

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 General 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 or can be supplied to via email at Your request. It is Your duty to speak to the Bank by contacting the Merchant Services helpdesk 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. PURPOSE OF THE MERCHANT AGREEMENT

- 1.1 Approval of the Merchant's Application for Acquiring Services and products is subject to the Bank conducting an assessment on the Merchant and the Merchant providing additional information or documentation, which may be requested by the Bank.
- 1.2 The Bank agrees to make Acquiring Services available to the Merchant under the Terms and Conditions for the duration of the Merchant Agreement. By using the Acquiring Services and products, including any additional outlets which may be added to the Merchant profile. You agree to be bound by the Terms and Conditions of the Merchant Agreement.

2. INTERPRETATION

- 2.1 First National Bank of Lesotho Limited is represented in the Merchant Agreement by FNB Merchant Services, a business unit of the Bank.
- 2.2 In the Merchant Agreement, unless the context otherwise indicates:
 - 2.2.1 natural persons shall include juristic entities (incorporated or unincorporated) and vice versa;
 - 2.2.2 the headings in the Merchant Agreement are used for the sake of convenience and shall not govern the interpretation hereof;
 - 2.2.3 all expressions contained in the Merchant Services General Terms and Conditions shall have the same meaning in the Product and/or Services Terms and Conditions; the Master Agreement (if applicable); and related Annexures; Schedules; and merchant documentation unless if otherwise defined;
 - 2.2.4 if any provision in a definition is a substantive provision conferring rights or imposing obligations on any Party, notwithstanding that it is only in the definition's clause, effect shall be given to it as if it was a substantive provision of the Merchant Agreement;
 - 2.2.5 reference to a statutory enactment shall be construed as a reference to that enactment as at the Effective Date and as amended or substituted from time to time;
 - 2.2.6 reference to "days" shall be construed as Calendar Days unless qualified by the word "Business";
 - 2.2.7 unless specifically otherwise provided, any number of days prescribed shall be determined by excluding the first and including the last day or, where the last day falls on a Saturday, Sunday or public holiday, the next succeeding Business Day;
 - 2.2.8 where figures are referred to in numerals and in words and there is any conflict between the two, the words shall prevail;
 - 2.2.9 any reference to payments in the Merchant Agreement refers to both the Lesotho Loti (LSL) and South African Rands (ZAR). You must adhere to the Central Bank of Lesotho's ("CBL") and South African Reserve Bank's ("SARB") financial limits specified in LSL and ZAR when processing an amount in foreign currency;
 - 2.2.10 no provision herein shall be construed against or interpreted to the disadvantage of a Party by reason of such Party having or being deemed to have structured, drafted and/or introduced such provision;
 - 2.2.11 the words "include" and "including" mean "include without limitation" and "including without limitation". The use of the words "include(s)" and "including" followed by a specific example or examples shall not be construed as limiting the meaning of the general wording preceding it;

- 2.2.12 the Merchant Agreement is subject to the Financial Institutions Act, 2012, Money Laundering and Proceeds of Crime Act, 2008, Data Protection Act, 2011 and all other legislation and regulations as well as the Card Scheme Rules and industry requirements, as amended from time to time;
- 2.2.13 the Parties acknowledge that each clause of the Merchant Agreement is separate. If any clause of the Merchant Agreement is or becomes illegal, invalid and/or unenforceable for any reason, it must be treated as if it had not been included in the Merchant Agreement. This will not result in the remainder of the Merchant Agreement being illegal, invalid or unenforceable;
- 2.2.14 defined terms used in a sentence will generally have the initial letter capitalised; and
- 2.2.15 **terms printed in bold place a strict obligation on You and should therefore be carefully read and understood.**

3. DEFINITIONS

- 3.1 **“Acquiring Bank”** means the bank or financial institution that processes payments for You;
- 3.2 **“Acquiring Services”** means the services that the Bank, in its capacity as an Acquiring Bank, makes available and renders to You, which include but are not limited to:
 - 3.2.1 processing of Virtual Transactions, Integrated Solutions, Stand-Alone Solutions, Mobile POS Solutions and any other payment acceptance services and solutions agreed to between the Parties;
 - 3.2.2 providing a facility that allows You to accept Payment Instruments as a means of payment;
 - 3.2.3 providing the means for Transactions to be routed and Authorised; and/or
 - 3.2.4 collecting funds from the Issuing Bank and settling Transactions with You.
- 3.3 **“Affiliate”** means (a) any subsidiary or a holding company of either Party or any entity that controls, is controlled by or is under common control of either Party. The terms "subsidiary" and "holding company" shall have the meaning assigned thereto by the Companies Act, 2011, as amended, and (b) any entity that controls, is controlled by or is under common control of either Party. For the purposes of this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty percent) plus 1 (one) of the possible votes;
- 3.4 **“Aggregation”** means the practice whereby a Merchant acts as a payment facilitator for other merchants (sub-merchants), which results in several sub-merchants sharing one common merchant facility or Merchant number. The term **“Aggregator”** will be construed accordingly;
- 3.5 **“Amex”** means American Express, a financial services corporation;
- 3.6 **“Annexure”** means a document marked “Annexure” and signed by both Parties;
- 3.7 **“API”** means application point integration;
- 3.8 **“ASV”** means Approved Scan Vendor, an organisation that uses a set of security services and tools to conduct external vulnerability scanning services to validate adherence with the PCI DSS requirements;
- 3.9 **“Authorise” or “Authorisation”** means the process whereby You or Your Third Party Service Provider transmits a message to the Bank enquiring whether a Customer has sufficient funds in his/her bank account to enter into a Transaction in terms of which the Customer purchases goods and/or services from You. Should the Bank receive confirmation from the Issuing Bank that it is satisfied that sufficient funds are available to the Customer, the Bank shall in turn transmit a message to You or Your Third Party Service Provider “Authorising” the intended Transaction. Should the Bank receive confirmation from the Issuing Bank that there are insufficient funds in the Customer’s account, the Transaction will be declined. Where the Transaction is Authorised, “Authorisation” is said to have taken place. The Bank may in its discretion withhold Authorisation;
- 3.10 **“Authorised Representative/s” or “Duly Authorised Representative/s”** means a key person duly appointed by a Party to perform and execute the rights and obligations in terms of this Merchant Agreement and to send and receive instructions on behalf of such Party;
- 3.11 **“the Bank”** means First National Bank of Lesotho Limited, a division of FirstRand Bank Limited, a commercial bank and a company with limited liability, duly incorporated in accordance with the company laws of the Kingdom of Lesotho with registration number I2008/729, together with its successors in title.;
- 3.12 **“BIN”** means bank identification number;
- 3.13 **“Bot Army – Scripted Attack”** means an attack where computer programs work automatically and are used to send spam (unwanted electronic messages), or to attack other computers and cause them to stop working correctly;
- 3.14 **“Brute Force Attack”** is also known as brute force or brute force cracking and describes a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive

guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organisation's network security. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

- 3.15 **"Budget Transaction" or "Budget Transactions"** means a Transaction where the Issuing Bank Authorises the Customer to make a payment over an extended period;
- 3.16 **"Business Day" or "Business Days"** means any day other than a Saturday, Sunday or a public holiday
- 3.17 **"Business Rescue"** shall have the meaning set out in Insolvency Proclamation as amended from time to time;
- 3.18 **"Calendar Day" or "Calendar Days"** means any day in a month, including a Saturday, Sunday or public holiday;
- 3.19 **"Calendar Month"** means each of the twelve named periods into which a year is divided, commencing on the 1st day of that month and ending on the last day i.e. the 28th; 29th; 30th or 31st day as the case may be;
- 3.20 **"Captcha"** means a program that protects websites against Bot Army-Scripted Attacks by generating and grading tests that human beings can pass but current computer programs cannot. For example, humans can read distorted text, but current computer programs cannot;
- 3.21 **"Card" or "Cards"** means the presentation of payment Data used to facilitate Authorisation and settlement; and includes any physical or virtual card and/or token, issued by a bank; Card Scheme; a Bank approved Card loyalty scheme and private label organisation. Reference to Card(s) includes Fleet Card(s);
- 3.22 **"Card Scheme" or "Card Schemes" or "Card Association" or "Card Associations"** means Visa, MasterCard, UPI, RCS, Diners and Amex card schemes etc.;
- 3.23 **"Card Not Present Transaction" or "Card Not Present Transactions" or "CNP Transaction" or "CNP Transactions"** means a Transaction which takes place without a physical Card being presented to You by the Customer;
- 3.24 **"Cashback with Purchase Transaction" or "Cashback with Purchase Transactions"** means an agreement concluded between You and a Customer in terms of which the Customer purchases goods and services from You and simultaneously withdraws cash from You;
- 3.25 **"Cash Advance"** means an agreement concluded between You and a Customer in terms of which the Customer withdraws cash from You without purchasing goods and services from You;
- 3.26 **"CAVV"** means Customer Authentication Verification Value, the 3 (three) digit number on the back of a Card;
- 3.27 **"Chargeback" or "Chargebacks" or "Charged Back"** means the return of a payment instruction by the Issuing Bank as a result of a Customer dispute, an Invalid Transaction or a Fraudulent Transaction;
- 3.28 **"Chip Card" or "Chip Cards"** means a Card which has a chip embedded in it and which is driven by a PIN;
- 3.29 **"CMS"** means Content Management System;
- 3.30 **"CMS Portal"** means the Content Management System Portal which provides You with insight into the performance of Your business by providing transactional, financial and fraud related data;
- 3.31 **"Communication"** means the imparting of information to a Party; or the exchange of information between the Parties;
- 3.32 **"Communication Network"** means the connectivity between the Speedpoint® Device, Third Party Service Provider and/or the Bank network. This includes satellite communication;
- 3.33 **"Companies Act"** means the Companies Act of 2011 as amended from time to time;
- 3.34 **"Contactless"** means processing a Card Transaction by using a dual interfaced Card, without making physical contact with a contactless enabled Speedpoint® Device. The Card details are accessed and processed electronically by the contactless enabled Speedpoint® Device;
- 3.35 **"Cooling Off Period"** means a period of 5 (five) Business Days from the date of conclusion of the Merchant Agreement or the date reflected on the notification of the updated Merchant Agreement, or such other period as advised of by the Bank or agreed to by the Parties;
- 3.36 **"CPA"** means Consumer Protection Act number 68 of 2008 as amended from time to time;
- 3.37 **"CPI"** means the Consumer Price Index (all groups, all areas) and "CPI inflation" shall mean the percentage escalation of the Consumer Price Index for the average twelve (12) months preceding the anniversary of the Effective Date, as published by Statistics South Africa from time to time, provided that if the publication of the CPI ceases at any time, a substitute index shall be applied which reflects the general rate of inflation in the Republic of South Africa;
- 3.38 **"CSP"** means Commerce Service Provider (including FNB CSP, unless otherwise stated), a service provider that specialises in providing web-based secured electronic commerce services;

- 3.39 **"CSP Network"** means the CSP's information technology network (connected between its entry and exit core routers), which includes routers, switches, firewalls, cabling, the CSP Software, any other hardware, software and infrastructure forming part thereof or related thereto;
- 3.40 **"CSP Software"** means the software components (including any updates and/or upgrades thereto) utilised by the CSP to provide payment services to You;
- 3.41 **"Customer"** or **"Customers"** or **"Cardholder"** or **"Cardholders"** means the person/entity who uses a Payment Instrument to pay for goods and services at a Merchant;
- 3.42 **"CVC"** or **"CVC 2"** means Card Verification Check;
- 3.43 **"CVV"** or **"Card Verification Value"** means the 3 (three) digit number printed on the reverse of a Card;
- 3.44 **"Data"** means any data and/or information, including personal data and information as defined in the POPI and any other legislation; regulations; Card Scheme Rules and industry requirements, relating to the protection of: data and information, Customer data and information supplied by the Bank, data and information stored, collected, collated, accessed, received, recorded, modified, retrieved, altered, used and/or processed;
- 3.45 **"Data Compromise"** means the unauthorised access, transmission or use of Data or the damage, erasure, copying, disruption, alteration, corruption, loss, theft, degradation, dissemination or distribution of the Data in any manner;
- 3.46 **"DCC"** means Dynamic Currency Conversion a point-of-sale service whereby international Visa and MasterCard Customers can choose to pay for goods and service in their own home currency, rather than the domestic currency of the country where the purchase is taking place;
- 3.47 **"Debit Card"** means a Card that deducts money directly from a Customer's bank account when a Transaction is processed on the Card;
- 3.48 **"Defaced"** or **"Mutilated"** means a Card that is damaged;
- 3.49 **"Dispatch"** or **"Dispatched"** means the release of goods and/or services;
- 3.50 **"Diners"** or **"Diners Club"** means Diners Club International, a financial services corporation;
- 3.51 **"Duel Interfaced Card"** means a Card that may be used for both Contactless and contact Transactions;
- 3.52 **"eBucks"** means the Bank's multi-partner rewards programme;
- 3.53 **"eBucks Card"** or **"eBucks Cards"** means a private label eBucks branded Card, a Payment Instrument that can be used to earn and spend eBucks;
- 3.54 **"eCommerce Services"** means the Acquiring Services and facilities that the Bank makes available and renders to You for the purposes of processing Virtual Transactions;
- 3.55 **"ECI"** means Electronic Commence Indicator, a 2 (two) or 3 (three) digit code issued by the Card Scheme or the Bank to notify You of the authentication of the Cardholder and the status of the Cardholder's Issuing Bank under 3D Secure;
- 3.56 **"Effective Date"** means the date on which the Terms and Conditions become effective, being the date upon which the Equipment is installed at Your Premises or the date upon which You processed Your first Transaction, whichever is the earliest of the dates;
- 3.57 **"eReceipt"** means an electronic confirmation of a Transaction processed by You, recording the date, Merchant name, Merchant location, PAN, amount and reference number, sent by SMS or email to You and the Customer;
- 3.58 **"EMV"** means a global standard for Card-based chip technology;
- 3.59 **"Equipment"** means the Bank's: Speedpoint® Devices, keypads, terminal driver, network switch, router, Communication Networks, satellite dish, router and modem; and any other utilities and attachments, which are provided by the Bank and utilised when processing Transactions from time to time;
- 3.60 **"Equipment Rental Amount"** means the monthly Equipment rental amount payable by You to the Bank as reflected on Your Statement;
- 3.61 **"eWallet"** means an electronic store of cash value, offered by the Bank to eWallet Customers enabling eWallet Customers access to funds by way of a cellphone rather than a bank account or Card;
- 3.62 **"eWallet Balance"** means the cash value available to the User (the holder of the eWallet);
- 3.63 **"eWallet Transactions"** means any purchase Transaction in respect of which an eWallet Customer purchases goods and/or services for which Authorisation has been obtained; any Cash Advance (cashback only) Transaction in respect of which an eWallet Customer withdraws cash and for which Authorisation has been obtained; and any Cashback with Purchase Transaction;
- 3.64 **"Excessive Authorisation Attempt"** means each Authorisation: (i) after 20 (twenty) previously declined Authorisations attempts; (ii) made on the same Card; (iii) made at the same Merchant; (iv) and made within a 24 (twenty-four) hour period, as amended from time to time;

- 3.65 **"Fallback Transaction"** means the process that is followed when a normal Chip Card Transaction cannot be completed on a Speedpoint® Device due to a Speedpoint® Device being unable to read the Chip Card, and where the Speedpoint® Device prompts You to complete the Transaction using the magnetic strip;
- 3.66 **"MLPCA"** means the Money Laundering and Proceeds of Crime Act, 2008 as amended from time to time;
- 3.67 **"Fleet Card" or "Fleet Cards"** means a Card which can be used as a means of payment by Customers for procuring goods and services as specified in the Fleet Card Terms and Conditions;
- 3.68 **"Floor Limit"** means a set amount which a Customer may spend on a single Transaction using a Payment Instrument without obtaining Authorisation;
- 3.69 **"FNB Pay"** means a digital platform within the FNB Banking App that enables a Customer to use a mobile device to make mobile payments to FNB Merchants;
- 3.70 **"FNB CSP"** means the FNB Commerce Service Provider appointed by You to provide web based secure electronic commerce services;
- 3.71 **"FNB CSP Switch Solution"** means routing Transactions from You, through the FNB CSP Network to the Acquiring Bank network for Authorisation by the Issuing Bank and/or settlement by the Acquiring Bank;
- 3.72 **"FNB Fuel Solution"** means a solution that is specifically created to address the needs of fuel merchants;
- 3.73 **"FNB PSP"** means FNB payment service provider appointed by You to perform, amongst other things, Transaction switching services and configuration management at Your Premises;
- 3.74 **"FNB PSP Network"** means the FNB PSP's information technology network (connected between its entry and exit core routers), which includes routers, switches, firewalls, cabling, the FNB PSP Software, any other hardware, software or infrastructure forming part thereof or related thereto;
- 3.75 **"FNB PSP Software"** means the software components (including any updates and/or upgrades thereto) utilised by the FNB PSP to provide the payment services to You;
- 3.76 **"FNB PSP Switch Solution"** means routing Transactions from You, through the FNB PSP Network to the Acquiring Bank for Authorisation by the Issuing Bank and/or settlement by the Bank;
- 3.77 **"FNB Satellite Services"** means services rendered by the Bank in terms of which a satellite dish is installed on Your Premises;
- 3.78 **"FSR"** means the FirstRand Group;
- 3.79 **"Fraud" or "Fraudulent"** means a wrongful or criminal deception intended to result in financial or personal gain;
- 3.80 **"Fraudulent Transaction" or "Fraudulent Transactions"** means: any transaction that constitutes Fraud under the law and/or common law (irrespective of whether or not the Card Transaction was Authorised or whether or not an Authorisation code number was provided to You by the Bank); a Transaction that is processed using a Customer's financial detail, account information or Payment Instrument which is not authorised by the Customer; or the use of a card which has not been issued by a genuine Card Issuer;
- 3.81 **"Force Majeure" or a "Act of Disaster"** means an inevitable event that directly and exclusively results from the occurrence of a natural disaster that could not have been prevented by exercising foresight or caution;
- 3.82 **"General Packet Radio Service Device" or "GPRS Device"** means equipment authorised by the Bank which uses cellular communication infrastructure;
- 3.83 **"General Terms and Conditions" or "Merchant Services General Terms and Conditions"** means these terms and conditions governing the relationship between the Parties in relation to the Acquiring Services and products. The General Terms and Conditions have to be read in conjunction with the Product and/or Services Specific Terms and Conditions; and the Master Agreement (where applicable);
- 3.84 **"Hot Card"** means a Card that has been reported as being lost or stolen;
- 3.85 **"Hold and Call" or "Code 10"** means the code that You will use to inform the Bank of a Customer who is acting suspiciously or to report a suspicious transaction;
- 3.86 **"In-App Purchases"** means the purchase of goods and services using an application on a mobile device, such as a smartphone or tablet;
- 3.87 **"Interchange Rate"** means a fee paid by the Acquiring Bank to the Issuing Bank. It is generally calculated as a percentage of the Transaction value. The fee is regulated and prescribed by the SARB on local Transactions. International Transactions attract various interchange fees that are not regulated by the SARB;

- 3.88 **"Integrated Solutions"** means an integrated Speedpoint® Device, offering Payment Instrument acceptance as part of an integrated cash register system. This solution may include a computer, computer software and Speedpoint® Device hardware components;
- 3.89 **"Intellectual Property"** means, without limitation, any know-how, patent, copyright, registered design, trademark or other industrial or intellectual property rights, whether registered or not and whether or not capable of being registered and any application for any of the aforementioned;
- 3.90 **"Internet"** means the collection of local area networks, wide area networks and third party networks which all use the same protocol to form a seamless, packet switching network;
- 3.91 **"ISO"** means International Organisation for Standardisation;
- 3.92 **"Issuing Bank"** means a bank that issues Cards;
- 3.93 **"Invalid Transaction"** means:
- 3.93.1 a Transaction which arises as a result of the following (irrespective of whether or not the card Transaction was Authorised or whether or not an Authorisation code number was provided to You by the Bank):
- 3.93.1.1 an act and/or omission by You and/or Your employees which results in a Loss or Chargeback;
- 3.93.1.2 the use of a Payment Instrument by a person other than the lawful Customer;
- 3.93.1.3 processing a Transaction without the Bank's prior Authorisation;
- 3.93.1.4 a Transaction where the date of the Transaction is earlier than the start date shown on the Card;
- 3.93.1.5 accepting Cards which are: Defaced; blank; illegible or Cards from which the embossed legends are not readable or legible;
- 3.93.1.6 accepting a Card which has expired;
- 3.93.1.7 accepting a Payment Instrument for any purpose other than current Transactions;
- 3.93.1.8 duplicating a Transaction;
- 3.93.1.9 a Transaction for which You do not have a corresponding Receipt or eReceipt;
- 3.93.1.10 a Transaction for which the Receipt is illegible;
- 3.93.1.11 a Transaction for which the Receipt or eReceipt is materially incomplete or different from the Receipt or eReceipt provided to the Customer;
- 3.93.1.12 a Transaction for which You launder Receipts or eReceipts;
- 3.93.1.13 a Transaction where the value exceeds the authorised Floor Limit and no Authorisation has been obtained from the Bank;
- 3.93.1.14 a Transaction which does not comply with the obligations set out in the Rules;
- 3.93.1.15 a Transaction for which the goods or services were not delivered within the agreed period or at all;
- 3.93.1.16 a Transaction where the supply of goods and/or services is for any reason illegal;
- 3.93.1.17 a Transaction which was performed by Your employee(s) not authorised to do so; or
- 3.93.1.18 a Transaction which occurred as a result of an error on Your, Your employee(s) or Third Party Service Providers' part;
- 3.93.1.19 a Fraudulent Transaction; or
- 3.93.1.20 accepting a Payment Instrument from You or Your Authorised Representative in respect of any type of Transaction for any reason other than the valid supply of goods and/or services, which shall be evidenced upon request by the Bank;
- 3.93.2 Should a Transaction be regarded as an Invalid Transaction or incomplete, the Bank has the right to charge each such Invalid Transaction or incomplete Transaction back to You and You will be held liable for all Losses incurred as a result of the Invalid Transaction or incomplete Transaction. The Bank further has the right to immediately terminate the Merchant Agreement;
- 3.94 **"Loss"** or **"Losses"** means any and all damages, fees, costs, charges, Chargebacks, expenses, instructions, commitments, disputes, claims, defences, fines and penalties imposed upon or incurred by the Bank, howsoever arising in connection with You, Your employees and/or Your Third Party Service Providers;
- 3.95 **"Malware"** means malicious software, which can perform a variety of different functions such as stealing, encrypting or deleting Confidential Information and/or Data, altering or hijacking core Equipment and/or computing functions and monitoring users' computer activity without their permission;
- 3.96 **"Manual Entry Facility Transaction"** or **"Manual Entry Facility Transactions"** means a Transaction whereby the Card details are manually keyed into the Speedpoint® Device, instead of the Card being swiped on the Speedpoint® Device or inserted (dipped) into the Speedpoint® Device;
- 3.97 **"Mastercard"** means Mastercard Incorporated or Mastercard Worldwide, an American multinational financial services corporation headquartered in the Mastercard International Global Headquarters, Purchase, New York, United States. MasterCard facilitates electronic funds transfers throughout the world, most commonly through MasterCard branded cards;

- 3.98 “**Mastercard Secure Code**” means Mastercard’s interpretation of the 3D-Secure code specification;
- 3.99 “**Master Agreement**” or “**Merchant Services Master Agreement**” or “**Service Level Agreement**” or “**SLA**” means an agreement entered into between You and the Bank, which sets out the rights and obligations specific to Your business and which forms part of Your Merchant Agreement;
- 3.100 “**Material Amendment**” means an amendment to the Terms and Conditions, which impacts Your day-to-day business operations in respect of the Acquiring Services and products provided to You by the Bank;
- 3.101 “**Merchant**” means the entity or person which has entered into a Merchant Agreement with the Bank;
- 3.102 “**Merchant Agreement**” means the application form (online or paper based); recorded telephone calls (when signing up or accepting the Terms and Conditions or pricing over the telephone); the Terms and Conditions; Statements, any Merchant Services specific schedules or annexure to a Master Agreement and the Master Agreement (if applicable);
- 3.103 “**Merchant Commission**” means a percentage of the monetary value of the Transactions which is payable monthly by You to the Bank as reflected on Your Statement;
- 3.104 “**Message**” means an electronic communication from Your server to Your Third Party Service Provider or vice versa, in the format as prescribed by the Bank from time to time;
- 3.105 “**MMF**” means Minimum Merchant Fee i.e. the amount payable by the Merchant to the Bank, should the Transactions processed be less than the threshold set by the Bank;
- 3.106 “**Mobile Point of Sale**” or “**Mobile POS Solution**” means the functionality that enables Transactions to be processed using a smartphone or tablet instead of a Speedpoint® Device;
- 3.107 “**Month**” also referred to as “Calendar Month” means any of the twelve parts, into which a calendar year is divided;
- 3.108 “**MOTO**” means a Mail-Order, Telephone-Order, a Transaction in which a Customer orders goods or services from a Merchant by way of mail or telephone and where neither the Payment Instrument nor the Customer is present at the Merchant’s Premises during the time that the Transaction is processed;
- 3.109 “**NCA**” means National Credit Act, number 34 of 2005 as amended from time to time;
- 3.110 “**Network Operators**” means MTN, Vodacom, Cell C, Virgin Mobile and any other network operator that the Bank may advise You of from time to time;
- 3.111 “**Nominal Amount Authorisation**” means any approved Card Not Present Transaction, Authorised for a nominal amount, equal to or less than 1 (one) ZAR (Rand) (or an equivalent single unit of currency, if the Transaction currency is not ZAR (Rand)), with a subsequent reversal;
- 3.112 “**Nominated Bank Account**” or “**Clearing Account**” means the bank account that will be debited and credited by the Bank in respect of the Merchant Agreement;
- 3.113 “**PAN**” or “**Primary Account Number**” means the Card number printed on the front of the Card;
- 3.114 “**Party**” or “**Parties**” means either the Bank or You, or both, as the context indicates;
- 3.115 “**PASA**” means the Payment Association of South Africa and its successor in title, being the payment system management body as approved by the South African Reserve Bank and which determines industry requirements applicable to the Bank and in turn, its Merchants;
- 3.116 “**Payment Instrument**” means a Card, mobile, key fob and any other mechanism that is designed to hold secure data and that enables the flow of funds from the holder of the payment instrument to another party, which shall include third party mobile payment and digital wallet services such as Samsung Pay, Apple Pay and the like;
- 3.117 “**PCI**” means Payment Card Industry;
- 3.118 “**PCI DSS**” means Payment Card Industry Data Security Standard;
- 3.119 “**PED**” means pin entry device;
- 3.120 “**PFI**” means a **PCI forensic investigator accredited by the Card Schemes to investigate the occurrence of a Data Compromise and determine when and/or how a Data Compromise may have occurred;**
- 3.121 “**Phishing Attacks**” means a type of online scam where criminals send out Fraudulent email messages that appear to come from a legitimate source. The email is designed to trick the recipient into entering Confidential Information and/or Data (for example: Merchant Account numbers, passwords, Card Data, PIN, etc.) into a fake website, by clicking on a malicious link. The email will include a malicious link or attachment, which once clicked, will steal Confidential Information and/or Data or infect computers and/or Equipment with Malware. Cybercriminals will use this information to commit identity fraud or sell it on to another criminal third party;
- 3.122 “**PIN**” means the personal identification number of a Card;
- 3.123 “**DPA**” means the Data Protection Act, 2013 as amended from time to time;
- 3.124 “**Portal**” means a web-based management and reporting system that allows Merchants to Monitor and

analyse the Transactions they process on Speedpoint® App;

- 3.125 **"Pre-Authorisation"** means a Transaction processed by You in terms of which a temporary hold is placed for a specific amount on the available balance on a Customer's Card;
- 3.126 **"Premises"** or **"Stores"** or **"Dealers"** means the Merchant location at which the Equipment is in use and/or installed;
- 3.127 **"Prepaid Airtime"** means Network Operator minutes, the sale of which is facilitated through the use of the Speedpoint® Device;
- 3.128 **"Prepaid Airtime Service Facility Account"** means an account(s) held by the Bank in Your name that is pre-funded and that will be debited with the value of the sales of the Prepaid Products;
- 3.129 **"Prepaid Airtime Service Facility Customer"** means a Customer who purchases a Prepaid Product, the sale of which is facilitated through the use of the Speedpoint® Device;
- 3.130 **"Prepaid Products"** means prepaid products and services of Network Operators and Third Party Service Providers, which are offered to Customers by way of a Speedpoint® Device;
- 3.131 **"Product and/or Service Specific Terms and Conditions"** means the terms and conditions governing the use of the Bank's Acquiring Service and products for example: Terms and Conditions for the Use of the Speedpoint® Device; eCommerce Terms and Conditions etc. These Terms and Conditions are available on the FNB website and a copy can be obtained from the Merchant Services National Call Centre or can be supplied to You by post and email at Your request;
- 3.132 **"PSP"** means a Third-Party Payment Service Provider (including the FNB PSP, unless otherwise stated) appointed by You to perform amongst other things, the routing of Transactions from You to the Bank and configuration management;
- 3.133 **"QR-Code"** means a bar code that is allocated to You to enable You for every Transactions which a Customer will scan to purchase goods or services;
- 3.134 **"QSA"** means a Qualified Security Assessor, an independent security organization that has been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS;
- 3.135 **"RCS"** means RCS Cards (Pty) Limited, a company registered according to the company laws of South Africa, with registration number: 2000/017891/07;
- 3.136 **"Receipt"** means the written confirmation of a Transaction processed by You, recording the date, Merchant name, Merchant location, PAN, amount, and reference number and shall include an **eReceipt** if the context or circumstances require;
- 3.137 **"Recipient Cellphone Number"** means the cell phone or mobile number selected by You or the Customer which will be credited with Prepaid Airtime;
- 3.138 **"Refund"** means a Transaction that is the opposite of a purchase Transaction. A refund is a credit payment instruction issued by You to the Issuing Bank to credit a Customer's account. Such credit payment instruction is issued by You subsequent to a debit payment instruction. For example: the Customer returns goods to You and is credited for the value of the goods;
- 3.139 **"Remedial Maintenance"** means to remedy, repair and correct malfunctions, breakdowns and/or faults in the Equipment and Equipment software;
- 3.140 **"Reversal"** means the cancellation of a previous Transaction;
- 3.141 **"ROC"** means a Report on Compliance, a form that must be completed by all Level 1 Merchants as defined in the PCI DSS clause herein;
- 3.142 **"Routine Maintenance"** means maintenance that is required to maintain the Equipment in good working order and condition;
- 3.143 **"RPI"** means Recurring Payment Instruction whereby multiple Transactions are processed at predetermined intervals, not exceeding one year periods. RPI comprises an agreement between a Customer and You to purchase goods or services over a period of time;
- 3.144 **"Rules"** means the provisions set out in the Merchant Agreement, applicable local or international legislation and regulations; Card Scheme rules; the Bank and industry requirements, as amended from time to time;
- 3.145 **"SAQ"** means a PCI DSS Self-Assessment Questionnaire, which is a validation tool intended to assist Merchants and service providers who are permitted by the Card Schemes to self-evaluate their compliance with the PCI DSS;
- 3.146 **"CBL"** means the Central Bank of Lesotho, the regulator of banks and all financial institutions, which is governed by the Central Bank Act, 2000.;
- 3.147 **"Schedule"** means any document marked as such and signed by both Parties;
- 3.148 **"Schedule of Fees and Charges"** means a document setting out the fees and charges payable by You to the Bank in respect of the Acquiring Services and products provided to You by the Bank. Your Statement is regarded as Your latest Schedule of Fees and Charges;

- 3.149 **Security Assessment**” means the validation of compliance of You and Your Third Party Service Providers with the Rules;
- 3.150 **“Speedee®”** means any mobile, standalone Speedpoint® Device, which issues an eReceipt sent by SMS or email instead of printing a Receipt;
- 3.151 **“Speedpoint® App”** means a digital platform within the FNB Banking App, that allows FNB Merchants to use mobile devices to accept mobile payments;
- 3.152 **“Speedpoint® Device”** or **“Speedpoint® Devices”** means any standalone or integrated pin entry device and shall include a **Speedee®** if the context or circumstances require;
- 3.153 **“Stand-Alone Solution”** or **“Stand-Alone Speedpoint® Device”** means a solution whereby a Speedpoint® Device is not integrated with other systems in the Payment Instrument acceptance environment. It is a free-standing Speedpoint® Device connected by way of a dedicated Communication Network facility to the Bank;
- 3.154 **“Statement”** means a Tax Invoice setting out the fees and charges payable by You to the Bank;
- 3.155 **“Terms and Conditions”** means the Merchant Services General Terms and Conditions and Product and/or Service Specific Terms and Conditions, collectively;
- 3.156 **“Third Party Service Provider”** or **“Third Party Service Providers”** means a third-party company appointed by a Party from time to time to perform services on behalf of such Party; for example, a third party appointed by the Bank to perform installation services, Routine Maintenance and/or Remedial Maintenance or a PSP or CSP appointed by You;
- 3.157 **“Transaction”** or **“Transactions”** means any transaction in respect of which the Customer purchases goods and/or services from You and for which Authorisation has been requested or obtained;
- 3.158 **“Three Domain Secure”** or **“3D-Secure”** means an XML-based protocol designed to be an additional security layer for online credit Card and Debit Card Transactions. 3D-Secure improves online Transaction performance and provides the ability to authenticate Customers during an online purchase, thus reducing the likelihood of Fraudulent usage of Cards;
- 3.159 **“UPI”** means Union Pay International, an association for China's banking card industry, operating under the approval of the People's Bank of China;
- 3.160 **“User”** means the holder of the eWallet wanting to undertake eWallet Transactions;
- 3.161 **“VAT”** means Value Added Tax as defined in terms of the Value-Added Tax Act, as amended from time to time;
- 3.162 **“Verified by Visa”** means Visa’s interpretation and application of the 3D-Secure code specification;
- 3.163 **“Virtual Transaction”** or **“Virtual Transactions”** means the purchase of goods and/or services over the Internet by the Customer from You, whether the Transaction is facilitated by an Aggregator or not, for which Authorisation has been obtained, or the purchase of goods and / or services using the FNB Banking App;
- 3.164 **“VISA”** means Visa Inc., an American multinational financial services corporation headquartered in Foster City, California, United States. VISA facilitates electronic funds transfers throughout the world, most commonly through Visa-branded Cards;
- 3.165 **“Warranty”** means a confirmation on Your part that something is or will be as You have represented and/or promised the Bank and/or Customer;
- 3.166 **“Writing”** or **“Written”** means any written communication between the Parties concerned and shall include email; and
- 3.167 **“You”** or **“Your”** means the Merchant.

4. DURATION

4.1 Duration - General

- 4.1.1 **This Merchant Agreement will commence on the Effective Date and shall endure indefinitely thereafter until terminated by the Merchant in Writing or telephonically, by providing no less than a Calendar Months’ notice (i.e. notice on or before the 1st day of a month for the end of that month) to the Bank or as provided for herein.**
- 4.1.2 **This Merchant Agreement may be terminated by the Bank as provided for in the Merchant Agreement or on 30 days’ notice to the Merchant or otherwise in the sole discretion of the Bank.**
- 4.1.3 **You have the right to terminate this Merchant Agreement within the Cooling-Off Period.**
- 4.1.4 **Upon termination of the Merchant Agreement for whatever reason, You will be responsible for the remaining responsibilities in respect of the Acquiring Services and products delivered by the Bank and for all Losses incurred as a result of Your actions and/or omissions.**
- 4.1.5 **When the Merchant Agreement terminates, the clauses in this Merchant Agreement will**

continue to apply to Transactions which were processed by the Merchant on or before the date on which the termination of this Merchant Agreement took effect. Termination of this Merchant Agreement will not affect any rights and/or obligations of the Parties that arose in terms of the Merchant Agreement on or before the termination became effective.

4.1.6 Upon the termination of this Merchant Agreement, You will return to the Bank all papers, materials and other property of the Bank in Your possession or held by You in connection with the performance of this Merchant Agreement.

4.2 Upon termination of the Merchant Agreement, You shall not honour any Cards. In the event of You honouring Cards after the termination of this Merchant Agreement, then, without prejudice to any other remedies which might thereupon be available to the Bank, the Bank may elect to apply the provisions of the Merchant Agreement to any subsequent Transaction as if the Merchant Agreement had not been terminated.

4.3 **FNB Satellite Services**

4.3.1 The agreement between You and the Bank in respect of the FNB Satellite Services will endure for a period of 3 (three) years, commencing from the date of installation of the FNB Satellite equipment at Your Premises ("Initial Term").

4.3.2 The relationship between You and the Bank will be governed by the Terms and Conditions.

4.3.3 Upon the expiry of the Initial Term, the agreement between You and the Bank in respect of the FNB Satellite Services shall proceed on a month to month basis, on the Terms and Conditions of the Merchant Agreement, until terminated by the Merchant in Writing or telephonically, by providing no less than a Calendar Months' notice to the Bank or as provided for herein.

4.3.4 Should the Merchant Agreement be terminated prior to the expiry of the Initial Term, the Bank shall hold the Merchant liable for an early termination fee that will be calculated based on the remaining term of the Initial Period, the deinstallation fee incurred by the Bank for the deinstallation of the Equipment, the Equipment finance costs and the software licence fee payable in respect of the remaining term.

4.4 **FNB PSP Switch Solution and FNB CSP Switch Solution**

4.4.1 The agreement between You and the Bank in respect of the FNB PSP Switch Solution or FNB CSP Switch Solution will endure for a period of 3 (three) years, commencing from the date of installation of the Equipment at Your Premises or the activation of the FNB CSP Switch Solution ("Initial Term"), whichever is applicable at the time.

4.4.2 The relationship between You and the Bank will be governed by the Terms and Conditions.

4.4.3 Upon the expiry of the Initial Term, the agreement between You and the Bank in respect of the FNB PSP Switch Solution or FNB CSP Switch Solution shall proceed on a month to month basis, on the Terms and Conditions of the Merchant Agreement, until terminated by the Merchant in Writing or telephonically, by providing no less than a Calendar Months' notice to the Bank or as provided for herein.

4.4.4 Should the Merchant Agreement be terminated prior to the expiry of the Initial Term, the Bank shall hold the Merchant liable for an early termination fee that will be calculated based on the remaining term of the Initial Period, the deinstallation and deactivation fee incurred by the Bank for the deinstallation of the Equipment or deactivation of the FNB CSP Switch Solution, the Equipment finance costs (for the FNB PSP Switch Solution) and the software licence fee payable in respect of the remaining term.

4.5 **FNB Fuel Solution**

4.5.1 The agreement between You and the Bank in respect of the FNB Fuel Solution will endure for a period of 3 (three) years, commencing from the date of installation of the FNB Fuel Solution equipment at Your Premises ("Initial Term").

4.5.2 The relationship between You and the Bank will be governed by the Terms and Conditions.

4.5.3 Upon the expiry of the Initial Term, the agreement between You and the Bank in respect of the FNB Fuel Solution shall proceed on a month to month basis, on the Terms and Conditions of the Merchant Agreement, until terminated by the Merchant in Writing or telephonically, by providing no less than a Calendar Months' notice to the Bank or as provided for herein.

4.5.4 Should the Merchant Agreement be terminated prior to the expiry of the Initial Term, the Bank shall hold the Merchant liable for an early termination fee that will be calculated based on the remaining term of the Initial Period, the deinstallation fee incurred by the Bank for the deinstallation of the Equipment, the Equipment finance costs and the software licence fee payable in respect of the remaining term.

4.6 **Speedee®**

4.6.1 The agreement between You and the Bank in respect of Speedee® will endure for a period of 1 (one) year, commencing from the date of installation of the Equipment at Your Premises or the activation of Speedee® ("Initial Term"), whichever is first in time.

- 4.6.2 The relationship between You and the Bank will be governed by the Merchant Agreement.
- 4.6.3 Upon the expiry of the Initial Term, the agreement between You and the Bank in respect of Speedee® shall proceed on a month to month basis, on the Terms and Conditions of the Merchant Agreement, until terminated by the Merchant in Writing or telephonically, by providing no less than a Calendar Months' notice to the Bank or as provided for herein.
- 4.6.4 Should the Merchant Agreement be terminated prior to the expiry of the Initial Term, the Bank shall hold the Merchant liable for an early termination fee that will be calculated based on the remaining term of the Initial Period, the installation, deinstallation and deactivation fees incurred by the Bank for the deinstallation of the Equipment or deactivation of Speedee®.

5. CONFLICTING PROVISIONS

- 5.1 In the event of a conflict, the provisions of the Merchant Agreement are to be read in the following order of precedence in relation to that conflict:
- 5.1.1 Master Agreement (if applicable);
- 5.1.2 Product and/or Services-Specific Terms and Conditions;
- 5.1.3 Merchant Services General Terms and Conditions;
- 5.1.4 Statement; and
- 5.1.5 Application form.

6. AMENDMENT TO THE TERMS AND CONDITIONS

- 6.1 The latest version of the Terms and Conditions of the Merchant Agreement is available on the FNB website and replaces all previous Terms and Conditions You have entered into with the Bank in respect of the Acquiring Services.
- 6.2 The Bank may, from time to time during the course of the Merchant Agreement revise and update the Merchant Agreement; discontinue or otherwise modify, temporarily or permanently, the Acquiring Services and/or any part of Your access thereto. The Bank reserves the right to make any such changes effective immediately if necessary to maintain the integrity and security of the Acquiring Services and related systems, and to comply with the Card Scheme Rules, legislation, regulations and industry requirements.
- 6.3 The onus is on You to access the FNB website to view the Merchant Agreement, as well as any amendments made thereto and to contact the Bank in the event of any queries You may have.
- 6.4 Any Material Amendments to the Terms and Conditions will be communicated to You by way of Bank pre-recorded telephone calls; letters, emails; Statement messages; website notices; post or SMS.
- 6.5 If You do not agree with any changes, You can, prior to the expiry of the Cooling Off Period, exercise Your right to terminate the Merchant Agreement by immediately discontinuing the use of the Acquiring Services and products and by notifying the Bank in Writing or by contacting the Merchant Services National Call Centre.
- 6.6 If You do not notify the Bank of Your intention to terminate the Merchant Agreement within the Cooling-Off Period, Your continued use of the Bank's Acquiring Services and products after the expiry of the Cooling-Off Period will serve as confirmation that the Bank has given You adequate opportunity to read and understand the Merchant Agreement and constitutes Your acceptance of the Terms and Conditions of the Merchant Agreement.
- 6.7 Any Transactions processed after the Cooling-Off Period will be governed by the amended Terms and Conditions of the Merchant Agreement.

7. GENERAL PROVISIONS

- 7.1 The Bank is dependent on Third-Party Service Providers for the availability or quality of the Communication Network and/or up-time and in the circumstances cannot accept any responsibility for the Third-Party Service Providers or Communication Networks.
- 7.2 By using the Acquiring Services and Products, You confirm that You shall, throughout the duration of the Merchant Agreement:
- 7.2.1 not conduct unlawful business activities;
- 7.2.2 not violate anti-money laundering laws;
- 7.2.3 ensure that there is due compliance with all the Rules;
- 7.2.4 provide the Bank with Your VAT number;
- 7.2.5 contact the Bank if You be unsure of what is required from You in terms of the Merchant Agreement;
- 7.2.6 honour each Payment Instrument legally presented to You for payment of goods and/or services;

- 7.2.7 not discriminate against any Customer by setting a minimum or maximum Transaction amount as a condition of honouring a Payment Instrument Transaction;
- 7.2.8 ensure that You take due care in accepting Transactions to ensure that no Fraudulent Transactions are concluded and that no Invalid Transactions are accepted. Please visit the VISA and Mastercard website for more information (this provision is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions);
- 7.2.9 ensure that You provide the Customer with a Receipt and that same is legible;
- 7.2.10 ensure that Your Receipt does not differ from the copy given to the Customer;
- 7.2.11 **accept full responsibility for Your actions, as well as the actions of Your employees and Your Third-Party Service Providers at all times;**
- 7.2.12 provide the Bank with any information and documentation that the Bank may require from time to time under the Merchant Agreement, within the timelines communicated to You by the Bank;
- 7.2.13 allow the Bank and the Bank's Third Party Service Providers such access to Your Premises and provide reasonable and necessary support as may be necessary for the Bank to carry out the Bank's obligations under the Merchant Agreement;
- 7.2.14 ensure that an appropriate agreement is in place between You and Your Third Party Service Providers;
- 7.2.15 **safely secure all information and documentation in respect of each Transaction, including the Receipt for a minimum period of 3 (three) years from the date of the Transaction, or as provided for otherwise in terms of applicable legislation, regulation and Card Scheme rules (whichever is the longest); and**
- 7.2.16 provide 10 (ten) Business Days' prior Written notification to the Bank of any changes to the following:
- 7.2.16.1 a change in Your business that may impact the availability and provisioning of the Acquiring Services and products by the Bank;
- 7.2.16.2 a change in the nature of Your business;
- 7.2.16.3 a change of address or contact details; and
- 7.2.16.4 a change of Your banking details.
- 7.3 In the event that You omit to advise the Bank of any changes, the Bank reserves the right to immediately terminate the Merchant Agreement and debit Your Nominated Bank Account or net settle or set off any amounts from Your Nominated Bank Account in respect of the Losses incurred by the Bank in terms of the Merchant Agreement.
- 7.4 By using the Acquiring service and products You understand and agree to the Bank acting on instructions received from Your employees and warrant that Your employees are authorised to instruct the Bank.
- 7.5 If You consist of two or more persons, You will be held jointly and severally liable to the Bank as co-principal debtors for all Losses and obligations arising out of the Merchant Agreement.
- 7.6 **No Party will have any claim or right of action arising from any undertaking, representation, or Warranty not included in the Merchant Agreement.**
- 7.7 Where the Bank gives You extra time to comply with Your obligations, it shall not be construed to mean that the Merchant Agreement has been amended, or that it no longer applies to You.
- 7.8 The Bank may treat a Transaction as valid even if You did not comply with Your obligations as set out in the Merchant Agreement. If the Bank treats a Transaction as valid, You still have a duty to comply with Your obligations for all future Transactions.
- 7.9 The Bank shall not lose any of the Bank's rights under the Merchant Agreement if the Bank does not immediately and in every instance, insist on them. You may not raise it as a defence if the Bank did not enforce its rights at the relevant time.
- 7.10 The Parties shall act as independent contractors for all purposes under this Merchant Agreement. Nothing contained in the Merchant Agreement shall be deemed to constitute either Party as an agent or representative of the other Party, or both Parties as joint venturers or partners for any purpose.
- 7.11 You will not have the authority to speak for, represent or obligate the Bank in any way without the prior Written approval of the Bank.
- 7.12 **You may not, without securing the prior Written consent of the Bank:**
- 7.12.1 **cede any rights in terms of Your Merchant Agreement; or**
- 7.12.2 **delegate any obligations in terms of Your Merchant Agreement.**
- 7.13 The Bank shall be entitled to sub-contract its obligations under this Merchant Agreement to Third Party Service Provider(s) in order to fulfil its obligations in terms of this Merchant Agreement. The Bank has further the right to cede its rights and delegate its obligations in terms of the Master Agreement.

8. DORMANT ACQUIRING FACILITIES

- 8.1** When You do not use the Acquiring Service or product that has been made available to You by the Bank for a period of 3 (three) Months, Your Merchant facility will be regarded as dormant. When Your Merchant facility is dormant, the Bank reserves the right to do the following:
- 8.1.1** suspend the Acquiring Service and products immediately without prior notice;
- 8.1.2** terminate the Merchant Agreement immediately without prior notice and without prejudice to any other rights in law;
- 8.1.3** hold You liable and debit Your Nominated Bank Account, notwithstanding that such account may be held at another bank or apply set-off or net-settle amounts and Losses owing by You to the Bank;
- 8.1.4** place a hold on Your Nominated Bank Account and pledge an amount equal to an estimate of any potential Losses that the Bank may incur as a result of Your default; and
- 8.1.5** the Bank may further rely on any of the remedies available to it by law.

9. PCI DSS

It is important that You familiarise Yourself with and comply with the requirements set out herein.

9.1 PCI DSS Certification

- 9.1.1** PCI DSS provides a baseline of technical and operational requirements that are designed to protect Customer data. PCI DSS applies to all entities involved in payment processing, including Merchants, processors, Acquiring Banks, Issuing Banks, Third Party Service Providers, as well as all other entities that store, process or transmit Customer Data and information. PCI DSS may be enhanced from time to time by additional controls and practices to further mitigate risks. A brief overview of the PCI requirements is set out below. By using the Acquiring Services and products You confirm and agree that You will ensure that:

- 9.1.2** The requirements for PCI DSS compliance vary depending on the number of Transactions You process in a year. Please see below a breakdown of Merchant levels and validation requirements:

Level	Merchant Criteria	Validation Requirements
1	All channels - Merchants processing over 6,000,000 (six million) Transactions annually or a global Merchant identified as Level 1	<ul style="list-style-type: none">▪ ROC by a QSA▪ Quarterly network scan by ASV▪ Attestation of Compliance Form
2	All channels - Merchants processing 1,000,000 (one million) to 6 000 000 (six million) Transactions annually	<ul style="list-style-type: none">▪ Annual SAQ▪ Quarterly network scan by ASV▪ Attestation of Compliance Form
3	eCommerce - Merchants process- ing 20 000 (twenty thousand) to 1 000 000 (one million) eCommerce Transactions annually	<ul style="list-style-type: none">▪ Annual SAQ▪ Quarterly network scan by ASV▪ Attestation of Compliance Form
4	eCommerce - Merchants process- ing less than 20 000 (twenty thou-sand) eCommerce Transactions annually All channels (excluding eCommerce) - Merchants process- ing up to 1 000 000 (one million) Transactions annually	<ul style="list-style-type: none">▪ Adherence and compliance with the Validation Requirements set out below▪ Quarterly network scan by ASV

- 9.1.3** In order to meet the validation requirements, the Merchant shall refer to the PCI Security Standards website. It is the Merchant's obligation to ensure compliance with the PCI Rules and the Merchant shall (including but not limited to):

- 9.1.3.1** build and maintain a secure network in accordance with PCI Rules;
- 9.1.3.2** protect Cardholder Data;
- 9.1.3.3** maintain a Vulnerability Management Program;
- 9.1.3.4** implement strong access control measures in accordance with PCI Rules;
- 9.1.3.5** regularly monitor and test networks; and
- 9.1.3.6** maintain an information security policy.
- 9.1.3.7** all Your employees are appropriately trained to process Transactions securely and that You will ask the Bank to conduct training for You and Your employees on PCI DSS as and when required;
- 9.1.3.8** Customer Data (expiry date, PIN Number, Track 2, 3-digit CVV) is destroyed after every Transaction and not stored electronically otherwise;
- 9.1.3.9** the Card number is masked on the Customer receipt. The minimum requirements for masking are that the first 6 and last 4 digits be displayed, and the middle digits be masked. The Bank will ensure that

the PAN is masked on all Stand Alone Devices. **You should notify the Bank immediately when You notice that the PAN is not masked;**

- 9.1.3.10 all paper-based documentation containing full, unmasked Card numbers shall be marked confidential, stored securely and destroyed in accordance with the PCI DSS requirements;
- 9.1.3.11 Your authorised employees and Third Party Service Providers do not have access to the supervisor cards or supervisor PIN other than for the purpose of processing Transactions;
- 9.1.3.12 You monitor the compliance status of Your Third Party Service Providers with which You share Customer Data and information and You must maintain Written agreements with all Third Party Service Providers whereby they acknowledge their responsibility for Data in their possession;
- 9.1.4 PCI DSS Validation Requirements: Levels 1-3
- 9.1.4.1 **In addition to the information set-out herein, You must adhere to the requirements set-out on the PCI Security Standards Council's website.**
- 9.1.4.2 **You obtain and keep a current and valid PCI DSS certificate in accordance with the applicable PCI standards in effect at the time and comply with all the requirements set out by the PCI DSS.** You must provide a copy of such certificate to the Bank within the period specified by the Bank, alternatively You must furnish the Bank with written proof of Your application for such certificate. The Bank will determine whether such proof is adequate in the Bank's sole discretion.
- 9.1.4.3 You furnish the Bank annually and as requested from time to time, with proof of Your PCI DSS compliance certificate and any data records pertaining to the implementation and monitoring of PCI DSS compliance, including but not limited to any Data and information related to a potential or actual occurrence of a Data Compromise;
- 9.1.5 PCI DSS Validation Requirements: Level 4
- 9.1.5.1 By entering into a Merchant Agreement with the Bank, You are automatically enrolled into the PCI DSS Program in terms of which the Bank will provide you with continuous awareness training on PCI level 4 validation requirements. Kindly ensure that the requirements are implemented within your business and that You instil a culture of a secure environment when processing Payment Instruments.
- 9.1.6 Requirements for storing card data

	Data Element	Secure Storage permitted	Storage of data
Customer Data	PAN	Yes	If PAN is stored with other elements of Customer Data, please ensure that the PAN is masked.
	Customer name	Yes	
	Service code	Yes	
	Expiration date	Yes	
Sensitive authentication Data	Full magnetic stripe data	No	Sensitive authentication Data may not be stored.
	CAV2/CVC2/CVV2/CID	No	
	PIN	No	

- 9.2 Failure by You to comply with the above may, without prejudice to the Bank's rights hereunder or in law, result in:
- 9.2.1 the Bank suspending the Acquiring Services pending receipt of Your PCI DSS certificate;
- 9.2.2 the Bank terminating the Merchant Agreement forthwith;
- 9.2.3 You bearing liability for your PCI obligations and compliance as set out in the Rules; and
- 9.2.4 Your Nominated Bank Account being debited or set-off or net-settlement being applied in respect of all Losses and penalties incurred by the Bank as a result of Your non-compliance.
- 9.3 It is Your responsibility to ensure that You remain PCI DSS compliant at all times.
- 9.4 **The costs of becoming and remaining PCI compliant shall be borne by You.**
- 9.5 Please contact the Merchant Services National Call Centre for further details regarding to Your PCI status

10. CARD SCHEME RULES AND INDUSTRY REQUIREMENTS

By using the Bank's Acquiring Services, You acknowledge that You are aware that the Card Schemes publish and make available updated rules (including regulations, bulletins, alerts and directives from

time to time) and the Bank may communicate industry requirements to You for Your attention and compliance. It is Your responsibility to review the Rules and You agree to be bound by the Rules that are applicable to You.

- 11. DINERS, AMEX, UPI AND RCS CARDS FACILITY (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)**
 - 11.1 Separate agreements must be entered into with Diners' Club, American Express, UPI and RCS ("Card Schemes") as they are not covered by the Merchant Agreement. You may not use the Equipment and/or Acquiring Services and products to process Transactions on Diners, Amex, UPI and RCS Cards prior to entering into a separate agreement with the respective Card Schemes, failing which, You will be held liable for all Chargebacks received and Losses incurred by the Bank as a result thereof.**
 - 11.2 Upon receipt of approval from the respective Card Schemes, You may accept all valid and current Diners, Amex, UPI and RCS Cards as a form of payment, provided that You inform the Bank of Your agreement with the respective Card Schemes.
 - 11.3 The relevant Card Scheme rules must be read in conjunction with the Terms and Conditions. By accepting Diners, Amex, UPI or RCS Cards You agree to be bound by the Terms and Conditions of Your Merchant Agreement, as well as the relevant Card Scheme rules. Non-compliance may result in the withdrawal of the respective Amex, Diners, UPI or RCS Cards facilities by the Bank.
 - 11.4 You must obtain the Bank's prior Authorisation for all Transactions. In the event that You are unable to obtain Authorisation for a Diners, Amex, UPI or RCS Card Transaction, You may not accept any of these Cards as a form of payment. For the avoidance of doubt, it is recorded that in the event of a Speedpoint® Device malfunction, You will be unable to obtain Authorisation for Diners, Amex, UPI and RCS Card Transactions and You will consequently be unable to process Diners, Amex, UPI and RCS Cards Transactions.
 - 11.5 The termination of Your Diners, Amex, UPI and/or RCS Card facility will also be dependent on the termination of Your facility with the respective Card Schemes. You are required to inform the Bank in the event that you terminate any of the facilities as aforesaid. The Bank will not be held liable for any Transactions that are not processed as a result of the withdrawal of the service by the respective Card Schemes.
 - 11.6 If You accept a Diners/Amex/UPI/RCS Payment Instrument, You provide the Bank with explicit permission to send Your contact details to the respective card schemes in order for them to contact You to enter into an agreement for the acceptance of Payment Instruments.**
- 12. UPI CARDS (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)**

Where You are unable to obtain Authorisation for UPI Transactions as a result of a Speedpoint® Device malfunction, a decline message or any other reason, You may not obtain voice Authorisation to process the Transaction.
- 13. PRE-AUTHORISATION OF TRANSACTIONS**
 - 13.1 When processing Pre-Authorised Transactions, You must ensure that:
 - 13.1.1 all Pre-Authorisation Transactions are finalised by either cancelling, completing or reversing same within 30 (thirty) Calendar Days of the date of the original Pre-Authorisation Transaction:-
 - 13.1.1.1 by selecting one of the menu options on the Speedpoint® Device i.e. "Pre-Auth Cancel" or "Pre-Auth Complete"; and
 - 13.1.1.2 on the same Speedpoint® Device that was initially used to process the Pre-Authorisation Transaction **or** by contacting the originator of the Pre-Authorisation Transaction to perform a cancellation, completion or reversal of the original Pre-Authorisation Transaction;
 - 13.1.2 You may only process a further Transaction for a Customer, after either cancelling, completing or reversing the original Pre-Authorisation Transaction:-
 - 13.1.2.1 where the amount due by the Customer to You is less than the Pre-Authorisation amount, You must cancel the Pre-Authorisation Transaction and, if applicable, process a separate Transaction for the lesser amount due to You;
 - 13.1.2.2 where the amount due by the Customer to You exceeds the Pre-Authorisation amount, You must complete the Pre-Authorisation Transaction and process a separate Transaction for the balance of the amount due to You;
 - 13.1.2.3 the final Transaction that is processed by You must always be equal to the Pre-Authorisation amount;

- 13.1.3 the invoice issued by You to the Customer for the Transaction must reflect an amount equal to the Pre-Authorisation Transaction;
- 13.1.4 Should the Pre-Authorisation Transaction not be completed by either cancelling, completing or reversing same within 30 (thirty) Calendar Days, the Pre-Authorisation may be regarded as invalid.
- 13.1.5 Your non-compliance with the above requirements will result fines or penalties levied by PASA or the Card Association, which fines or penalties will be debited from Your Nominated Bank Account.

14. AUTHORISATION OF TRANSACTIONS

14.1 When the Bank provides Authorisation for a Transaction it simply means that the Customer has sufficient funds in his or her bank account to pay for the Authorised Transaction at the time and date of the Authorisation.

14.2 You must ensure that Authorisation is obtained from the Bank for each respective Transaction undertaken by You in accordance with the Merchant Agreement.

14.3 You may only request Authorisation at the time of processing a Transaction.

14.4 Authorisations are only valid for specific Transactions and amounts.

14.5 You may not split or disguise Transactions or act in a way to avoid obtaining Authorisation from the Bank.

14.6 You must contact the Bank to cancel the Authorisation if You do not proceed with the Transaction.

14.7 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.

14.8 The Bank does not have to provide You with reasons for declining a request for Authorisation.

14.9 Obtaining voice Authorisation from the Bank and/or receiving an Authorisation code from the Bank is merely a confirmation that there are sufficient funds available in the Customer's bank account and does not mean that the Bank warrants or guarantees:

14.9.1 that a Transaction is not a Fraudulent Transaction;

14.9.2 the validity or genuineness of the Transaction;

14.9.3 the validity of the identity of the Customer presenting the Payment Instrument;

14.9.4 that the Bank will pay the value of the Authorised Transaction;

14.9.5 that the intended Transaction will not be declined later; or

14.9.6 that the Transaction will not be subject to a Chargeback.

14.10 Obtaining an Authorisation code does not exempt You from the duty to prevent Fraudulent Transactions.

14.11 Brute Force Attacks

14.11.1 Common Attacks:

14.11.1.1 The use of Bot Army – Scripted Attacks to directly target a Merchant's website checkout page for rapidly conduct multiple and successive test Transactions;

14.11.1.2 Merchant Account takeovers through exploiting vulnerabilities, by:

14.11.1.2.1 compromising Merchant credentials through social engineering or credential cracking;

14.11.1.2.2 using aggressive Phishing Attacks via Malware through infected emails;

14.11.1.2.3 creating fictitious Merchant names with valid Merchant identification numbers.

14.11.2 Indicators of Brute Force Attacks:

14.11.2.1 Brute Force Attacks have the following distinctive characteristics:

14.11.2.1.1 The test of a Merchant Account number and/or Card commonly begins with a nil or small Rand value Transaction, and in some instances is followed by a larger Rand value test Transactions in quick succession;

14.11.2.1.2 The Merchant category code (MCC) used in the test Transaction often does not match the Merchant's primary business

14.11.3 Merchants should ensure that they implement the following measures:

14.11.3.1 use widely available tools, such as CVC 2 validation, 3D-Secure, real-time Authorisation, monitoring, and Captcha to limit the scope of Bot Army-Scripted Attacks;

14.11.3.2 deploy technology, such as web application firewalls, to detect and mitigate the effect of bot attacks and

14.11.3.3 generally requiring Cardholders to create complex passwords; limiting the number of times a Cardholder can unsuccessfully attempt to log in and temporarily locking out Customers who exceed the specified maximum number of failed login attempts

14.11.4 For Card Not Present Transactions, Mastercard prohibits subsequent Authorisation requests where an original Authorisation response includes any of the declined responses listed below:

14.11.4.1 "04" (Capture Card);

14.11.4.2 "14" (Invalid Card Number);

- 14.11.4.3 "15" (Invalid Issuer);
- 14.11.4.4 "41" (Lost Card);
- 14.11.4.5 "43" (Stolen Card);
- 14.11.4.6 "54" (Expired Card).
- 14.11.5 A Merchant receiving any of the above-mentioned codes may request the Customer to present a different account (to pay from), but may not re-present the same account.
- 14.12 **Undesirable Transaction Processing Behaviour, including but not limited to Excessive Authorisation Attempts and Nominal Amount Authorisations will be subject to assessment and if determined to exceed the Card Association's threshold, will result in fines or penalties levied by the Card Association which fines or penalties will be debited from Your Nominated Bank Account.**
- 15 **FRAUDULENT TRANSACTIONS**
- 15.1 The onus is on You to implement Fraud prevention measures and to establish processes and controls aimed at combating, preventing and detecting Fraud when processing Transactions and to ensure that You are adequately protected against Fraudulent activities. You are required to report any Fraudulent Transactions by contacting the Merchant Services Call Centre by telephone on 22241061.
- 15.2 Fraud prevention training materials, which include Fraud prevention videos and brochures, are now available on the FNB website. It is Your responsibility to view the Fraud prevention training materials on the FNB website and to ensure that Your employees also view such material. Should You or Your employees require further training after viewing the Fraud prevention training, You may contact the Fraud Helpdesk on 22241061 for further assistance.
- 15.3 By entering into this Merchant Agreement, You undertake to co-operate with the Bank in furnishing all information and documentation requested by the Bank to enable the Bank to investigate Fraudulent Transactions.
- 15.4 You must not honour Transactions and/or accept cards that You know or suspect are Fraudulent Transactions, Fraudulent cards or Transactions that are not authorised by the Customer.
- 15.5 If You are suspicious of a Payment Instrument or Customer at any time during the Authorisation process, You are required to make a Code 10 authorisation request. The Code 10 authorisation request alerts the Card Issuer to the suspicious activity.
- 15.6 **You shall immediately inform the Bank, by contacting the Bank's helpdesk on 22241061, of a Fraudulent Transaction, or a suspected Fraudulent Transaction, or of any suspicious activity of a Customer.**
- 15.7 If a Fraudulent Transaction or a suspected Fraudulent Transaction occurs, or if the Bank suspects the Transaction is for any reason suspicious, an Invalid Transaction, erroneous or illegal; the Bank is irrevocably authorised to:
 - 15.7.1 withhold or delay settlement of the Transaction;
 - 15.7.2 recover from You by debiting Your Nominated Bank Account, notwithstanding that such account may be held at another bank, or applying set-off or net settle amounts due to You with the value of any Fraudulent Transactions and Losses that the Bank incurred or suffered, as a result of or in connection with any Fraudulent Transaction; Invalid Transaction; erroneous or illegal Transactions processed by You. You indemnify the Bank in respect of all Losses in this regard;
 - 15.7.3 place a hold on Your Nominated Bank Account;
 - 15.7.4 pledge an amount equal to an estimate of any potential Losses that the Bank may incur as a result of the Fraudulent Transactions, Invalid Transactions and suspicious Transactions;
 - 15.7.5 suspend the Acquiring Service and products; or
 - 15.7.6 terminate the Merchant Agreement immediately without prior notice and without prejudice to any other rights in law.
- 16 **CHARGEBACKS (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)**
- 16.1 **Transactions may be reversed through a process called Chargeback for any reason specified in the Card Scheme rules. According to the Card Scheme rules, You are not allowed to dispute any Chargebacks which relate to Manual Entry Transactions processed on a MasterCard. You therefore accept full risk and liability for all these Transactions.**
- 16.2 Chargebacks will be dealt with in accordance with the Card Scheme rules.
- 16.3 The onus is on You to provide the Bank with the information and documentation (including Receipts) that the Bank may require from time to time under the Merchant Agreement, within the timelines

communicated to You by the Bank.

16.4 Reasons for Chargebacks include, but are not limited to the following:

16.4.1 Transactions that are subject to a Customer dispute (i.e. if the goods or services were not received and/or failed to meet the required standard etc);

16.4.2 Goods or services received by the Customer, or a person authorised by the Customer are not as depicted on the Receipt or vary from the marketing specifications supplied, including but not limited to items of wrong colour, size, quality or quantity;

16.4.3 goods were broken or destroyed and could not be used for the purpose for which it was purchased as a result thereof;

16.4.4 the Transaction was not Authorised;

16.4.5 the Transaction is a Fraudulent Transaction, an Invalid Transaction, erroneous and/or illegal; and

16.4.6 the Transaction has not been processed in accordance with the provisions of the Rules.

17 AGGREGATION (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)

You may not be involved in Aggregation without obtaining the Bank's prior Written approval.

18 SURCHARGING (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)

18.1 A surcharge is where You "penalise" a Customer for using a credit Card and/or Debit Card for a purchase Transaction. The practice of surcharging is thus where You charge Customers more for the goods and/or services than You would normally charge Customers when they pay for the goods and/or services in cash. The amount charged to all Customers must match the displayed or advertised price.

18.2 The practice of levying surcharges is clearly prohibited by the Card Scheme rules and industry requirements.

19 FLOOR LIMIT

19.1 A zero Floor Limit applies to all Transactions.

19.2 The Bank has the right to change the Floor Limit at the Bank's own discretion.

20 BIN FILES AND HOT CARD FILES

You must ensure that all BIN files and Hot Card files are successfully downloaded onto Your Speedpoint® Device. If the Speedpoint® Device identifies a particular card as being present on a current Hot Card file, You may not under any circumstances attempt to process a Transaction on such card, as You will be held liable for the Transaction.

21 DISPUTES BETWEEN YOU AND YOUR THIRD PARTY SERVICE PROVIDERS

Notwithstanding that the Bank may have introduced You to a Third Party Service Provider, the Bank shall not be a party to any disputes raised between You and Your Third Party Service Providers, nor shall the Bank be liable for any Losses suffered by You as a result of any failure or malfunction of such infrastructure between You and Your Third Party Service Provider or as a result of an action or omission of the Third Party Service Provider. You have to contact Your Third Party Service Provider directly in respect of any disputes between You and Your Third Party Service Provider.

22 DISPUTES RAISED BY YOUR CUSTOMER

22.1 If a Customer lodges a complaint about any Transaction which is considered to be reasonable or returns Goods purchased on reasonable grounds, You may not refuse to exchange or process a Refund for such Transaction.

22.2 You shall, at Your own cost and expense, satisfy all claims and complaints arising in connection with any Transaction and cause any such claim or complaint that is justified to be satisfied without any undue delay.

22.3 You must provide the Bank with information and documentation required within the timelines communicated by the Bank in order for the Bank to resolve a dispute which has been raised by Your Customer with the Bank. You will be bound by the settlements negotiated between the Bank and the Customer and any defences that the Bank raise against the Customer.

23 REPUTATION

You, Your employees, agents, representatives and Third Party Service Providers shall not do anything, or engage in any activity, which is likely to adversely affect or damage the Bank's name and reputation.

24 DISPLAYING OF SYMBOLS (This clause is not applicable to the acceptance of Fleet Cards and the processing of Fleet Card Transactions)

24.1 You shall display the marks and symbols of the Card Schemes as required in terms of the Card Scheme rules.

24.2 You may not in any way whatsoever state, imply or create the impression that the Bank, or any Card Scheme endorses or guarantees any of Your goods and/or services.

25 USE OF BANK MARKS

25.1 You shall not use the Bank's names, trademarks or trade names, whether registered or not, in publicity releases, advertising or in any other manner, without having secured the prior Written approval of the Bank.

25.2 Where the Bank has provided You with Written approval as contemplated above, You shall in no way represent, except as specifically permitted by the Bank, that You have any right, title or interest in or to the Bank's names, trademarks or trade names, whether registered or not, or in and to any other Intellectual Property rights of the Bank.

25.3 You must ensure that You use the Bank's names, trademarks or trade names, whether registered or not, strictly in accordance with the criteria provided by the Bank.

25.4 Upon termination of the Merchant Agreement or earlier if required by the Bank, You will:

25.4.1 immediately cease all use whatsoever of the Bank's names, trademarks or trade names, whether registered or not, and other Intellectual Property rights of the Bank; and

25.4.2 deliver to the Bank and/or destroy all materials in Your possession or control that bear the Bank's names, trademarks or trade names, whether registered or not, and other Intellectual Property rights of the Bank and confirm in Writing to the Bank that You have done so.

26 SECURITY ASSESSMENT

26.1 By using the Acquiring Services and products You confirm that the Bank may conduct a Security Assessment, and You agree to provide the Bank and/or an independent accredited Third Party Service Provider or auditor appointed by the Bank access to conduct a physical inspection of Your Premises and a Security Assessment of Your Communication Network, records, documentation and systems pertaining to the Merchant Agreement, in order to establish whether it is compliant with the Rules.

26.2 You agree to cooperate with the Bank's Security Assessment requirements and provide reasonable assistance as required by the Bank.

26.3 You must take all reasonable steps to ensure that the security and integrity of Your Communication Network is not compromised;

26.4 You must ensure that Your Communication Network is at all times compliant with applicable law. This shall include implementation of enhancements to the Communication Network on a continuous basis and as and when the applicable law changes.

26.5 You must ensure that Your Third Party Service Providers do not implement any enhancements to Your Communication Network, which could have an impact on the Bank network or the Acquiring Services (save for any which are necessary and/or emergency and/or for maintenance), during the following periods:

26.5.1 peak periods;

26.5.2 the Bank's financial year-end;

26.5.3 the Easter weekend;

26.5.4 the year-end freeze;

26.5.5 month-end, being the period commencing 7 (seven) days prior to the last day of the month and ending 3 (three) days after the last month; and

26.5.6 during any other periods of major system conversions being undertaken where the Bank has notified the TSP in writing (including electronic mail) prior to the conversion.

26.6 You hereby indemnify and hold the Bank harmless against all Losses and actions of whatsoever nature arising from Your non-compliance with Rules or Your failure to ensure the integrity and security of Your Communication Network.

26.7 Any such Security Assessment shall not unreasonably interfere with Your normal business operations.

26.8 In the event that the Security Assessment determines that You are not compliant:

26.8.1 You will be held liable for the cost of the Security Assessment;

- 26.8.2 You will be held liable for all Losses incurred by the Bank as a result of Your non-compliance;
- 26.8.3 the Bank will have the right to terminate the Merchant Agreement with immediate effect;
- 26.8.4 the Bank may further rely on any of the remedies available to it by law.
- 26.9 In the event of any confirmed or suspected Data Compromise, You warrant You shall:**
- 26.9.1 contact the Bank immediately in Writing, by emailing [msdatacompromises\(at\)fnb.co.za](mailto:msdatacompromises(at)fnb.co.za), to report any suspected or confirmed Data Compromise**
- 26.9.2 request guidance from the Bank on the procedure and timelines for reporting the confirmed or suspected Data Compromise to the relevant authorities and Card Schemes.**
- 26.9.3 report the confirmed or suspected Data Compromise to the relevant authorities and Card Schemes as directed by the Bank. Reporting on confirmed or suspected Data Compromises is mandatory and You must ensure that the procedure and timelines communicated by the Bank are adhered to, failing which, You will be liable for any fines and/or penalties that may arise as a result.**
- 26.9.4 contact Your PSP and/or CSP to report the confirmed or suspected Data Compromise.**
- 26.9.5 preserve evidence to identify the root cause and facilitate investigations. It is important to ensure the integrity of Your system components and environment by preserving all evidence. The following steps serve as a guideline on the execution of this obligation:**
- 26.9.5.1 You shall not access or alter the compromised system (e.g. do not log on to the compromised systems and change passwords; do not log in with administrative credentials, etc.). It is recommended that the compromised systems be taken offline immediately and must not be used to process payments or interface and/or integrate with any payment processing systems;**
- 26.9.5.2 You shall not turn off, restart, or reboot the compromised systems. Instead, isolate the compromised systems from the rest of the Communication Network by unplugging the network cable(s) or through any other means;**
- 26.9.5.3 You shall identify and document all confirmed or suspected compromised components (e.g. Equipment, PSP and/or CSP Networks, networks, logs, security events, databases, etc.);**
- 26.9.5.4 You shall document containment and remediation actions taken, including dates/times, individuals involved, and detailed actions performed;**
- 26.9.5.5 You shall preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).**
- 26.10 Within three (3) business days of a suspected or confirmed Data Compromise, You shall provide the Bank with a completed initial investigation report. A copy of the required initial investigation report can be obtained from the Bank.**
- 26.11 You shall appoint a Card Scheme accredited PFI at Your own costs, to conduct a full forensic investigation within the timelines provided by the Bank and/or the Card Schemes. A list of approved PFI organizations is available on the PCI website or may be accessed at: [www\(dot\)pcisecuritystandards\(dot\)org/assessors_and_solutions/pci_forensic_investigators](http://www(dot)pcisecuritystandards(dot)org/assessors_and_solutions/pci_forensic_investigators).**
- 27 MERCHANTS PLACED UNDER BUSINESS RESCUE**
- 27.1** In the event that You are placed under Business Rescue, the Bank reserves the right to retain 100% (one hundred percent) of the gross settlement value as a reserve for potential Losses that the Bank may suffer ("the Retained Amount") should You, for any reason whatsoever, not be in a position to fulfil Your obligations as set out in the Merchant Agreement. The Bank may request additional documentation and information from You in relation to legislative and regulatory requirements.
- 27.2** The Retained Amount will be retained by the Bank for a period of 6 (six) Months after which, in the event that the Bank has not incurred any Losses, the Retained Amount will be released into Your Nominated Bank Account. The Retained Amount will be released on a rolling 6 (six) Month basis. For the avoidance of doubt, the recovery of any and all Losses suffered by the Bank will not be limited to the value of the Retained Amount and You hereby indemnify the Bank against any and all Losses which the Bank may incur subsequent to releasing the Retained Amount into Your Nominated Bank Account.
- 27.3** The rights granted to the Bank in this clause shall survive the termination of this Merchant Agreement for any reason whatsoever.
- 28 MLPCA**
- The use of the Bank's Acquiring Services is subject to You providing the Bank with updated documentation and/or information required to satisfy the "Know Your Client" regulations ("KYC") as amended from time to time including, amongst others, MLPCA and legislation against terrorism, money-laundering, local and international sanctions and related provisions.

29 CONFIDENTIAL INFORMATION

- 29.1 You acknowledge that all Data, material and information provided to You by the Bank, or which You have or which will come into Your possession or become known, or to which You may be exposed during the course of the Merchant Agreement, shall constitute confidential and proprietary information, and where applicable, Intellectual Property belonging to the Bank.
- 29.2 By using the Acquiring Services or products You agree to hold such material and information in confidence and not to make use thereof other than for the performance of this Merchant Agreement; to release it only to employees reasonably requiring such information in the execution of their duties in terms of this Merchant Agreement; and not to release or disclose it to any other person, unless so required by law.
- 29.3 Confidential and proprietary information will not include any information which:
- 29.3.1 at the time of disclosure, is generally known by the public without breaching the provisions of this Merchant Agreement; or
- 29.3.2 is known to be or is lawfully in Your possession before it is received from the Bank (save where it was previously received by You under an obligation of confidence).
- 29.4 The confidentiality obligations under the Merchant Agreement shall survive the termination of the Merchant Agreement for any reason whatsoever.**

30 CONSENT TO DISCLOSE INFORMATION (THE PROTECTION OF PERSONAL INFORMATION ACT, 2013)

- 30.1 By using the Bank's Acquiring Services, You hereby consent that the FNBL may process (collect, use, update, make available, destroy, store, or otherwise deal with and conduct the necessary checks) Your personal information (including processing such information outside the borders of South Africa) for the purposes of providing services and products to You, in accordance with any of the terms and conditions for products and services provided by the FNBL and the requirements of the law. You also confirm that the information provided by You, from time to time, to the FNBL is up to date, correct and complete, including information about Your residency and citizenship for tax purposes and that You will immediately inform the FNBL if this information changes.
- 30.2 Information includes amongst others, information regarding marital status, national origin, age, language, birth, education, financial history, identifying number, e-mail address, physical address, telephone number, online identifier, social medial profile, biometric information (like fingerprints, Your signature or voice) and Your name.
- 30.3 You confirm that the FNBL may process any information and documentation relating to Your business or that of Your employees, directors and members in relation to the services provided by the FNBL.
- 30.4 You agree that the FNBL can access any information about You that is recorded with any credit bureau, or held by any other division of the FNBL, or obtain Fraud reports and checks at any time during the course of Your relationship with the FNBL. The credit bureau provides credit profiles on persons as well as a credit score on the credit-worthiness of persons.
- 30.5 FNB Merchant Services shall give You at least 20 (twenty) Business Days' notice of its intention to submit adverse information (relating to the non-compliance with the agreements You entered into with the Bank) concerning You to TransUnion and Experian (credit bureau);
- 30.6 How FNBL will use Your information:
- 30.6.1 the FNBL will process personal information from You directly; and from Your usage of FNBL's products and services; from Your engagements and interactions with FNBL; from public sources and from third parties; and
- 30.6.2 Your personal information will be confidential and will only be processed if: You consented thereto; it is necessary to conclude or perform in terms of a contract with You; the law requires it or Your FNBL's or a third parties lawful interest is being protected or pursued.
- 30.7 By applying for a bank service or by using a bank service You confirm that FSR may process Your personal information for the following reasons (amongst others):
- 30.7.1 to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules), voluntary and involuntary codes of conduct and industry agreements or to fulfil reporting requirements and information requests;
- 30.7.2 to detect, prevent and report theft, fraud, money laundering and other crimes;
- 30.7.3 to enforce and collect on any agreement when You are in default or breach of the agreement's terms and conditions, like tracing You or to institute legal proceedings against You;
- 30.7.4 to conduct market and behavioural research, including scoring and analysis to determine if You qualify

- for products and services;
- 30.7.5 to develop, test and improve products and services;
- 30.7.6 for historical, statistical and research purposes;
- 30.7.7 to process Payment Instruments and payment instructions;
- 30.7.8 to create, manufacture and print Payment Instruments and payment devices (like a Debit Card);
- 30.7.9 to do affordability assessments, credit assessments and credit scoring;
- 30.7.10 to manage and maintain Your accounts or relationship with the FNBL;
- 30.7.11 to disclose and obtain information from credit bureaus regarding Your credit history;
- 30.7.12 to enable You to participate in the debt review process under the Credit Reporting Act, 2011.;
- 30.7.13 to enable the FNBL to deliver goods or documents or notices to You;
- 30.7.14 for security purposes, identity verification and to check the accuracy of Your personal information;
- 30.7.15 to communicate with You and carry out Your instructions and requests; and
- 30.7.16 for Customer satisfaction surveys, promotional and other competitions.
- 30.8 The FNBL may share Your personal information with the following persons (amongst others) who have an obligation to keep Your information secure and confidential:
 - 30.8.1 attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements;
 - 30.8.2 debt counsellors, payment distribution agents and other persons that assist with the debt review process under the Credit Reporting Act, 2011;
 - 30.8.3 payment processing service providers, banks and other persons that assists with the processing of Your payment instructions;
 - 30.8.4 insurers, brokers and other financial institutions that assist with providing insurance and assurance;
 - 30.8.5 law enforcement and Fraud prevention agencies and other persons tasked with the prevention and prosecution of crime;
 - 30.8.6 regulatory authorities, government departments, local and international tax authorities and other persons in terms of the law;
 - 30.8.7 credit bureaus;
 - 30.8.8 the FSR's service providers, agents and sub-contractors like couriers and other persons the FSR uses to offer and provide products and services to You; and
 - 30.8.9 persons to whom the FSR cedes their rights or delegates their obligations under agreements.
- 30.9 The FSR can process Your personal information outside of the borders of South Africa, according to the safeguards and requirements of the law.
- 30.10 The FSR may process Your personal information using automated means (without human intervention in the decision-making process) to make a decision about You or Your application for any product or service. You may query the outcome.
- 30.11 You have the right to access the personal information the FNBL has about You by contacting DLFNABLESOTHOSSD@fnb.co.za or 22241061.
- 30.12 You have the right to request the FSR to correct or delete the personal information the FSR has about You if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or no longer authorised to be kept.
- 30.13 You have the right to withdraw Your consent which allow the FNBL to process Your personal information.
- 30.14 You have the right to file a complaint with the FNBL about an alleged contravention of the protection of Your information at DLFNABLESOTHOSSD@fnb.co.za
- 30.15 Please refer to the FSR's Privacy Policy located on the FNB website for more information on the FNBL's privacy practices.

31 DATA PROTECTION

31.1 By receiving Data pertaining to or from a Customer, You shall:

- 31.1.1 **treat such Data as confidential and not use it other than as strictly necessary in terms of the Merchant Agreement;**
- 31.1.2 disclose such Data only to parties involved in the Transaction, only as is necessary to give effect to the Transaction;
- 31.1.3 keep all systems and media containing Data, whether physical or electronic, in a secure manner, to prevent access by or disclosure to anyone other than Your authorised employees or the Bank;
- 31.1.4 destroy all such Data that is no longer necessary or appropriate to store in a manner that will render the Data unreadable; and

- 31.1.5 at all times be liable for any Losses resulting from any misuse of Data by You, Your employees and Your Third Party Service Providers; including any failure to keep Data secure and any Data Compromise.
- 31.2 The Data protection obligations under this Merchant Agreement shall survive the termination of this Merchant Agreement for any reason whatsoever.

32 REAL TIME SCREENING

- 32.1 The Bank endeavours to stop or prevent any criminal activities including money laundering, corruption and terrorist financing. In the light of the above the FNBL can do any of the following if it considers it necessary, or if Lesotho or international laws, rules, regulations, restrictions and policies ('the rules') require it to do so:
- 32.1.1 verify (check and confirm) at the commencement of the business relationship with the FNBL and as often as may be necessary or as requirement by the Rules, the identity of any customer and entity as well as that of any persons related to or acting on behalf of or involved with such customers or entities. This includes, but is not limited to, mandated persons, directors, signatories, shareholders and related entities;
- 32.1.2 refuse to conduct business with any person or entity that it considers undesirable or if such a person appears on any sanction list as prescribed by legislation or used by the FNBL in the management of the FNBL's risk, or that is linked to any person who appears on such sanction list, or if such person is linked to any restricted countries or the government agencies of such restricted countries as determined from time to time;
- 32.1.3 terminate its relationship with a customer at any time during the term of the relationship;
- 32.1.4 monitor any Transactions and instructions;
- 32.1.5 request further information before the FNBL acts on any instruction or processes the Transaction. This may result in a delay by the FNBL in carrying out the instruction or in processing the Transaction;
- 32.1.6 refuse to carry out any instruction or Transaction;
- 32.1.7 place a hold on any account or facility;
- 32.1.8 request You to assist the Bank to comply with the Rules by providing FNBL with all the required documents; and
- 32.1.9 despite the real time screening measures set out above, the FNBL will not be responsible for any Losses suffered by You as a result of Your failure to comply with the above requirements.

33 INDEMNITY

- 33.1 **By using the Acquiring Services, You agree to indemnify the Bank, its owners, directors, employees, suppliers, agents and representatives fully from any Losses and penalties that are suffered by or imposed on You, the Bank and any other person due to:**
- 33.1.1 **You, Your employees' or Your Third-Party Service Providers' actions, omissions or non-compliance with the Rules;**
- 33.1.2 **Your PCI DSS and 3D-Secure non-compliance;**
- 33.1.3 **You not taking the required steps to safeguard the Equipment; software; secure access codes and associated information and/or follow the steps recommended by the Bank from time to time, including performing software or hardware updates;**
- 33.1.4 **any dispute between You and the Customer about any goods or services which You supplied or delivered to the Customer;**
- 33.1.5 **any dispute between You and Your Third Party Service Provider about any goods or services which You supplied or delivered to the Customer;**
- 33.1.6 **a breach of security or a Data Compromise occurring as a result of:**
- 33.1.6.1 **an action or omission of You and/or Your Third Party Services Provider, which may result in Loss and/or damage in respect of the Intellectual Property of a third party;**
- 33.1.6.2 **Data being stored on Your PSP's or CSP's Network (this provision excludes data being stored on the FNB CSP Network);**
- 33.1.6.3 **Data being transmitted from Your PSP's or CSP's Network to the Bank's Network; and/or**
- 33.1.6.4 **Data being received by Your PSP's or CSP's Network from the Bank's Network.**
- 33.2 In the event of a breach, the indemnities provided in the Merchant Agreement the default clause shall apply, without prejudice to any other remedies available in law.

34 WARRANTY

- 34.1 **You warrant that when You present a Transaction to the Bank for payment:**

- 34.1.1 all information and statements of fact in the record of that Transaction are true and correct;
- 34.1.2 You charged the Customer Your normal cash price for all goods or services (whichever is applicable);
- 34.1.3 the Transaction is not illegal or a Fraudulent Transaction;
- 34.1.4 You complied with all the Rules;
- 34.1.5 You supplied all the goods and/or services referred to in the Transactions to the Customer, at the agreed location and within the agreed time period and that You retained proof of the delivery of goods or services; and
- 34.1.6 the information sent by You or Your Third Party Service Provider is secured at all times in accordance with the Rules.
- 34.2 If the warranty provisions provided in the Merchant Agreement the default clause shall apply, without any prejudice to any other remedies available in law.
- 35 POSTING OF RECEIPTS**
- The Bank will endeavour to credit Your Nominated Bank Account with the total value of all banked Transactions and all valid Receipts received from You within 2 (two) Business Days from the date of receipt of the Transaction, subject to the necessary verification and Fraud checks been conducted by the Bank.
- 36 SETTLEMENT**
- 36.1 Immediate settlement may not take place, except if otherwise agreed to by the Bank in Writing. Should immediate settlement take place, You take full responsibility and liability for Fraudulent Transactions, Chargebacks and/or any Losses that may be incurred as a result thereof.
- 36.2 The Bank may withhold payment in the case of excessive Chargebacks, bankruptcy, sequestration, Business Rescue, liquidation, Fraud, suspected Fraud and/or Invalid Transactions processed by You.
- 37 PRICING**
- 37.1 The fees and charges payable by You to the Bank in respect of the Acquiring Services are set out on Your Statement and exclude VAT.
- 37.2 Your Statement reflects Your latest and most up to date Schedule of Fees and Charges.**
- 37.3 Your latest Statement shall apply at all times.**
- 37.4 For any Month where the Merchant Commission payable is lower than the MMF payable, You will be required to pay the MMF to the Bank.
- 37.5 The amounts quoted or charged in terms of the pricing are subject to pricing reviews.
- 37.6 Unless You are making use of the FNB CSP or FNB PSP, the Merchant Commission negotiated between You and the Bank is separate to the fees negotiated between You and the CSP or PSP.
- 37.7 The Bank may at any time amend or introduce new fees for the use of existing products and/or Acquiring Services on reasonable notice to You. In the event that a change in the scope and/or pricing of the Acquiring Services is required during the term of this Merchant Agreement, an appropriate adjustment to the fees and charges will be made and communicated to You by any of the following means: Statement messages; telephone calls; online messages; email, website notice; post or SMS.
- 37.8 The Merchant Commission will be payable on the gross amount, except if otherwise agreed to in Writing by the Parties. The reference to "gross amount" in this provision includes the total amount of all purchases, before the deduction of Refunds, Reversals, Chargebacks and other amounts.
- 37.9 For Interchange Plus rates, the Bank may offer a Merchant a Merchant Commission rate that comprises Interchange plus a set fee. The Merchant Commission rate will fluctuate in accordance with the type of Transaction processed by the Merchant and the Interchange Rate prescribed by the South African Reserve Bank.
- 37.10 The Bank may introduce new products, and/or Acquiring Services from time to time, with their own qualifying requirements.
- 37.11 The Bank may offer preferential or special pricing options for market niches and sectors. Franchises for example, have fees and charges negotiated and communicated with the franchise head office, who in turn, communicate same to You/the franchisee.
- 37.12 Preferential or special pricing options are not automatically applied to all Merchants. Upon Your request to negotiate pricing, the Bank will consider same based on all the information available.
- 37.13 It is Your responsibility to liaise with the Bank to ensure that You have the most appropriate and favourable fees and charges to suit Your Business.

38 INTEREST

No interest will be payable by the respective Parties in respect of the Merchant Agreement.

39 STATEMENTS OF ACCOUNT

39.1 The Bank will provide You with a monthly breakdown of the amounts You owe the Bank. The breakdown will be provided in the form of a monthly Statement.

39.2 The Statement will be sent by post, email or SMS to the contact details on the application form or to the contact details contained in a subsequent notice of change of contact details. It is therefore important to ensure that the Bank has the most up to date contact details for You on record, as the Bank will not be responsible in the event that You do not receive Your Statements due to outdated contact details.

39.3 Your monthly Statement constitutes a demand by the Bank for payment and settlement of the amounts You owe the Bank within the timelines provided by the Bank.

39.4 The funds in Your Nominated Bank Account must be equal to or more than the amount You owe the Bank.

39.5 It is incumbent on You to verify the information contained in the Statement.

39.6 You must raise any query regarding the correctness of Your monthly Statement, including but not limited to any debit and/or credit entry to Your Nominated Bank Account or any amounts invoiced to You, within 30 (thirty) days from the date reflected on Your Statement, failing which the Bank will assume that all the entries on the monthly Statement are correct and that the amount so debited and credited to Your Nominated Bank Account or invoiced to You (as the case may be) is correct.

39.7 You must reconcile daily. You must raise any query regarding the correctness of Your reconciliation with the Bank, within 7 (seven) Calendar Days from the date on which the Transaction was processed, failing which the Bank may not in terms of the Card Scheme rules be able to collect the funds from the Customer.

39.8 The Bank may grant You access to reconciliation reports by way of an internet application provided by the Bank. The Terms and Conditions for the Use of the CMS Portal will govern Your access to the reconciliation reports and internet application.

40 DEBITING YOUR NOMINATED BANK ACCOUNT

40.1 The Merchant confirms that the Nominated Bank Account is in the Merchant's name. The Merchant authorises the Bank to verify the banking details as provided above.

40.2 The Merchant confirms that the Nominated Bank Account is compliant with the MLPCA, 2008 as amended.

40.3 The Merchant hereby authorises the Bank to debit the Merchant's Nominated Bank Account stated above with the amount due (the outstanding balance) in accordance with the Schedule of Fees and Charges, on a monthly basis on the date on which the amount becomes payable as reflected on the Merchant's Statement or as required by the Bank.

40.4 By using the Bank's Acquiring Service and products, You irrevocably authorise the Bank to recover from You by way of any means, the full amounts owing by You in terms of the Merchant Agreement. The Bank shall be entitled to withhold, defer and debit Your Nominated Bank Account, apply set-off or net-settle any payment due to You and obtain deferment of judgement in terms of the Merchant Agreement in respect of amounts owing to the Bank.

40.5 You may not deduct or set off from any amount You owe the Bank.

40.6 Amounts owing by You include:

40.6.1 the amount reflected on Your monthly Statement;

40.6.2 any Refunds which are due to Customers;

40.6.3 any amounts which the Bank has overpaid to You or paid in error;

40.6.4 an administration fee for each debit returned by the Bank;

40.6.5 exchange loss;

40.6.6 the value of Transactions arising out of disputes raised by the Customers with the Bank, Chargebacks received, Fraudulent Transactions, suspected Fraudulent Transactions and the value of the Transaction or a Receipt which is for any reason invalid, erroneous or illegal;

40.6.7 fees and penalties imposed on the Bank and/or You as a result of an act and/or omission or non-compliance by You, Your employees and/or Your Third-Party Service Provider with the terms of the Merchant Agreement;

40.6.8 the value of the Loss incurred by the Bank as a result of any act and/or omission or non-compliance by

- You, Your employees and/or Your Third Party Service Provider;
- 40.6.9 a penalty charge for overdue amounts;
- 40.6.10 any fees associated with the recovery of all sums from You; and/or
- 40.6.11 costs, fees and expenses (including legal fees on the attorney and own client scale, expert witness fees, collection commission and other out-of-pocket expenses and any VAT or other similar tax) which the Bank incurs in connection with maintaining and enforcing the Bank's rights under the Merchant Agreement.**
- 40.7 You are required to pay all amounts owing to the Bank upon presentation. Failure by You to do so constitutes a breach of the Merchant Agreement and such debits shall be immediately due and payable by You, and the Bank shall be entitled, in its sole discretion, to immediately suspend the Acquiring Service or terminate the Merchant Agreement forthwith. Please note that the Merchant will be held liable for any claims, losses or damages of whatsoever nature arising out of debits made by the Bank should the Merchant's Nominated Bank Account **have insufficient funds, be incorrect or held in the name of any other person.**
- 40.8 The Bank has the right to place any of Your funds (credits) or Your Nominated Bank Account on hold pending a discussion with You about any amount You owe the Bank. The Bank can place a hold on Your Nominated Bank Account at any time before the Bank debits Your Nominated Bank Account with the amounts that the Bank is entitled to recover from You under the Merchant Agreement. The Bank will remove the hold once the Bank has recovered the amounts in full which You owe the Bank.**
- 40.9 The rights granted to the Bank herein shall not preclude the Bank from any other remedy available to it whether in terms of the Merchant Agreement or in law.
- 40.10 You agree that the Bank shall have the right to recover from You and can continue to debit Your Nominated Bank Account after termination of the Merchant Agreement with any outstanding amounts for Transactions processed, including but not limited to the Merchant Commission, MMF, Equipment rental fees, fees and charges detailed in Your Statement, Losses incurred by the Bank and fines and penalties imposed on the Bank as a result of You, Your employees' or Your Third Party Service Providers' actions or omissions, Chargebacks, Refunds, amounts overpaid to You or paid in error, exchange losses etc. payable in respect of the Acquiring Services and products provided to You by the Bank.**
- 40.11 The Bank reserves the right, in the Bank's sole discretion, to waive, reduce or reverse charges or fees in individual situations.
- 40.12 The Merchant's instruction to cancel the debit order mandate, does not cancel the Merchant Agreement. The Merchant acknowledges that the authority to debit may be assigned to a third party if the Merchant Agreement is assigned to a third party, with the written permission of the Bank.
- 41 SET-OFF AND CONSOLIDATION**
- 41.1 The Bank may set-off any amount that is due and payable by You, against any:
- 41.1.1 amounts available in Your Nominated Bank Account;
- 41.1.2 amounts available in an account held in Your name;
- 41.1.3 any reserve the Bank may hold; or
- 41.1.4 amounts which are due to You.
- 41.2 You must notify the Bank beforehand, in Writing if funds in any of Your bank accounts are held by You on behalf of a third party. If You do not do this, the common-law principle of set-off will apply.
- 41.3 The Bank may consolidate all accounts which You hold with the Bank, as may be permissible in law. No partial consolidation will prevent the Bank from exercising the Bank's rights in respect of any accounts or amounts which the Bank did not include in this consolidation.
- 42 DEFAULT**
- 42.1 If any of the following things happen, You will be in default of Your Merchant Agreement:
- 42.1.1 You do not comply with the terms of Your Merchant Agreement;
- 42.1.2 You do not pay the amounts You owe the Bank under the Merchant Agreement on time (including any penalties owing);
- 42.1.3 You do not comply with the Rules, directions and instructions provided by the Bank; or
- 42.1.4 You have provided the Bank with false, Fraudulent or incorrect information ("misrepresentation"), which information was material to the Bank entering into the Merchant Agreement with You.
- 42.2 Consequences of Default
- 42.2.1 In the event that You are in default of the Merchant Agreement, irrespective of any clause to the**

- contrary in the Merchant Agreement, the Bank reserves the right to do the following:
- 42.2.1.1 withhold settlement of Transactions until such time as that the default has been rectified;
 - 42.2.1.2 hold You liable and debit Your Nominated Bank Account notwithstanding that such account may be held at another bank; apply set-off or net settle amounts owing by You to the Bank;
 - 42.2.1.3 place a hold on Your account and pledge an amount equal to an estimate of any potential Losses that the Bank may incur as a result of Your default;
 - 42.2.1.4 suspend the Acquiring Services immediately without prior notice; and
 - 42.2.1.5 terminate the Merchant Agreement immediately, without prior notice to You and without prejudice to any other rights in law.
- 42.3 The Bank may further rely on any of the remedies available to it in law.

43 SUMMARY TERMINATION

- 43.1 The Bank shall be entitled to terminate this Merchant Agreement, at any time and with immediate effect, without prejudice to any other rights it may have hereunder or in law, by providing You with notice of such termination if:
- 43.1.1 any judgment is granted against You, or Your guarantor or surety and such judgement is not satisfied within 15 (fifteen) Business Days thereafter or any of Your, or Your guarantor's and/or surety's asset(s) are attached under a warrant of execution;
 - 43.1.2 You are, other than for the purposes of reconstruction or amalgamation, placed under voluntary or compulsory winding up, or receivership or under the equivalent of any of the foregoing;
 - 43.1.3 You make any arrangement or composition with Your creditors generally, or cease or threaten to cease to carry on business or disposes of any of Your material assets other than in the normal course of business;
 - 43.1.4 You consolidate with or merge into any entity where the beneficial ownership of 20 (twenty) percent or more of the outstanding voting securities or other ownership interests in You are acquired by any entity, or group of entities acting in concert;
 - 43.1.5 there is any change in ownership in Your business and You have not advised the Bank in writing in accordance with the Terms and Conditions;
 - 43.1.6 if You sell the whole or a major portion of Your assets;
 - 43.1.7 a substantial part of Your property becomes subject to levy, seizure, assignment or sale for or by any creditor or governmental agency;
 - 43.1.8 You take any action intended to commence Business Rescue proceedings (as such proceedings are defined in the Companies Act);
 - 43.1.9 there is a change in classification of Your business i.e. the nature of Your business changes and You omitted to advise the Bank in Writing of such change;
 - 43.1.10 if You institute any proceedings with the intention to commence Business Rescue proceedings (these proceedings are only applicable to companies and close corporations in terms of the Companies Act);
 - 43.1.11 if You or Your guarantor or surety is: provisionally or finally sequestrated/liquidated (voluntarily or compulsorily); placed under Business Rescue; or, being a partnership, dissolved;
 - 43.1.12 You, being an individual:
 - 43.1.13 Your guarantor or surety commit an act of insolvency mentioned in the Insolvency Proclamation, 1989 as amended from time to time, or an act that gives or may give rise to Your or them being liable to be wound up by a court of law;
 - 43.1.14 You publish notice of the voluntary surrender of Your estate;
 - 43.1.15 You are placed under administration in terms of the Insolvency Proclamation 1989 as amended from time to time, or debt counselling;
 - 43.1.16 You have an application or other proceedings brought against You in respect of which a third party seeks to have You sequestrated or placed under curatorship, whether in a manner which is provisional or final, voluntary or compulsory; and/or

44 CLOSURE, RESTRICTED OR SUSPENDED ACCESS TO ACCOUNT

You acknowledge and agree that the Bank has the right to close, restrict or suspend access to any of Your bank accounts held with the Bank, should the Bank be informed or suspect that Your Bank accounts are being used fraudulently, negligently, or for illegal activities; or if the Bank is required to do so in order to comply with the Rules. You hereby indemnify the Bank against any and all Losses suffered howsoever arising, from the Bank closing, restricting or suspending access to Your bank account(s).

45 INTELLECTUAL PROPERTY

- 45.1 Subject to the remaining provisions of this clause, all Intellectual Property owned by either Party (whether before or after the Effective Date) shall remain the sole and exclusive property of that Party.
- 45.2 You acknowledge that the Bank shall, by operation of law, become the owner of the Intellectual Property in any work which is created or executed by the Parties, whether alone or with others, in the course and scope of this Merchant Agreement.
- 45.3 Upon termination of this Merchant Agreement for any reason whatsoever, the Parties agree that the Intellectual Property rights which have accrued to the Bank, will remain vested in the Bank and that notwithstanding such termination, You will have no rights in or to the Intellectual Property.

46 FORCE MAJEURE

- 46.1 Should the Bank be prevented from fulfilling any of its obligations in terms of this Merchant Agreement as a result of any "Acts of God", load-shedding, power-outage, illegal strikes or a cause beyond the reasonable control of the Bank, the Bank will forthwith give Written notice thereof to You:
- 46.1.1 specifying the cause and anticipated duration of the Force Majeure; and
- 46.1.2 upon termination of the Force Majeure, stating that such Force Majeure has terminated.
- 46.2 Performance of any obligations will be suspended from the date on which notice is given of a Force Majeure event until the date on which notice of termination of a Force Majeure event is given (hereinafter referred to as "the Suspension Period"), subject always to the remaining provisions of this clause.
- 46.3 The Bank will not be liable for any delay and/or failure in the performance of any obligation hereunder, or Loss incurred due to and/or resulting from the Force Majeure during the Suspension Period, provided that:
- 46.3.1 the Bank uses and continues to use its best efforts to perform such obligation; and
- 46.3.2 if the Force Majeure continues for more than 21 (twenty-one) consecutive days, You will be entitled to terminate the Merchant Agreement on the expiry of such 21 (twenty-one) day period but will not be entitled to claim damages from the Bank as a result of the delay or the failure in the performance of any obligations hereunder due to or resulting from the Force Majeure.

47 LIMITATION OF LIABILITY

- 47.1 Neither Party shall be liable to the other for indirect or consequential damages, including but not limited to loss of profits or savings arising out of or relating to that Party's performance or failure to perform under this Merchant Agreement.
- 47.2 The limitation of liability set forth above shall not:
- 47.2.1 apply in any way to Your liability to the Bank arising from or relating to a breach of: Warranty, indemnity, confidentiality, or Data protection obligations or Intellectual Property rights;
- 47.2.2 apply to liability resulting from the gross negligence or wilful misconduct of either Party; and/or
- 47.2.3 apply to claims for death or personal injury.
- 47.3 For avoidance of doubt any claim instituted under the aforementioned clause shall include indirect, special and consequential damages and shall be uncapped.
- 47.4 Unless the Bank acted with gross negligence, the Bank will not be liable for events beyond the Bank's reasonable control, or for any Losses You may suffer, which include, but will not be limited to:
- 47.4.1 system failures;
- 47.4.2 Equipment malfunctions;
- 47.4.3 any Communication Network breakdown or lack of coverage;
- 47.4.4 load shedding;
- 47.4.5 failure by the Bank to perform or process a Transaction as a result of sabotage; terrorism; loss or destruction of Data; destruction, hacking or deterioration of storage media; power failures; natural phenomena; riots and acts of vandalism;
- 47.4.6 any Loss, which You or any other party may suffer due to unauthorised interception, monitoring and Data Compromise;
- 47.4.7 any unauthorised use of the Equipment, Acquiring Services and products by You, Your employee or Your Third Party Service Providers, Fraud, theft of Equipment or as a result of a compromise of the confidentiality of Your security mechanisms or systems;
- 47.4.8 Your use of, or inability to use the Bank's Acquiring Services and/or products;
- 47.4.9 any Losses incurred if You did not take the required steps to safeguard the Equipment; software, hardware; secure access codes and associated information and/or follow the steps recommended by the Bank from time to time, including performing software or hardware updates; and

47.4.10 late or delayed Transactions or eReceipts.

48 DOMICILE AND COMMUNICATIONS

- 48.1 The Bank hereby selects the following address as the address to which all legal notices in relation to the Merchant Agreement must be delivered: First National bank of Lesotho Limited, Legal and Compliance: 1st Floor, Star Lion Group Building, Cnr Kingsway and parliament Roads, Maseru, 100. This address is known in law as the Bank's *domicilium citandi et executandi*, or "domicile address".
- 48.2 Any legal notice or communication required or permitted to be given by You in terms of this Merchant Agreement will be valid and effective only if in Writing.
- 48.3 By using the Acquiring Services and products You confirm that:
- 48.3.1 You choose the physical address of the Merchant (an address in Lesotho) reflected on the application form or subsequent Written notification of change of contact details as Your Domicile address;
- 48.3.2 the Merchant contact and address details on the application form or subsequent Written notification of change of contact details will be used by the Bank to:
- 48.3.2.1 send billing reports and Statements
- 48.3.2.2 send notifications of updates to the Merchant Agreement;
- 48.3.2.3 serve any legal notices, processes and communications;
- 48.3.2.4 execute any judgment obtained against You; and
- 48.3.2.5 send day-to-day (operational) communications.
- 48.4 By using the Bank's Acquiring Services and products and notwithstanding termination of the Merchant Agreement, You provide the Bank with authority to act on any instructions received from You Your Authorised Representatives or Your employees; or any instructions received from Your Merchant contact details, including the email address reflected on the application form or Merchant address or; or the address reflecting on a subsequent Written notification of change of contact details.**
- 48.5 If You change Your address but do not notify the Bank, Your continued use of the Acquiring Services and products will serve as confirmation that the Bank may send and receive notices to and from You and serve legal processes to and from Your last address known to the Bank, or any other address which You advised the Bank of in Writing.**
- 48.6 For clarity, day-to-day (operational) communications may be communicated to You by the Bank by way of by way of: Online Banking, the FNB Banking App, Bank pre-recorded telephone calls; email; statement message; website messages; post and SMS service.
- 48.7 You agree that the Bank will transmit the following information to You in accordance with clause 48.6: masked PAN, date of Transaction, amount of Transaction, Merchant identification number, Merchant number, terminal identification number; daily and pending settlement amounts and any other Transaction Data.
- 48.8 Notwithstanding anything to the contrary contained herein, it is specifically recorded that by using the Acquiring Service and products You agree that the Bank may send Statements, billing reports and/or invoices to You by way of email and may notwithstanding any other provisions of the Merchant Agreement communicate billing information to You by way of Bank pre-recorded telephone calls.
- 48.9 It is therefore important to ensure that the Bank has the most up to date contact details on record, as the Bank will not be responsible in the event that You do not receive communications from the Bank due to outdated contact details.
- 48.10 A notice will be treated and presumed as having been received by You, unless the contrary is proven:
- 48.10.1 if delivered by hand during normal hours - on the date of delivery;
- 48.10.2 if posted by prepaid registered post - at 10:00 on the 4th (fourth) day after the post office issued the registration receipt;
- 48.10.3 if sent by post - at 10:00 on the 7th (seventh) day from the date of posting;
- 48.10.4 if sent by fax - on the date shown on the receipt generated by a fax machine; and
- 48.10.5 if sent by email - on the date on which the notice was emailed.
- 48.11 When the Bank presumes that You received a notice by a certain date in accordance with the aforementioned clause, the Bank does not have to prove that You did receive the notice on such date.
- 48.12 If You claim that You did not receive the notice by that date, then You will have to prove it.
- 48.13 Notwithstanding anything to the contrary contained in this Merchant Agreement, a Written notice or communication actually received by one of the Parties from another shall be regarded as adequate Written notice or communication to such Party, notwithstanding that the provisions of this clause were not strictly complied with.

49 GOVERNING LAW

- 49.1 This Merchant Agreement will be governed, construed and take effect in all respects in accordance with the laws of the Kingdom of Lesotho.
- 49.2 You agree that the Bank may bring legal proceedings against You relating to the Merchant Agreement in any Magistrates Court that has authority to hear and decide on the matter at hand (this authority is called "jurisdiction"). You agree to the jurisdiction of the Magistrates Court even if the amount the Bank claims from You is more than the Magistrates Court limit. The aforementioned provision does not prevent the Bank from bringing legal proceedings against You in a High Court that has jurisdiction.

50 COMPLAINTS PROCESS

- 50.1 You may contact the Merchant Services Helpdesk to log a complaint or alternatively use the Bank's CARE system available on the FNB Website.
- 50.2 You further have the right to resolve a complaint with the Bank by way of Alternate Dispute Resolution. To do this, You must file Your complaint with the CBL **22232225** or visit the website at **www.centralbank.org.ls**

51 CONTACT INFORMATION

- 51.1 If You have any queries, You must contact the Bank at the Merchant Services Helpdesk by telephone on 22241061 or by email **DLFNBLESOTHOSSD@fnb.co.za**.

52 MERCHANT LITE

- 52.1 Merchant Lite is a suitable option for Merchants who do not meet the Bank's credit and risk scoring criteria, but still wish to make use of limited Acquiring Services and products.
- 52.2 Merchant Lite provides limited Acquiring Services and products as follows:-
- 52.2.1 for Stand-Alone Solution(s) and/or Stand-Alone Speedpoint® Device(s) only;
- 52.2.2 Merchants may only process the following Transactions on Merchant Lite:-
- 52.2.2.1 Purchase, Contactless, Reversal of Last Transaction, Cash Advance, Cashback with Purchase Transaction, Balance Inquiry and eWallet Purchase; with either one of
- 52.2.2.2 a Chip Card, whether credit, debit or cheque only; by.
- 52.2.2.3 dipping the Chip Card into the Speedpoint Device® only;
- 52.2.2.4 Tapping the Chip Card on the Speedpoint Device® only (Contactless).
- 52.3 The Merchant applies for Merchant Lite by selecting the option on the Application Form.
- 52.4 A Merchant shall qualify for Merchant Lite when the following criteria are met:
- 52.4.1 the Merchant opens an FNB transactional account;
- 52.4.2 the Merchant's turnover is less than R10million;
- 52.4.3 Transactions processed on the Speedpoint® Device must be settled into the FNB transactional account described above.
- 52.5 If Merchant Lite is combined with the Gold Speedpoint® Bundle, the Gold Speedpoint® Bundle Terms and Conditions shall apply and must be read together herewith.
- 52.6 Subject to the Merchant meeting the criteria for the Gold Speedpoint® Bundle, the Merchant shall qualify for the rebate and the Gold Speedpoint® Bundle's Merchant Commission rate.
- 52.7 You may not process the following Transactions on Merchant Lite:
- 52.7.1 Refunds, Cash Withdrawal, Voice Override, Pre-Authorisation, Authorisation Only, Pre-Authorisation Cancel, Pre-Authorisation Complete, Manual Entry and Fallback Transactions.
- 52.7.2 You may not process the following Cards on Merchant Lite:
- 52.7.3 Magstripe Cards (including RCS, Edcon and Loyalty Cards including eBucks Cards);
- 52.7.4 Fleet Cards, Garage Cards and Petrol Cards;
- 52.8 Merchant Lite will terminate:
- 52.8.1 in the Bank's sole discretion to discontinue Merchant Lite and on 20 (twenty) business days' notice to the Merchant; or
- 52.8.2 if the Merchant closes its FNB bank account or terminates the Merchant Agreement in accordance with these Terms and Conditions.
- 52.9 The remaining provisions of this clause apply to Merchant Lite, only insofar as they specifically relate to Merchant Lite.
- 52.10 You may not upgrade from Merchant Lite. In the event that You require additional functionality, new application must be made therefor, subject to credit vetting and scoring criteria.
- 52.11 Merchant Lite is only available in the Republic of South Africa.

52.12 The Bank strives to keep the information provided as accurate as possible and will not be held responsible if an error or omission is found.

53 SORTING AT SOURCE

53.1 'Sorting at Source' is where You have acquiring relationships with different banks with the intention of processing Transactions directly to the cardholder's bank. Multiple primary acquiring relationships, which result in the bypass of clearing is not permitted by.

53.2 You may not be involved in, develop, allow, process or in any way whatsoever facilitate Sorting at Source.

53.3 The secondary use of multiple acquiring relationships, e.g. back-up Speedpoint® Devices for disaster recovery or as part of Your business continuity plan does not constitute Sorting at Source.

53.4 Your non-compliance with the above requirements may result in fines or penalties being levied by the regulator or the Card Associations, which fines or penalties will be debited from Your Nominated Bank Account.

54 AUTHORISED REPRESENTATIVES

54.1 In the event that there are more than 2 (two) Authorised Representatives:-

54.1.1 the Merchant shall provide the Bank with a company resolution or similar document, which empowers and authorises the persons named therein as Authorised Representatives;

54.1.2 In the event of conflicting instructions from the Authorised Representatives, the Bank shall carry out the first instruction received first in time and no further conflicting instructions until such time as the deadlock is resolved between Authorised Representatives and communicated in a joint manner to the Bank.