1. COMMON CONDITIONS

The Common Conditions International Cards shall apply to these Service Conditions International Cards. For the purposes of applying the Common Conditions, the following terms shall be defined as indicated below:

- **Sales Voucher:** the document or log file produced by the payment terminal or Processing Software by way of proof of the transaction.
- **Payment Device:** the Processing Software.

2. ADDITIONAL DEFINITIONS

- **3DSecure:** the additional security layer than can be enabled for Internet transactions. The technical name "3DSecure" is also known under various commercial names, such as *"Verified By Visa", "MasterCard SecureCode", "American Express SafeKey" and "J/Secure"*.
- **Certificate:** the digital code reflecting a relation between electronic data and an identity (of the Merchant). It contains a collection of electronic data comprising a public key, information regarding the public key holder's identity, as well as validity information, which were electronically signed by a Certification Authority.
- **Certification Authority (CA):** entity that issues and manages Certificates.
- **Credit Voucher:** the document produced at the moment of (partial) cancellation of a transaction.
- **CVV2-CVC2 code:** three-digit code indicated on the back of the Card, and submitted to the Processing Software.
- **Limited Payment Guarantee:** means that if a transaction was successfully executed with 3DSecure and the Merchant fully complies with this Contract, the Merchant is assured that the transaction amount will not be debited from his Internal Account due to a transaction dispute initiated by the Card-holder for the sole reason that the transaction was not authorized by the Cardholder. The Limited Payment Guarantee does not prevent, however, that the Internal Account is debited for other reasons mentioned in the Common Conditions. The Merchant therefore acknowledges the limited scope and relative nature of the guarantee that is granted, for which the conditions and limitations are further described in clause 7. 2.
- **Processing Software:** the certified software that, in addition to authorizing the transaction, also transmits the transaction to the Acquirer. For online sales, this will for example consist of the web pages on which the Cardholder can submit the Card data; for sales by telephone or fax, this will for example consist of the software that is locally installed at the Merchant's premises, through which employees can enter Card data.
- **Processing Software Service Provider:** the company which offers the Processing Software, takes care of the technical connection with the Acquirer, and is certified by the Card Scheme and competent verification bodies. If the Merchant uses KB SmartPay's Processing Software, then KB SmartPay will qualify as the Processing Software Service Provider.

3. SCOPE

These Service Conditions cover all Card-based transactions which can be accepted by the Merchant for Card Not Present situations.

4. EXECUTION OF TRANSACTIONS

In practice, the obligations imposed on the Merchant in this clause 5 shall typically be met by the Processing Software Service Provider (possibly in cooperation with the Merchant).

4.1. The Merchant shall ensure that the Processing Software is functioning correctly.

4.2. Internet payments require that (the Processing Software of) the Merchant has a Certificate issued by a Certification Authority. At the Acquirer's or KB SmartPay's first request, the Merchant shall submit proof of this Certificate and its current validity. The Merchant shall be responsible for correctly performing the certification procedure, and renewing the certificate on time. The Merchant shall also be responsible for the correct implementation, management and security of the Certificate.

4.3. The Acquirer can impose certain settings in the Processing Software. Any non-compliance in this regard shall give the Acquirer the right to immediately terminate the Contract in accordance with the Termination Modalities.

4.4. The Merchant shall protect the transaction data against any form of interception during its transmission and storage. Certain data, for example the data referred to in PCI/DSS, must never be stored in an unprotected manner: the name of the Cardholder, the full Card number, the expiry date, the Authorization Code, the service code, the date, and the amount of the transaction. Furthermore, storage of the full da-ta contained on the magnetic strip, the CVC2/CVV2/CID and the PIN/PIN block after Authorization processing, is not allowed, not even in encrypted form. The Merchant shall be fully liable for all damage in this regard, including any penalties and costs imposed by the Card Scheme on the Acquirer, as a consequence of the non-compliance with these obligations.

4.5. The Merchant shall secure his infrastructure (including his website and Processing Software) against hacking and other types of data compromise.

5. VERIFICATIONS

5.1. The Merchant acknowledges that the risk for fraudulent transactions is significantly higher for Card Not Present situations, as compared to situations where the Cardholder and the Card are in physical proximity of the Merchant. Because of this higher risk on fraud in Card Not Present situations, the Merchant shall act even more prudently and carefully than with other transactions. The Merchant also explicitly commits to train his employees and agents on these aspects, and draw their attention to the fraud risk.

5.2. The Merchant shall use all efforts available to him to reduce the fraudulent transaction risk, e.g. by verifying whether:

- there is a match between the name of the Cardholder, the name possibly mentioned in the email address, and the name mentioned in the delivery address;
- in Internet sales, there is a match between the presumed geographical location of the computer address (IP address) and the delivery address;
- the presumed customer undertook an unusual number of attempts for the transaction;
- any remarkable questions or unusual requests were asked by the customer.

In this risk assessment, the Merchant shall take account of all relevant factors – such as the nature of the products or services, their sensitivity to fraud, as well as the transaction amount.

Several of these verifications may be fully or partially implemented as a parameter in the Processing Software. In addition, several Processing Software Service Providers and other third parties also offer fraud detection tools in order to limit the risk associated with Card Not Present situations. The Acquirer strongly advises to use these possibilities.

6. ELECTRONIC PROCESSING

6.1. General provisions

The Merchant can initiate the electronic processing of a transaction either by using the Processing Software, or by manually entering data into a payment terminal.

The Acquirer shall only process transactions when the Merchant sent all required infor-mation (such as the full Card number, the Card expiry date, the name and first name of the Cardholder, the amount and date of the trans-action, the Authorization Code and the CVV2-CVC2 code) in a secured manner, in accordance with either applicable industry standards, or a security protocol made available by The Acquirer.

The Merchant accepts that communicating the name and first name (and/or address) of the Cardholder not necessarily implies the verification of this data by The Acquirer.

If the 3DSecure technology is not used, then the Limited Payment Guarantee set forth in clause 6.2 shall not apply. The Merchant shall then bear the full financial risk for all disputes initiated by (a Cardholder through his) Card issuer, e.g. because the contents of the magnetic strip or the contents of the Card was not received, or be-cause the transaction was accepted in physical absence of the Card.

If the Merchant engages other parties in his payment process (e.g., the Processing Software Service Provider), then these other parties cannot bind the Acquirer or KB SmartPay in any way. For example, if a third party would claim to guarantee certain verifications or payments, then the Merchant accepts that this guarantee shall not bind the Acquirer or KB SmartPay in any way.

6.2. Processing Software & 3DSecure

To the extent all of the following criteria are met, the Merchant shall qualify for the Limited Payment Guarantee:

- **The Merchant's Processing Software is compatible** with the most recent security standards relating to 3DSecure that are imposed by the Card Scheme.
- **The Merchant remains within the limits of 3DSecure, as determined by the Card Scheme.** If the maximum amounts for disputes determined for 3DSecure are exceeded, then the 3DSecure coverage offered by the Card Scheme will be suspended, possibly retroactively and without such suspension being motivated. The applicable maximum amounts shall be communicated by The Acquirer at the Merchant's simple request.
- The Merchant has activated 3DSecure in his Processing software.
- The transaction type is eligible for 3DSecure. 3DSecure can only be used for situations where the Cardholder explicitly intervenes in the transaction process in order to securely transfer the data associated with him (e.g., the temporary code generated by the Card reader, a password, a code received by SMS, etc.) to the Card issuer. This requirement prevents 3DSecure from being used for transactions by phone, fax or letter; neither can 3DSecure be used for recurring transactions (e.g., a periodically repeated payment, where the Merchant deliberately avoids the Cardholder's intervention to increase user convenience).
- The Card used for the transaction is technically eligible for 3DSecure.
- According to the Card Scheme, the Card used for the transaction is eligible for 3DSecure. This depends on various factors defined by the Card Scheme, such as the Card type (consumer – corporate), the geographical origin of the Card, the Merchant's place of establishment, etc. In addition, the Merchant acknowledges that these factors change over time. At the Merchant's simple request, The Acquirer will provide a list of description of the eligible Cards.

It may also happen that in case of technical failures at the Card Scheme or Card issuer side (e.g., when the "Discovery server" of VISA In-ternational, which signals the Merchant's eligibility for 3DSecure, is unavailable) the transaction does take place, but without 3DSecure.

- There exist no **other reasons** why 3DSecure would be unavailable. In this regard, the Merchant shall carefully monitor the communications from The Acquirer and his Processing Software Service Provider, as well as the logs of his Processing Software.

The Limited Payment Guarantee shall not relieve the Merchant from his increased duty of care for Card Not Present situations (clause 6).

7. CREDIT VOUCHERS

7.1. If the Cardholder has legitimate complaints about the goods or services sold, or if the Card-holder returns the goods for a legitimate reason, then the Merchant cannot refuse to exchange them or to draw up a Credit Voucher, for the sole reason that the goods or services were paid with a Card.

7.2. The reimbursement shall never be realized in cash, by bank transfer, by money transfer, or by any other means outside the means allowed by the Card Scheme or by KB SmartPay. If the Merchant draws up a Credit Voucher in order to cancel a transaction performed with a Card, he will only be entitled to use the Credit Vouchers approved by KB SmartPay. The Card data, as well as date and amount, shall then be mentioned on the Credit Voucher. The Credit Voucher is to be sent to KB SmartPay within twelve calendar days of their issuing date. The Credit Voucher shall only be drawn up to the benefit of the Card that was used to realize the transaction.

Merchants equipped with a payment terminal are entitled to cancel a transac-

tion through the payment terminal within a period of twelve calendar days, by entering the Authorization Code, the date and time of the transaction.

8. STORING SALES VOUCHERS AND SUPPORTING DOCUMENTS

8.1. During a period of at least two years, the Merchant shall store the transaction proof and its subsequent follow-up, the proof of the successful delivery/service, as well as the original documents of the orders (fax, mail, etc.) and deliveries (e.g., the delivery addresses).

8.2. Upon KB SmartPay's first written request, the Merchant shall send a complete and legible copy of the relevant evidence to KB SmartPay within a period of fifteen calendar days. Such request implies that the Cardholder has submitted a possible dispute. In order to allow KB SmartPay to handle the case and take the Merchant's interests into account in doing so, the Merchant shall communicate all relevant doc-uments regarding the sales/service (e.g., emails exchanged with the Cardholder, proof of delivery, documents communicated to the Cardholder, etc).

8.3. In case of non-compliance with the above obligations, KB SmartPay has the right to debit the Merchant's Internal Account, in accordance with the Common Conditions.