REGULATIONS FOR SALES PAID BY CARD
REMOTE TRADING (Card Not Present)
(October 2015)

These regulations, the "Remote Trading Regulations", apply to sales paid by Card in Remote Trading. "Remote Trading" refers to Sales Methods where the Card is not present in conjunction with payment. The "Sales Methods" covered by the Remote Trading Regulations include, for example, sales over the Internet, sales by mail and/or telephone order, mobile payments, repeat payments using stored card numbers (referred to as Account on File) and subscriptions (referred to as Recurring Payments).

The Remote Trading 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 Remote Trading Regulations, the Remote Trading Regulations shall take precedence. Words that begin with an upper case letter, that is, a capital, are words that have been assigned special significance/definitions in the Master Document and in these Remote Trading Regulations such words shall have the same meaning as in the Master Document.

1. Card Payments in Remote Trading in general

For Card Payments over the Internet all cards in the Agreement and, in applicable cases, MasterPass and V.me are accepted with the exception of Maestro cards, which can only be accepted if 3D Secure is installed and activated. Maestro, however, is never accepted for mail or telephone order sales.

2. Special obligations in Remote Trading

The Merchant agrees to:

- On the order form or Internet website clearly inform the Cardholder, before the payment instructions, in which country the Transaction will be processed and in which country the Merchant pays value added tax;
- On the website not have information or links to websites with illegal and/or in Embracy's assessment unethical activities or to activities that on objective grounds can be considered to damage Embracy's reputation;
- Immediately inform Embracy if the website on which the Merchant's sales are made changes www address and/or if new www 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 checks shall always be made in conjunction with payment, regardless of the purchase sum. The authorisation shall be coded with the correct Sales Method.

When checking the status of the Cardholder's Card (card status check) a so-called "zero value authorisation" shall always be used.

3.2 Identification of the Cardholder

3.2.1 Internet
Card transactions shall be processed in accordance with 3D Secure unless otherwise agreed between the parties.

3.2.2 Telephone Order and Mail Order
In the case of Telephone and Mail Order, the Merchant cannot confirm the Cardholder's identity. For this reason, the Merchant is always liable for the risk associated with all payment transactions made by Telephone Order and Mail Order. This means that Embracy has the right to reclaim from the Merchant any amounts for which Cardholders claim refunds (chargebacks). 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 Card Number;
- 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 Embracy, 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 5.2. If the Cardholder files a complaint and delivery confirmation was used, the subsequent investigation is better facilitated. The investigation may, however, still conclude that Embracy has the right to a Chargeback for a redeemed Card Transaction in accordance with the stipulations of the General Terms and Conditions.

The Merchant always bears all risks associated with Chargebacks for redeemed Card Transactions in accordance with the stipulations of the General Terms and Conditions if the Cardholder disputes that goods or services have been received regardless of how the Cardholder was identified in accordance with section 3.3.

4. Reporting

4.1 Submitting payment transactions etc.
Electronically collected payment transactions shall be transferred to Embracy 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 payment transactions shall be submitted to Embracy within thirty (30) days.

4.2 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 Embracy 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 an Internet transaction;
- The transaction type (purchase or 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 Card Transaction is not available, such as for certain types of Internet commerce, the Merchant shall establish and save a Transaction Log and at Embracy's request provide the following information on:

The Card Transaction:
- The Merchant's name;
- The Merchant's reporting number at Embracy;
- 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 transaction type (purchase or return);
- Indicator for electronic commerce; and
- The orderer's IP address.

The Transaction Log shall fulfil the requirements of PCI DSS.

The Merchant shall at Embracy's request provide information about Card Transactions from the system that processes 3D Secure. If this system is managed by a Payment Service Provider (PSP), the Merchant shall ensure that the PSP can present this information on behalf of the Merchant. This even applies to requests for information about Card Transactions in the Transaction Log.

5. Other

5.1 Merchant
The Merchant's marketplace on the Internet must include at least the following information:

- The Merchant's name. The name shall be the same as that provided to Embracy 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 for Verified by Visa and MasterCard SecureCode, as well as V.me and MasterPass; 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.

5.2 Risk reduction

Activated support for 3D Secure, MasterPass and V.me on the Merchant's website on the Internet means that the Merchant receives a so-called risk reduction, which means that the Card Issuer cannot normally make any claims for fraudulent Card Transactions.

Embracy 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.

Embracy has the right to retract the right to risk reduction if fraud levels, in the Payment Card Networks' assessment, exceed the currently applicable permitted levels.

The Merchant is aware that 3D Secure, MasterPass and V.me are not a guarantee for protection from fraudulent Card 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 Card 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 Card Transactions if the risk reduction available for 3D Secure, MasterPass and V.me is not used.

5.3 Special stipulations regarding Recurring Payments 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 "zero value authorisation".
- When the Merchant registers a new Cardholder who is to pay by Card, the Merchant sends the first debit transaction in accordance with 3D Secure. The currently applicable 3D Secure risk reduction applies to this transaction.
- For subsequent recurring card payments (debits), the 3D Secure risk reduction does not apply and 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 other Cardholder Data in its systems unless security validation and, in applicable cases, certification in accordance with the Payment Card Networks' 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.
- Card Transactions shall include information about Recurring Payments. The Merchant is responsible for establishing requirements for PSPs so that the card transaction content is in line with the General Terms and Conditions, Regulations and Instructions.
- Card 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.

5.4 Special stipulations regarding Account on File for sales over the Internet

- When the Merchant registers a new Cardholder who is to pay by Card, the Merchant sends the first transaction in accordance with 3D Secure. The currently applicable 3D Secure risk reduction applies to this transaction.
- When the Merchant registers a new Cardholder for recurring payments and debiting is not applicable at the time of registration, a so-called status check shall be conducted on the Cardholder's Card, that is, a so-called "zero value authorisation".
- For subsequent card payments (debits), the 3D Secure risk reduction does not apply and the Merchant bears all risk, unless otherwise agreed.

6. Security

6.1 Processing of certain 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 Payment Card Networks have 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
Systems 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. This audit or scan is conducted by a party chosen in consultation with Embracy.

6.3 Special regulations for Payment Service Providers
If the Merchant uses a third party (a so-called Payment Service Provider) for part or the whole of its Remote Trading, the Merchant must ensure that said third party complies with all of the requirements of PCI DSS.

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

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

6.5 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 ("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.