THE E-COMMERCE AND AMERICAN EXPRESS® SafeKey℠ ADDENDUM

IT IS RECORDED THAT:

- The merchant has entered into a Services Establishment Agreement (hereinafter referred to as "Merchant Agreement") with Nedbank, governing the acquiring relationship between the parties in respect of American Express Cards being accepted at the merchant.
- The Merchant wishes to market and sell its goods and/or services, over the internet, by accepting American Express Cardmember Cards as the method of payment, under Card not present conditions;
- This e-Commerce and American Express SafeKey Addendum must be read in conjunction with the Merchant Agreement;
- The Parties have had discussions and the Merchant has elected to implement the 3-D Secure protocol-based American Express SafeKey Cardmember Authentication Programme at its premises.

Wherefore the Parties agree as follows:

1 TERMS OF USE

1.1 **3-D Secure** means an e-commerce protocol (version 1.0.2.). American Express reserves the right to add or change the application version(s) from time to time that enable the secure processing of payment card transactions over the internet;
1.2 **AACS** means Attempts ACS
1.3 **ACS** means Access Control Server
1.4 **Acquirer** means Nedbank, the sole Issuer and Acquirer for American Express Cards in South Africa under license.
1.5 **AEVV** means American Express Verification Value, which is a Cardmember authentication field or e-commerce indicator used to identify an internet transaction
1.6 **Authentication** means the process of verifying that a person making an e-commerce purchase is entitled to use the payment card;
1.7 **Authorisation** means approval of a transaction by or on behalf of an issuer according to defined operating regulations.
1.8 **Card/s** means American Express charge, debit and credit cards;
1.9 **Cardmember** means a person who has been issued with a Card and whose name appears on a Card;
1.10 **Chargeback** means a procedure where the Issuer charges a card transaction back to the Acquiring bank and subsequently its Merchant in accordance with card network rules;
1.11 **Directory Server** means the American Express Directory Server, which receives messages from merchants for a specific card number/transaction and determines whether the card number is registered for SafeKey, thereafter directing the request for Cardmember authentication to the appropriate ACS. The ACS in question then responds, with the Directory Server forwarding the response to the merchant;
1.12 **Dispute** means a Cardmember's disagreement on a transaction which the Cardmember believes should be returned;
1.13 **ECI** means Electronic Commerce Indicator
1.14 **Fraudulent Transaction** means any transaction that would constitute fraud in terms of common law (irrespective of whether Nedbank has issued an authorisation code in good faith to the merchant). This includes any card purchase and/or transaction made by someone other than the authorised Cardmember, and the use of a card or card account number that has not been issued by a bona fide card issuer to conclude this purchase;
1.15 **Issuer** means Nedbank Limited which operates American Express Cards under license in South Africa
1.16 **Liability Shift** means Fraud Liability Shift ("FLS"). It applies to Transactions which were Attempted or Fully Authenticated, where a merchant is enrolled in the American Express SafeKey programme, allowing the burden of proof for qualifying online/e-commerce transactions to shift from the acquiring bank and its merchant to the card Issuer. This applies to chargebacks on transactions where the merchant attempted to authenticate (or where Full Authentication occurred) the American Express Cardmember using SafeKey, where the issuer is based within a SafeKey FLS market. An updated list of participating markets can be found at https://network.americanexpress.com/en/globalnetwork/safekey/
1.16.1 Issuers in American Express FLS markets may be liable for fraud losses, regardless of participation in American Express SafeKey by the Issuer, or its Cardmembers. Thus, regarding foreign-issued American Express Card transactions at South African Merchants, the Merchant is protected in that if they are American Express SafeKey enabled and attempt to authenticate the Cardmember using SafeKey, even if the issuing bank is not a SafeKey participant, the issuer may be liable for a resultant fraud loss.
1.17 **Merchant** means an entity that contracts with Nedbank to facilitate transactions that accept Cards as payment;
1.18 **Service Establishment Commission** means a portion of the total value of the Card Transactions carried out by the Merchant and payable to Nedbank at a rate that can be amended by Nedbank from time to time;
1.19 **Message** means an electronic communication from the Merchant's server to the payment gateway or vice versa, in a format currently prescribed by Nedbank;

1.20 **Merchant Server Plug-in (MPI)** (in conformance with American Express SafeKey MPI Functional Requirements version 1.1) means a component that is incorporated into the Merchant's web storefront and performs functions related to SafeKey on behalf of the Merchant;
1.21 **Nominated Bank Account** means the bank account nominated by the Merchant from time to time in accordance with clause 7 and which is used by Nedbank to credit amounts and debit , costs, chargebacks and/or amounts for which the Merchant is liable, in terms of this agreement;
1.22 **Parties** means Nedbank and the Merchant;
1.23 **Payer Authentication Request (PAReq)** means a message sent from the MPI to the Issuer ACS via the Cardmember's browser requesting the authentication of the Cardmember;
1.24 **Payer Authentication Response (PARes)** means a message formatted, digitally signed, and sent from the Issuer ACS to the MPI (via the Cardmember browser) providing the results of the issuer's authentication of the Cardmember;
1.25 **Payment Gateway** means software used by Nedbank to forward and receive messages and to adapt messages received from the Merchant's server in order to process transactions;
1.26 '**PCI DSS**' means Payment Card Industry Data Security Standards as published by the PCI Security Council and endorsed by the card networks;
1.27 **PI** means Programme Indicator
1.28 **SafeKey** means the 3-D Secure protocol-based, industry standard American Express SafeKey Cardmember Authentication Programme that, when employed by Issuing Banks, Cardmembers, Acquiring Banks, and Internet Service Enterprises, provides greater security for Internet Transactions, by authenticating the Cardmember during purchase;
1.29 **SafeKey Branding Guidelines** refers to the brand guidelines for American Express SafeKey which ensure that participants deliver a consistent brand image and build brand equity;
1.30 **S/E** means Service Establishment, i.e. Merchant;
1.31 **Transactions** means the purchase of goods and/or services from the Merchant by the Cardmember via the Internet;
1.32 **UCAF** means the Universal Cardholder Authentication Field (UCAF);
1.33 **VEReq** means Verify Enrollment Request;
1.34 **VERes** means Verify Enrollment Response;
1.35 **XID** means SafeKey Transaction ID.

2 ACCEPTANCE OF CARDS

2.1 American Express SafeKey Fraud Liability Shift protection is only provided for American Express Cards for e-Commerce Internet Transactions and this protection applies to Cardmember Disputes on Card not present transactions, which were Attempted or Fully Authenticated, as described under clause 3.2 below.
2.2 The Merchant must implement SafeKey in such a way that Cardmember account details are never stored in an unprotected manner, and Merchants must adhere to PCI DSS requirements. The Merchant may not under any circumstances retain or record the CVV2/CVC2/4DBC number, the expiry date of the card or the card number, as this is in direct violation of the PCI DSS. All penalties and fines imposed by American Express as a result of such violation will be charged to the Merchant.

3 RIGHTS AND OBLIGATIONS OF THE MERCHANT

3.1 The Merchant must implement SafeKey, and process all internet Transactions using this 3-D Secure technology, to be covered by FLS.
3.2 When conducting SafeKey Transactions, a Merchant must :
3.2.1 initiate a single authentication request per Transaction
3.2.2 not re-use authentication data other than as stated below:
3.2.2.1 In a SafeKey Transaction, a Merchant may only re-use the original authentication data when a subsequent POS authorisation request (1100) message is necessary on the original purchase. Original authentication data is valid for up to forty-five (45) days from the authentication date. Authentication data must not be submitted in the authorisation request for separate purchases. In the event of a Cardmember Dispute, the Acquirer and Merchant must be able to demonstrate that all authorization requests relate to the single, original authenticated purchase.
3.3 The Merchant agrees that, to be covered by FLS, the Transaction must comply with the following requirements:
3.3.1 The Acquirer and Issuer must be located in American Express SafeKey FLS Markets;
3.3.2 The Transaction Authentication must be completed as defined by the American Express SafeKey FLS Authentication type, meaning either the Transaction was Attempted or Fully Authenticated as evidenced by the ECI on the POS First Presentment (1240) message. Bit 23 (ECI) and Bit 97 (PI) of 1240 define the Safekey Transaction.
3.3.2.1 If a response message (VERes) of "N" (No) is returned by the Directory Server, the Merchant can continue with the transaction however, it will be treated as a standard, non-SafeKey Transaction. In this case, FLS will not be applicable and the Merchant agrees and acknowledges that the Merchant will not be protected and will assume all liability in respect of the Transaction.
3.3.3 The Merchant must not be on the High Risk merchant list, and it is the Merchant's duty to check this with the Acquirer
3.3.4 The Merchant must be in compliance with the American Express merchant fraud monitoring policies. A message received from the Merchant server will be deemed to be a message from the Merchant;
3.4 If all of these requirements in clause 3.3 are met, and the Issuer is SafeKey certified, American Express will provide the Issuer with a PI on the POS first presentment (1240) message. The PI with the SafeKey value indicates that the Transaction qualifies for SafeKey FLS. The Merchant must supply Nedbank with the merchant acquirer

authentication request (PAReq) and/or Issuer authentication response (PARes) messages if requested to do so in the resolution of Disputes

.

4 RIGHTS AND OBLIGATIONS OF NEDBANK

4.1 Nedbank shall immediately delete from the Directory Server any terminated/closed Merchant number, suspect Merchants, or any Merchant that fails to comply with the requirements of the e-Commerce and American Express SafeKey Addendum governing Merchant participation in SafeKey;

4.2 Nedbank retains chargeback rights under the conditions described in clause 3 above.

5 INVALID TRANSACTIONS

A Transaction will be invalid if:

5.1 The Merchant inserts falsified SafeKey authentication information into the Transaction message by inserting invalid card numbers or the UCAF indicators are incorrect,

5.2 The SafeKey authentication response from the Issuer is tampered with in any way by the Merchant.

5.3 The Merchant will be liable for all Invalid Transactions as mentioned in this clause 5.

6 PROVISIONS RELATING SPECIFICALLY TO SOFTWARE AND INFRASTRUCTURE

6.1 The Merchant shall carry the risk relating to the operational effectiveness of the Merchant server (or any other server attached to the merchant server through which transactions are being acquired), in the event that PCI DSS requirements are not complied with.

6.2 The Merchant must in accordance with the Nedbank's requirements, install or integrate with Nedbank's SafeKey MPI technology, to suitably identify the Merchant to the bank and/or the Cardmember in accordance with the standards and specifications of the bank.

7 DEBITING THE MERCHANT'S ACCOUNT

7.1 Nedbank is entitled to debit the Merchant's Nominated Bank Account, at which ever bank this account is held with Service Establishment Commission, fees and charges.

7.2 Chargebacks arising from a Disputed virtual Transaction will be debited to the Merchant's Nominated Bank account.

7.3 Nedbank reserves the right to levy other fees at any time but will always notify the Merchant accordingly one month before they become applicable.

8 DISPLAY OF SYMBOLS

8.1 The Merchant must on its website display the SafeKey symbols in accordance with the brand guidelines for American Express SafeKey to ensure that merchants deliver a consistent brand image and build brand equity. As a minimum, the Merchant must display the brand guidelines on its payment page and, optionally, also on either their home page and/or security information page.

8.2 The Merchant must adhere to the content and placement guidelines as supplied by Nedbank from time to time.

9 GENERAL

9.1 The Merchant Agreement is deemed to be amended by the provisions of this Addendum and to incorporate such provisions.

9.2 Subject to the provisions as set out herein, the provisions of the Merchant Agreement shall remain in place.

9.3 This agreement constitutes the entire agreement between the Parties regarding the subject matter of e-Commerce and SafeKey and is incapable of being varied or consensually terminated otherwise than in writing signed non-electronically by the duly authorized representatives of both Parties.

Signed at ..... (*place*) on ..... / ..... / ..... (*day*) (*month*) (*year*)

Witnesses

..... (*Signature*)

1. .....

2. ..... For and on behalf of the merchant, duly authorised

Signed at ..... (*place*) on ..... / ..... / ..... (*day*) (*month*) (*year*)

Witnesses

..... (*Signature*)

1. .....

2. ..... For and on behalf of Nedbank Limited, duly authorised

Signed at ..... on ..... / ..... / .....
(place) *(day)* *(month)* *(year)*

Witnesses

1. .....

2. .....

.....
(Signature)

For and on behalf of Nedbank Limited, duly authorised