eCommerce Facility Terms and Conditions

Date Last Amended: 23 February 2022

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. 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 Terms and Conditions is available on the FNB website, can be obtained from the Merchant Services National Call Centre or can be supplied to You by post and email at Your request. <u>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</u>.

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 Virtual 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 Rules;

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 Virtual 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 Virtual 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 Virtual 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 and cancellation provisions in your Customer agreement is required to:

1.2.1.3.1 point out to the Cardholder where the policy restricts the return of goods or cancellation of services;

1.2.1.3.2 be clearly disclosed to a Cardholder (which may be a link to a separate webpage), during the sequence of webpages before final checkout / payment page;

1.2.1.3.3 be accepted and/or agreed to by the Cardholder by way of pro-active conduct such as a "click to accept" button or marking a "checkbox" on the Merchant's website. The Cardholder should not be requested to make payment unless it has accepted the returns/refund and cancellation provisions. The Merchant may furnish any other evidence which proves the Cardholder's acceptance e.g. a Cardholder signed copy of the returns/refund and cancellation provisions or the Cardholder's return email accepting the returns/refund and cancellation provisions;

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 South African Rands (ZAR) are allowed);
1.2.1.6 Your delivery policy; and
1.2.1.7 consumer data privacy policy i.e. how the Customer's information will be used.

2. VIRTUAL 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 Virtual Transaction.

2.4 You may not split or disguise Virtual 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 delivery policy.

2.7 You are responsible for ensuring that Your CSP populates the correct CAVV and ECI indicators in the Virtual 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 Virtual 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 Virtual Transaction.

2.9 You must 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 Virtual Transaction to be invalid.

3. 3D-SECURE

3.1 All eCommerce Merchants must be 3D-Secure enrolled.

3.2 **You will be held liable for all Losses incurred as a result of Virtual Transactions processed by You that are not 3D-Secured.**

3.3 The 3D-Secure protocol improves Virtual 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 disabling 3D-Secure. Any and all such losses and instances of Fraudulent or Invalid Transactions will be Charged Back to you.**

4. CHARGEBACKS

4.1 Protection against Chargebacks is subject to the Rules and limited to 3D-Secure authenticated Virtual Transactions which have been correctly secured. You need to ensure that Your Virtual 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 in the ordinary course, 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 Virtual 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 Virtual Transactions):

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

4.4.2 If the 3D-Secure authentication is unavailable or unsuccessful for enrolled Cards and You decide to proceed with the Virtual 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 Virtual 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 Virtual 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 general risk mitigating measures, are recommended to assist eCommerce Merchants:

6.1.1 You and Your 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 in accordance with the PCI DSS requirements;

6.1.4 You must be aware of and query Virtual Transactions which are higher in value than the average Virtual Transactions processed on Your website;

6.1.5 You must create Your own PCI DSS compliant online Customer database;

6.1.6 You must be aware of Virtual 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 goods and services. A work telephone number is a more substantial reference and can usually be traced in a telephone directory.

6.2 These recommendations merely serve as guidelines since the Bank does not wish to prescribe to You how You should conduct Your online business, nor does the Bank suggest that these guidelines will eliminate all instances in respect of Virtual Transactions.

7. UNIVERSAL PAYMENT PAGE (UPP)

7.1 Introduction

7.1.1 These terms and conditions should be read together with the FNB Merchant Services General Terms and Conditions, eCommerce Terms and Conditions and CMS Portal Terms and Conditions.

7.1.2 UPP is available for Visa and Mastercard Transactions only and does not presently support Amex, Diner's Club or UPI Card Transactions.

7.2 Pre-Requisites

7.2.1 The Merchant is required to satisfy and comply with:

7.2.1.1 the Bank's eCommerce vetting and requirements;

7.2.1.2 the Bank's General Terms and Conditions relating to returns, Refund and/or cancellation by your Customer;

7.2.2 For Integrated UPP:

7.2.2.1 The Merchant is required to provide the Bank with relevant information as requested by the Bank, including but not limited to website development, hosting, shopping cart plug-in, transaction volumes and the timing of volumes, spike patterns and event or campaign detail. In the event that the Merchant fails to provide the information then the application will be declined.

7.2.2.2 The Merchant will require development in order to integrate its website with UPP.

7.2.2.3 In the event the Bank furnishes the Merchant with written APIs, the Merchant agrees that:

7.2.2.3.1 the Bank's sole obligation shall be to provide the written APIs to the Merchant;

7.2.2.3.2 the Merchant shall use the APIs subject to the Bank's written instructions only;

7.2.2.3.3 the Bank shall not be held responsible or be held liable in the event:

7.2.2.3.4 the Merchant is unable to successfully interact with the FNB eCommerce payment gateway and the Bank System, using the APIs; and/or

7.2.2.3.5 the Merchant relies on the APIs to the Merchant's detriment, resulting in any damages, harm or loss arising and/or being suffered by the Merchant;

7.2.2.3.6 The Merchant shall be liable for all costs related to the development for purposes of enabling ".mobi" site and/or mobile application to interact with the FNB eCommerce payment gateway and the Bank System;

7.2.2.3.7 The Merchant shall be solely responsible for all risk and liability that may arise from using of the API; and/or development of software and/or protocols in accordance with the API.

7.3 Processing Consent for Customer Information

7.3.1 The Merchant warrants that it will process (collect, use, update, make available, destroy, store, transmit or otherwise deal with and conduct the necessary checks) its Customer Data in accordance with applicable Data privacy laws.

7.3.2 The Merchant warrants that it will obtain and keep prior written consent from each of its Customers, in the format attached hereto marked “Annexure– Processing Consent Form”, to process and/or enable the Bank to process (collect, use, update, make available, destroy, store, transmit, or otherwise deal with and conduct the necessary checks) its Customer Data in accordance with this clause.

7.3.3 The Merchant shall provide the Bank with evidence of the Customer’s prior written or electronic consent, as and when requested by the Bank.

7.3.4 The Merchant hereby indemnifies and holds the Bank harmless against any Losses that may arise as a result of:

7.3.4.1 the Merchant’s actions and/or omission in accordance with this clause; and/or

7.3.4.2 the Bank performing its obligations in terms in accordance with this clause.

7.4 Transaction Processing

7.4.1 The eCommerce User must access the CMS Portal with unique credentials to create a UPP Payment Request.

7.4.2 The eCommerce User must complete the Merchant, Transaction and Customer Data to complete the UPP Payment Request.

7.4.3 The Merchant is solely responsibly to ensure that the correct Merchant, Transaction and Customer Data is captured and submitted in the UPP Payment Request.

7.4.4 The submission of a successful UPP Payment Request by the eCommerce user prompts the Bank to send the Customer an SMS or email (as per the Customer Data designated by the eCommerce user).

7.4.5 The Customer will receive a deactivated link by SMS or email. The Customer must copy the link and paste it in an internet browser to access the UPP Payment Request.

7.4.6 The Customer must input the UPN and OTP received and the follow instructions, where prompted to complete payment to the Merchant.

7.4.7 A UPP Payment Request expires 72 (seventy-two) hours from when the SMS or email is sent by the Bank. If the Customer has not accessed the link and completed the UPP Payment Request, then the eCommerce User will have to generate a new UPP Payment Request.

7.5 Refunds

7.5.1 The eCommerce User must locate and select the Transaction to be Refunded and follow instructions, where prompted to complete the Refund to the Customer.

7.6 CMS Portal Functionality

The Merchant may use CMS portal to view and manage UPP Payment Requests; to confirm a UPP Payment Request was sent; review Transaction history, including completed UPP Virtual Transactions; and filter Data according to Merchant numbers, Customers and other Data fields.

7.7 Liability

7.7.1 The Bank shall not be held liable for any Losses whatsoever and the Merchant hereby indemnifies the Bank for any such Losses as a result of:

7.7.1.1 the accuracy and completeness of the UPP Payment Request, Merchant, Transaction and Customer Data provided by the Merchant to the Bank;

7.7.2 the accuracy and completeness of the UPN, OTP and/or Card Data, input and/or provided by the Customer on the UPP Payment Request;

7.7.3 the Customer’s failure to complete a UPP Payment Request, for whatever reason;

7.7.4 the actions, omissions and/or negligence of the Merchant, Merchant’s employees, Admin User, eCommerce User and the Customer when using UPP;

7.7.5 the authorisation by the Merchant of its employees to use UPP and the misuse or unauthorised access of the Merchant’s login credentials to the CMS Portal;

7.7.6 failure or downtime in the Communication Network resulting in the delay or failure to send and/or receive the UPN and/or OTP.

Annexure – Processing Consent Form

This Consent for the referral and processing of Customer Data is provided:

	Customer Name:	Registration/Identity Number:	(“the Customer”)
by:	______________________	____________________	
	Merchant Name:	Registration/Identity Number:	(“the Merchant”)
to:	______________________	____________________	
in favour of:	FirstRand Bank Limited	1929/001225/06	(“the Bank”)

1. Definitions

In this Consent, unless the context requires otherwise:

1.1. “Data” means any data, including personal information as defined in the Protection of Personal Information Act, 2013 and any other legislation related to the protection of personal data.

2. Customer Consent

2.1. The Customer hereby unconditionally agrees to and accepts the following:

2.1.1. the Merchant is hereby expressly authorised to refer and submit the Customer Data to the Bank from time to time and that the Bank is hereby expressly authorised to receive, accept and process such Data in accordance with the below;

2.1.2. the Data provided to the Merchant and/or the Bank is accurate, true, correct, and valid;

2.1.3. that the Bank may process (which includes, without limitation, collect, store, update, use, make available or destroy) the Customer Data, to, amongst other things:

2.1.3.1. comply with legislative, risk and compliance requirements (including without limitation directives, sanctions and rules), voluntary and involuntary codes of conduct and industry requirements or to fulfil reporting requirements and information requests

2.1.3.2. detect, prevent and report theft, fraud, money laundering and other crimes; and/or

2.1.3.3. conduct security or identity verification and to check the accuracy of the Customer Data;

2.1.3.4. outside of the borders of South Africa, according to the safeguards and requirements of the law. The person processing the Customer’s Data will apply the same level of protection as required in South Africa; and/or

2.1.3.5. using automated means (without human intervention in the decision-making process) to make a decision about the Customer or the Customer’s application for any product or service. The Customer may query any decision made;

2.1.4. that the Bank may share the Customer Data with the following persons (amongst others), who have an obligation to keep the Customer Data secure and confidential:

2.1.4.1. share the results of the processing activities referred to in clause 2.1.3 with the Merchant;

2.1.4.2. law enforcement and fraud prevention agencies;

2.1.4.3. regulatory authorities, governmental departments, local and international tax authorities and other persons that the Bank under the law must share the Customer Data with; and/or

2.1.4.4. persons to whom the Bank cedes its rights or delegates its obligations.

Signed at ____________________ on this _____ day of ____________________ 20_____.

____
Customer

____
for and on behalf Customer
who warrants he/she is duly authorised
Name: __________________________
Designation: ______________________