FNB ZAMBIA eCOMMERCE FACILITY TERMS AND CONDITIONS

The Bank will provide You with Acquiring Services to enable You to accept Payment Instruments from Your Customers to pay for goods and/or services. The e-Commerce Terms and Conditions form part of Your Merchant Agreement and must be read in conjunction with the remaining Terms and Conditions of Your Merchant Agreement including your application, General and Specific Terms and Conditions. It contains important information about the rights and obligations relating to You and the Bank in respect of the Acquiring Services and products delivered by the Bank. A copy of the General Terms and Conditions is available on the FNB website, can be obtained from the FNB Zambia Call Centre or can be supplied to You by post and email at Your request. It is Your duty to speak to the Bank if You do not understand any part of the Terms and Conditions prior to entering into this Merchant Agreement.

BY USING THE BANK'S ACQUIRING SERVICES AND PRODUCTS THE PARTIES AGREE AS FOLLOWS:

1. YOUR OBLIGATIONS

1.1 You must do the following when processing e-Commerce Transactions:

1.1.1 only operate within the Acquirer's jurisdiction country as specified by the Acquiring Bank;

1.1.2 ensure that Your website complies with the Card Association Rules and any other applicable rules and laws ;

1.1.3 Install or integrate on Your website: software; internet infrastructure and processes that enable electronic data to identify You and the Customer by verifying You and the integrity of the Message;

1.1.4 Ensure that prior to carrying out Transactions: Your website and the merchant server; software; Internet

Infrastructure and processes comply with the Bank's standards and specifications for secure authentication protocol;

1.1.5 Implement hardware or software prescribed by the Bank to limit or reduce Fraud;

1.1.6 Notify the Bank of any changes relating to: Your CSP (unless you are making use of the FNB CSP); website developer and the location where Your website is hosted;

1.1.7 Carry the risk relating to the operational effectiveness through which Transactions are transmitted. Unless you are making use of the FNB CSP, any Message received from the Merchant server will be deemed to be a Message from You. The contents of the Message received by the Bank from your CSP will be deemed to be the contents of the Message forwarded by you via the Merchant server;

1.1.8 Inform the Customer of any tax implications, exchange control regulations and/or any other relevant legislation that may be applicable to the agreement between You and the Customer;

1.1.9 Unless You are making use of the FNB CSP, You must encrypt each Transaction; and

1.1.10 Ensure that the information printed and completed on the delivery note and/or proof of Dispatch is true and correct.

1.2 Website Requirements

1.2.1 In terms of the Card Scheme Rules it is a requirement that Your website contains the following information:

1.2.1.1 the Visa and MasterCard brand mark in full colour to indicate Visa and MasterCard acceptance, as specified in the respective Visa and MasterCard Product Brand standards;

1.2.1.2 A complete description of the goods and/or services offered;

1.2.1.3 Your returns/refund policy;

1.2.1.4 Your contact details which include a contact name, telephone number, physical address of Your permanent establishment and email address;

1.2.1.5 Transaction currency (only Zambian Kwacha (ZMW) are allowed);

1.2.1.6 Your delivery policy; and

1.2.1.7 consumer data privacy policy – how the Customer's information will be used.

2. TRANSACTIONS

2.1 You may not store a Cardholder's CVV number.

2.2 You must, via Your CSP, obtain the Bank's prior Authorisation before accepting any Virtual Transaction.

2.3 You may only request Authorisation at the time of and for a particular Transaction.

2.4 You may not split or disguise Transactions or act in a way to avoid obtaining Authorisation.

2.5 Authorisation is a prerequisite for the Dispatch of any goods and delivery of services. If the initial Amount for which Authorisation was obtained differs from the final amount charged to the Customer, You must cancel the initial Authorisation request by contacting the Bank.

2.6 If Authorisation is granted, You must Dispatch the goods or deliver the service within the time stipulated in Your terms and conditions.

2.7 You are responsible for ensuring that Your CSP populates the correct CAVV and ECI indicators in the Transaction Message, failing which You will be held liable for any Loss incurred.

2.8 You must forward a Message to Your CSP consisting of a record of all Authorised Transactions in

respect of which the goods and/or services have been Dispatched. Such Message will be construed as being a guarantee given by You that such goods and/or services have been Dispatched and will constitute an instruction to the Bank to process the Transaction.

2.9 You have to securely keep a record of Your Customers' addresses.

2.10 Failure to comply with any or all of the requirements set out above will render the Transaction to be invalid.

3. 3D-SECURE

3.1 All eCommerce Merchants have to be 3D-Secure enrolled.

3.2 You will be held liable for all Losses incurred as a result of Transactions processed by You that

are not 3D-Secured.

3.3 The 3D-Secure protocol improves Transaction performance online and provides the ability to

authenticate customers during an online purchase, thus reducing the likelihood of the Fraudulent usage of Cards.

3.4 You indemnify the Bank against any and all Losses and Fraud that may occur as a result of You

Or Your CSP (unless the FNB CSP) disabling 3D-Secure. Any and all such losses and instances of

Fraud will be Charged Back to you.

4. CHARGEBACKS

4.1 Protection against Chargebacks is subject to the Rules and limited to 3D-Secure authenticated

Transactions which have been correctly secured. You need to ensure that Your Transactions are

secured at all times in accordance with the Rules.

4.2 If the 3D-Secure authentication is successful for enrolled Cards, You will process the Authorisation as usual, passing on 3D-Secure authentication data to the Bank or the CSP for processing.

4.3 You acknowledge that it is in Your best interest to ensure that You have checks and balances in place for all Virtual Transactions, as all valid Chargebacks arising from disputed Virtual Transactions will be debited from Your Nominated Bank Account.

4.4 The following Transactions do not qualify for the Chargeback liability shift (You will be acting at Your own risk and will be held liable when processing these Transactions):

4.4.1 Transactions processed on business or corporate Cards for both MasterCard, Visa and UPI that are excluded from the Chargeback liability shift. You will remain liable for all disputed Transactions;

4.4.2 If the 3D-Secure authentication is unavailable or unsuccessful for enrolled Cards and You decide to proceed with the Transaction, or where the infrastructure and/or systems of any of the participating parties, other than that of the Bank, fail. You will remain liable for all disputed Transactions.

5. REFUNDS

5.1 FNB SWITCH REFUNDS:

5.1.1 Only Refunds on credit Cards are allowed and must be processed by using the Refund facility on the Merchant's e-Commerce facility;

5.1.2 The Merchant shall process Refunds on Debit Cards by refunding the Customer via EFT (Electronic Funds Transfer);

5.1.3 The Merchant shall process each Refund to the value of the Transaction;

5.1.4 The Merchant accepts all risk and liability associated with and arising from the Merchant's use of the Refund facility;

5.1.5 The Bank shall be entitled to terminate the Refund facility at any time, on Written notice to the Merchant.

6. RISK MITIGATING MEASUREMENTS

6.1 The following guidelines, amongst others, are recommended to assist eCommerce Merchants:

6.1.1 You and Your CSP (unless FNB CSP) must ensure that You both have adequate risk management and Fraud reduction tools in place;

6.1.2 You must not store the CVV/CVC number on Your systems or write these numbers down;

6.1.3 You may only store the full Card number on Your systems and print this number on an electronic receipt in accordance with the PCI DSS requirements;

6.1.4 You must be aware of and query Transactions which are higher in value than the average

Transactions processed on Your website;

6.1.5 You must create Your own PCI DSS compliant on-line Customer database; any loss or damage

occurring due default of this shall be for your account alone and you shall indemnify the Bank against any claims arising therefrom;

6.1.6 You must be aware of Transactions where the goods are delivered to the same address but different names or Card numbers are used, or the same name but different addresses are used;

6.1.7 You must deliver the goods to a house or office and not to a person at a general or unspecified

Location who claims to be the Customer; and

6.1.8 You must confirm telephone numbers prior to delivery, especially in the case of high-value articles. A work telephone number is a more substantial reference and can usually be traced in a telephone directory.

6.2 These recommendations in Clause 6.1 serve merely as a few guidelines as the Bank does not wish to prescribe to You how You should conduct Your on-line business, nor does the Bank suggest that these guidelines will eliminate all instances of Fraud over the Internet. You solely assume all risk associated with your business and you shall indemnify the Bank against any claims arising therefrom.