk reduction.

Bambora has the right to withdraw the right to risk reduction if fraud levels, in the Card Scheme's assessment, exceed the then current applicable permitted levels.

The Merchant is aware that 3D Secure is not a guarantee for protection from fraudulent Transactions.

Regarding the sale of high risk goods such as home electronics, watches, jewellery and gift vouchers, the Merchant is aware of its risk exposure to fraudulent Transactions as these are goods that are often subject to card fraud. Delivery confirmation for such orders is a requirement.

The Merchant shall at its own expense implement or acquire systems that prevent fraudulent orders.

The Merchant bears all risk for Transactions if the risk reduction available for 3D Secure is not used.

11.2 Use of exemption from SCA

Where an exemption from SCA has been applied for a certain Transaction in accordance with Section 4.1, the Merchant bears all risks.

****