These Payment Processing Services Terms of Use ("PPS Terms") are applicable when you make use of our Solutions. Our Solutions enable you to accept payments from your Customers for goods and/or services purchased online from you. The PPS Terms set out the rights and obligations of the Parties in respect of the Solution and form part of the Merchant Agreement entered into with us.

BY SIGNING THE APPLICATION FORM OR A REQUEST FOR AN ADDITIONAL SOLUTION, YOU AGREE TO BE BOUND BY THE PPS TERMS SET OUT HEREIN.

PROCESSING OF PERSONAL INFORMATION BY THIRD PARTIES AND ALTERNATIVE SERVICE PROVIDERS

By using the Solutions, your Personal Information and that of a Customer will be shared with third parties and Alternative Service Providers to enable us to render the Solutions under the various Payment Streams. The full list of third parties and Alternative Service Providers is provided in Section 15 of the PPS Terms

Your Personal Information will be used for the purposes, in the manner, and with the appropriate controls, set out in our Privacy Notice. To better understand how your Personal Information will be treated, please refer to our Privacy Notice which forms part of this privacy term, a copy of which is available on Adumo Online Website at www.adumoonline.com ("Privacy Notice").

By using our Solutions:

- you agree that we may share your Personal Information with the third-parties and Alternative Service Providers set-out herein;
- you warrant that your Customers agree that their Personal Information may be shared with the third-parties, Alternative Service Providers and us, for the processing of Customer Transactions.

1. DURATION

1.1. The PPS Terms will become effective from the earliest date of the following ("Effective Date"):

1.1.1. the date we confirm your activation of the Payment Gateway or Hosted Payment Page; Integrated Reporting; and/or Solution, as selected. Activation means the act or process that we perform to enable the Payment Gateway or Hosted Payment Page; Integrated Reporting; or Solution for your use; or

1.1.2. the date you start using the: Payment Gateway or Hosted Payment Page; Integrated Reporting; and Payment Streams individually, as selected.

1.2. The PPS Terms can be terminated by either of the Parties in accordance with the General Terms of Use.

2. GENERAL

2.1. By using the PPS Services, as selected on the Application Form, you agree to be bound by the PPS Terms as set-out herein.

2.1.1. We agree to enable the Solutions that you selected on the Application Form on the Payment Gateway or the Hosted Payment Page, as applicable.

2.2. From the Effective Date of this PPS Services, you appoint us to provide you with your selected PPS Services that enable you to accept payments from Customers to pay for goods and/or services purchased from you.

2.3. We agree to make the PPS Services available to you until terminated by either of the Parties in accordance with the Merchant Agreement.

2.4. The Solutions set-out herein are provided "as is" without any warranty from us. You accept all risk and liability associated with and arising from your use of the Solutions.

2.5. We make no representation that the operation of the Solutions will be uninterrupted and we will not be liable for the consequences of any interruptions or errors.

2.6. By using the PPS Services, you agree to:

2.6.1.   provide a comprehensive description of the goods and/or services on offer;

2.6.2.   provide comprehensive details of return and refund policies;

2.6.3.   display your contact details which include a contact name, telephone number, physical/registered address of your permanent establishment and email address;

2.6.4.   disclose your privacy policy, setting out how you will process your Customers' Personal Information;

2.6.5.   display the total price of the goods and/or services;

2.6.6.   include all relevant taxes and delivery charges (all prices quoted must be in South African rand) in the total amount payable by the client;

2.6.7.   disclose to your Customer where and when your returns/refund and cancellation provisions restrict the return of goods or cancellation of services;

2.6.8.   communicated to the Customer that you and not the supplier of the goods or service, are responsible for fulfilment;

2.6.9.   not accept payments on your website and/or mobile application until you inform your Customer about when the goods and/or services will be delivered;

2.6.10.   enforce appropriate terms and conditions on your Customers to reflect the terms set-out in in the Merchant Agreement;

2.6.11.   not split or disguise Card Not Present Transactions or act in a way to avoid obtaining Authorisation;

2.6.12.   not set or enforce a minimum or maximum limit on the Transaction amount for payments made using any of the Solutions unless otherwise indicated by us or the Alternative Service Provider;

2.6.13.   not directly or indirectly, increase the purchase price, add fees, charges, increase obligations or decrease benefits for products and services purchased using a Payment Instrument.

2.6.14.   comply with the terms of your agreement of each of the Alternative Service Providers that provide you with a Solution in conjunction with us;

2.6.15.   indicate to your Customers what Payment Instruments are accepted by you, based on the Payment Instruments you selected on our Application Form or additional Solution request;

2.6.16.   inform your Customer of any tax implications, exchange control regulations and/or any other relevant legislation that may be applicable to your Customer and/or the goods and/or services your Customer is purchasing online from you;

2.6.17.   ensure that the information printed and completed on the delivery note and/or proof of dispatch is true and correct;

2.6.18.   open a bank account with a South African bank and appoint an Bank for authorisation and settlement services;

2.6.19.   only operate within your Bank's jurisdiction as specified by your Bank;

2.6.20.   introduce fraud measures and controls;

    2.6.20.1. encrypt each Card Not Present Transaction, unless you have signed-up for our Tokenisation services;

    2.6.20.2. not to store a Customers CVV number.

2.7.   Authorisation

2.7.1.   You agree to only request Authorisation at the time of and for a particular Online Transactions. Authorisation is a prerequisite for the dispatch of any goods and delivery of services.

2.7.2.   If authorisation is granted, you must dispatch the goods or deliver the service within the time stipulated in your delivery policy or terms and conditions.

2.8.   Solutions

2.8.1.   By using the Solutions, you understand and agree that you may have to enter into an agreement with the Bank or an Alternative Service Providers (as applicable), as indicated in clause 15 below.

2.8.2.   It should further be noted that we merely act as a conduit for routing Transactions for authorisation and settlement to:

    2.8.2.1. Issuing Banks and acquiring Banks as well as Card Associations for the processing of all card transactions.

2.9. We are not responsible for settlement of Transactions. We merely route Transactions for authorization and settlement to third parties and Alternative Service Providers, as applicable.

3. FRAUD

Should fraudulent transactions account for more than 8% of your Card sales turnover in any month, we may review the terms of the Merchant Agreement, suspend the Solution or terminate our agreement with you for the provision of such Solution, without prejudice to any of our rights in law.

4. WARRANTIES: WHAT WE WARRANT TO EACH OTHER

4.1. The presentation of a Transaction to us will be a warranty by you that:

4.1.1. all information in the Transaction request is true and correct.

4.1.2. you did not levy additional fees to the normal price of your goods and/or service, in respect of Transactions processed through the Payment Gateway or Hosted Payment Page;

4.1.3. you have supplied the product and/or services on receipt to the Customer;

4.1.4. no fictitious and/or fraudulent Transactions were processed by you;

4.1.5. the Transaction is not an Invalid Transaction or illegal;

4.1.6. the Transaction has been Authorised by the Customer.

5. INDEMNITIES

5.1. You indemnify us and our Alternative Service Providers against any liability for any damages, Losses and/or consequential damage that you, our Alternative Service Provider or us may suffer as a result of the loss of Data, which loss was not attributable by us; erroneous, unauthorised or unlawful collections or Transactions processed by us on your instruction; us acting on your instruction; being unable to connect to Our System; the incorrect, late execution or non-payment of any of your instructions due to your actions or omissions; any other defect in Your System or Our System contributed by you.

5.2. By using the PPS Service, you agree to process Transactions at your own risk and indemnifies us for any and all Losses incurred as a result of processing Transactions that you may incur that is not a result of our actions or omissions.

6. FEES AND CHARGES

In return for the provision of the PPS Services, you will pay us the Charges as set-out in the Charges Schedule. The Charges are not dependent on whether the Transaction was successful or unsuccessful.

7. EXCLUSIONS

We are dependent on acquiring Banks, Card Associations, BankservAfrica, Alternative Service Providers and Issuing Banks for the availability of their systems to process Transactions. We do not accept any responsibility for the unavailability of their systems when processing Transactions.

8. TERMINATION

8.1. Upon termination of the PPS Terms:

8.1.1. the PPS Services will cease, provided that current and outstanding Transactions including approved submissions in your queue will be attended to and completed;

8.1.2. you remain responsible for Chargebacks, Charges, liability and responsibilities that arose in respect of the Transactions that were processed by you;

8.1.3. you agree not to process any Payment Instruments. Should you process Payment Instruments post termination of the PPS Terms, we may, without prejudice to any other remedies available to us, elect to apply the provisions of the Merchant Agreement to Transactions processed post termination of the PPS Terms, as if the PPS Terms had not been terminated.

9. QUERIES AND COMPLAINTS

Any product-, technical failure-, settlement, statement-, report, fraud-, authorization-, reconciliation query, Charges disputes and complaints can be raised directly with Adumo Support by contacting Adumo Online Support Contact Number or by sending an email to Adumo Online Support Email Address.co.za.

A. CORE OFFERING

The PPS Service consists of the provisioning of a Payment Gateway. The Payment Gateway can be accessed by a. Virtual integration method provides access to our Hosted Payment Pages.

1. VIRTUAL INTEGRATION – HOSTED PAYMENT PAGE

1.1.1. The Hosted Payment Page provides you with an end-to-end PCI compliant Transaction processing platform which includes Payment Instrument information collection and routing of the information to the Alternative Service Provider and/or Bank (as applicable), for authorization and settlement; sensitive data protection; fraud prevention; Transaction security and management; and support services to Customers.

1.1.2. You agree that you will ensure that no pornographic content is offered by you, unless there are sufficient technical restrictions to guarantee that minors are refused access.

1.1.3. The Hosted Payment Page does not include:

1.1.4. the connection and the transmission of Data between you and the Customer. Such connection and the transmission are beyond our control;

1.1.5. the transmission of Data in third-party telecommunications networks and Data communications via the Internet. Third-party telecommunications networks and Data communications through the Internet are beyond our control, and we will not assume any responsibility for the availability or reliability of third-party telecommunications networks, or for transmission errors, or for changes to the transmitted Data that occur in third parties' telecommunications networks or systems.

1.1.6. Right to Use the Hosted Payment Pages

1.1.6.1. Once your application for Hosted Payment Pages has been approved by us, we will grant you a non-exclusive, non-transferable right to use the Hosted Payment Pages and the written specifications for the interface ("Interface Information") to integrate into the Hosted Payment Page to process Transactions. Other than as provided for in this clause, you are not granted any further rights.

1.1.6.2. This right to use the Hosted Payment Pages enables you to process Payment Instruments for the payment of goods and/or services purchased by a Customer online from you.

1.1.6.3. The Hosted Payment Page will be operated and hosted by us. The Hosted Payment Page and any associated software provided by us will remain our Intellectual Property. You do not acquire any right to install and/or use the software or Hosted Payment Page in your own hardware environment.

1.1.6.4. With regard to Interface Information and the Hosted Payment Page, you agree not to:

1.1.6.5. grant third parties any manner of access to the Interface Information or the software application made available, the respective source code (if provided) or the product documentation, without our prior written consent. Notwithstanding the aforementioned, you may provide your authorised users with access to the Hosted Payment Platform to the extent technically necessary to perform under the Merchant Agreement.

1.1.6.5.1. process, copy, alter, combine or compile the source code or object code for the software (if provided) or any part thereof, unless the Merchant Agreement expressly provides otherwise;

1.1.6.5.2. decompile, disassemble or reverse engineer an object;

1.1.6.5.3. use the Interface Information for third parties who will become your contractual partners after termination of the Merchant Agreement.

1.1.7. Connection to the Platform

1.1.7.1. We will provide you with the Interface Information.

1.1.7.2. The access to the Hosted Payment Page will be provided at the point where the network of Our System ends and where you will retrieve access to the Hosted Payment Page by way of an access node with the Internet ("Point of Interconnection").

1.1.8. Any data link between you and the Point of Interconnection is your sole responsibility.

1.1.8.1. You are required to access the web-based software application which is hosted on the Hosted Payment Page by way of a telecommunication link (Internet).

1.1.8.2. You are responsible for transmitting the Data required for the processing of a Transaction.

1.1.9. Processing of Transactions

1.1.9.1. When the Hosted Payment Page is used, the Transaction is sent from you to the Hosted Payment Page. You agree to ensure that adequate security measures are applied to secure the transmission between you and your Customer. We will not be responsible for the security of the Data that is submitted from the Customer or you to the Hosted Payment Page.

1.1.9.2. We will pass the Transaction Data that we receive from you onto the relevant Alternative Service Provider and/or Bank (as applicable), for verification, processing and clearing. We will transfer the Transaction Data to the Bank in a PCI compliant manner.

1.1.9.3. The verification of Transaction Data related to payments is done exclusively by the Alternative Service Provider and/or Bank (as applicable), and we have no contractual obligation to you in this regard, unless required by applicable Rules.

1.1.9.4. You agree to transmit the Transaction Data in compliance with the form and format defined in the Interface Information.

1.1.10. Acting as Agent

1.1.10.1.1. You agree to at all times clearly demonstrate and depict that we merely act as a conduit in transmitting Transactions from you to third-parties.

1.1.10.1.2. If Customers institutes a claim on us relating to the use of the Hoisted Payment Page, you hereby indemnify us against all and any claims or demands to the maximum extent permissible by law.

1.1.11. Enhancements and Maintenance

1.1.11.1.1. From time to time, we will enhance the Hosted Payment Page, whereafter we will provide you with the new versions of the Hosted Payment Page for implementation within the timelines communicated in a notice to you. Your right to use the previous versions will come to an end on the date communicated in a notice to you.

1.1.11.1.2. We may interrupt the Hosted Payment Platform for maintenance upon 5 working days' prior notice or as communicated in a notice to you, provided urgency does not require a shorter notice-period.

2. INTEGRATED REPORTING

2.1. You must exercise the Client Portal with due skill and care.

2.2. You will have access to Integrated Reporting in the Client Portal.

2.3. You agree to only provide authorised employees access to the Client Portal to draw reports on the Transactions processed by you and to enquire the status of Transaction.

2.4. Any disputed information on the Client Portal should be brought to our immediate attention.

2.5. You agree not to solely rely on the Data provided in the reports, but to verify the Data in the reports with the Transaction Data you have on record.

2.6. We will not accept any liability arising from the use of the Client Portal and the information displayed thereon and you accordingly indemnify us against Losses incurred from the use of the Client Portal and the information displayed thereon.

3. PAYMENT LINK

3.1.   We will enable you to request payment from your Customer for goods and/or services purchased online from you by sending a Payment Link by email or SMS to the Customer.

3.2.   Once your Customers selects the payment button, the Customer will be directed to our Hosted Payment Page, provided you have embedded the Payment Link in an SMS, email or pdf document. The amount payable will be reflected on the Hosted Payment Page. The Customer must proceed in completing its billing and shipping information, whereafter the Customer can select the payment button for the payment to be processed.

3.3.   Transactions processed by way of a Payment Link will be processed as an ecommerce Transaction.

3.4.   Once the payment button is selected, we will submit the Transaction to the Bank for settlement and approval.

3.5.   The Bank will settle you directly for the Transaction processed using a Payment Link.

B. OFFERED AT CHECKOUT

1. CARD NOT PRESENT TRANSACTIONS

1.1.   This Solution presents the standard ecommerce product offering in South Africa. You will typically apply for your own Merchant relationship with the following acquiring banks: ABSA, FNB, Standard Bank, Nedbank.

1.2.   The Bank will provide the merchant ID (MID), along with the Merchant account where settlement funds are deposited.

1.3.   We support the following Cards: Mastercard Credit and Debit, VISA Credit and Debit, Diners Club, American Express, and foreign cards.

1.4.   You are responsible for the fees charged by the Banks and Alternative Service Providers for Transactions processed by you.

1.5.   Processing Card Not Present Transactions

   1.5.1.   A Customer will purchase product and/or services from you and proceed to checkout.

   1.5.2.   Upon checkout, you will open a secure payment page, either supplied by Hosted Payment Page or by using our Payment Gateway.

   1.5.3.   The Customer's captures its Card details either on the Hosted Payment Page or on your payment page when using our Payment Gateway.

   1.5.4.   The Transaction will be processed in a 3D Secure compliant manner and the Customer will be prompted to insert an OTP in the window provided.

   1.5.5.   The Issuing Bank approves/declines the 3DSecure request and sends it back to the Hosted Payment Page or on your payment page when using our Payment Gateway.

   1.5.6.   We will route the Transaction to the Issuer for authorization.

   1.5.7.   Settlement requests will either be initiated by you or automatically by us, depending on your settings.

   1.5.8.   The Bank will settle you.

1.6.   Chargebacks

   1.6.1.   Protection against Chargebacks is subject to the Card Association rules and limited to 3D-Secure authenticated Card Not Present Transactions.

   1.6.2.   You must ensure that all your Card Not Present Transactions are 3D-Secure.

   1.6.3.   You may not demand or require the Customer to waive their dispute rights to a payment.

1.7.   Refunds

   1.7.1.   The Consumer Protection Act 68 of 2008 provides that a customer may return goods to a supplier and receive a full refund of the consideration paid for those goods, under certain conditions.

   1.7.2.   You, as the supplier of goods, may be required to Refund the full purchase price to a Customer, if a Customer wishes to reject delivery, or return goods for the reasons stipulated in the CPA. If a Customer returns goods or cancel services purchased on reasonable grounds, you may not refuse to exchange, or process a Refund in respect of such goods and/or services. In the event that any Refund is required, you undertake to Refund the Customer the full purchase price or part thereof (whichever is applicable).

1.7.3. If you restrict the return of goods or cancellation of services, you must clearly disclose your return, Refund and cancellation rules to your Customer.

1.7.4. In the event that you are no longer our customer, there will be no obligation on us to assist you in processing a Refund to a Customer.

1.7.5. All Refunds requests that we receive from you in respect of Card Not Present Transactions, will be submitted by us to the Bank for processing.

1.8. Indemnities

1.8.1. By using our Solutions set-out herein, you agree to indemnify us for the Losses arising from:

1.8.2. all Card Not Present Transactions processed by you that are not 3D-Secured;

1.8.3. any disputed Transaction and/or Chargebacks.

2. EFT SOLUTION (INSTANT EFT)

2.1. Our PPS Services enables you to receive online payments from your Customers using the EFT Solution and to be instantly notified of the payment. EFT Solution payments ("EFT Payments") must be made through one of the South African banks supporting the EFT Solution.

2.2. This solution enables a Customer to pay using SecureEFT, enabled through Ahead start (Pty) Limited.

2.3. If you selected "EFT" on your Application Form, your Customers will be able to make payment by way of EFT.

2.4. The Alternative Service Providers owns all copyright, trademarks, trade names and other intellectual property rights, whether registered or not, subsisting in or used in connection with their respective brands. You will be provided with the Supplier's trade mark artwork for display on your website, for the duration of the EFT Solution. The trade mark artwork may solely be used in connection with the provision of the EFT Solution option to Customers.

2.5. Except as expressly permitted in these terms and conditions, you will not:

2.5.1. sell, rent or lease the EFT Solution application;

2.5.2. wilfully remove or obscure any copyright, trade make, brand name or proprietary right notices contained in or affix to the EFT Solution application.

2.6. You are hereby granted a right to use the EFT Solution for the sole purposes of processing EFT Payment requests at the request of Customer, for goods and services purchased by the Customer online from you.

2.7. We will not be held responsible for incorrect banking details provided by you or your Customers when making EFT Payments.

2.8. By using the EFT Solution, you acknowledge that the EFT Solution does not enable you to process any Refunds to your Customers.

2.9. You accept that you shall be solely responsible for processing such Refunds to your Customers.

2.10. You may not do something or cause something to be done that will allow the disablement of the authentication of Customer Transactions.

2.11. EFT Solution Transactions

2.11.1. When a Customer selects to pay for goods and/or services by way of EFT Payments, the Customer will be redirected from your website and/or mobile application to the Customer's mobile banking application, to initiate an EFT Payment and then redirected back to your website and/or mobile application to complete the Transaction.

2.11.2. The Alternative Service Provider sets up the beneficiary, and the payment.

2.11.3. The EFT Solution requires a Customer to login to their bank account and authenticate the payment through the bank's one time pin or authentication methodology.

2.11.4. The standard OTP/In APP security prompts are sent to the Customer's mobile phone.

2.11.5. The Alternative Service Provider will send notifications on the status of the Transaction to you and us.

2.11.6. The Issuing Bank will settle you directly for the value of the Transaction.

2.11.7.   You are not allowed to exceed a failure rate of 5% based on the total volume of EFT Solution Transactions submitted to us for processing. We reserve the right suspend or terminate your EFT Solution should these rates consistently remain above industry standards.

3. VISA CLICK TO PAY

3.1.   By selecting VISA Click to Pay on the Application Form, you agree that you will accept payment for goods and/or services on your website by allowing customers to pay with Visa Click to Pay.

3.2.   Processing Visa Click to Pay Transactions

3.2.1.   Upon selection of Visa Click to Pay at check out, we will forward the Transaction request to VISA.

3.2.2.   Visa will request the Customer to log in and select the Card it wants to use, or if not previously registered to register the Card.

3.2.3.   A 3DS verification will be performed on the selected Card if required, and an authentication message will be sent to the Customer.

3.2.4.   We will submit the Transaction for authorization and settlement to the Bank.

3.2.5.   The Bank will settle you directly for Transactions processed using VISA Click to Pay.

4. MOBICRED

4.1.   General

4.1.1.   Mobicred is an online revolving credit facility that can be used to pay for goods and/or services purchased online from you.

4.1.2.   You may not allow another merchant to use your Mobicred Solution to process Mobicred Transactions.

4.1.3.   A pre-authorization request must be submitted in respect of all Mobicred purchase Transactions. Upon the submission of a pre-authorization request, you will receive a Mobicred reference number.

4.1.4.   You agree not to communicate the pre-authorisation and/or approval of any Mobicred Transaction to a Customer where no such pre-authorisation and/or approval has been obtained from us.

4.1.5.   You agree not to initiate any Mobicred Transaction where a Mobicred Transaction has not been initiated by a Customer

4.1.6.   All subsequent pre-auth transactions, refunds, cancellations and approvals requests in respect of the Transaction must use the same reference number.

4.1.7.   In the event that you do not receive a reference number for a Mobicred Transaction, you may not accept Mobicred as a Payment Instrument.

4.1.8.   You may not split, disguise, or facilitate the slipping or disguising a Mobicred Transaction or act in any way not to obtain a pre-authorization.

4.1.9.   Pre-auth Transactions will automatically be cancelled, if a Mobicred Transactions in respect of which the reference number was issued, has not been approved within 60 (sixty) days of the date of issue.

4.1.10.   With the exception of reference numbers issued for pre-authorisation that were not approved within 60 (sixty) days, reference numbers do not expire.

4.1.11.   You must retain Transaction history of all Mobicred Transactions for a minimum period of 5 years from the date of the pre-authorization of each Mobicred Transaction, or for any further period thereafter as may be advised by us, or as may be prescribed by the Rules.

4.1.12.   No offline Mobicred Transactions will be allowed, supported or pre-authorized.

4.2.   Processing Mobicred Transactions

4.2.1.   A Customer have to register and apply for a credit facility.

4.2.2.   Upon approval, the Customer will receive a username and password from Mobicred.

4.2.3.   Upon check-out, the Customer may select Mobicred as payment option.

4.2.4.   Once Mobicred is selected, the Customer will be requested to log in to the Mobicred profile with their username and password.

4.2.5.   We will route the Mobicred Transaction to Mobicred for approval.

4.2.6.   Mobicred will approve the Transaction.

4.2.7.   Mobicred will settle you directly into the bank account provided to them.

4.3.   Illegal Transactions

4.3.1.   A transaction will be invalid and Mobicred will have no obligation to pay if:

4.3.2.   authorization was not obtained for a Mobicred Transaction;

4.3.3.   the Mobicred transaction is illegal or reasonably suspected to be illegal;

4.3.4.   you fail to adhere to the retention period set-out herein;

4.3.5.   an incorrect transaction reference number is used;

4.3.6.   you fail to adhere to the provisions of set-out herein.

4.3.7.   We will advise you if the Transaction is invalid and you hereby agree that we will be entitled to process a Refund in respect of an invalid transaction.

4.3.8.   You agree that we will be entitled to set-off any amount due and payable by you to us in respect of such invalid Mobicred Transaction against any amounts due by us to you.

4.3.9.   Notwithstanding anything to the contrary contained in this PPS Terms, you agree to, upon written demand, pay any amount owing to us in respect of a Mobicred Transaction processed by you.

4.3.10.   We will have no obligation whatsoever to pay you any amount in respect of any illegal Mobicred transaction.

4.4.   Refunds and returns

4.4.1.   All Refunds requests that we receive from you in respect of Mobicred Transactions, will be submitted by us to Mobicred for processing.

4.4.2.   If a Mobicred Payment is Refunded, the value of the Refund may be deducted by Mobicred from the settlement amount due to you in respect of the Mobicred Payments processed by you.

4.4.3.   The value of the Refund should be equal to the value of the initial Mobicred Transactions.

4.4.4.   In the event that you are no longer our customer, there will be no obligation on us to assist you in processing a Refund to a Mobicred Customer.

4.4.5.   You agree, at your own cost and expense, to satisfy all claims and complaints arising in connection with any Mobicred Payment and cause any such claim or complaint that is justified, to be satisfied without any undue delay.

4.4.6.   For Refund requests submitted after 12 months, you must contact Mobicred directly to process such Refund request. You agree that we will not be a party to a refund process after 12 months and that we cannot be held liable for any losses incurred as a result of the processing of the refund.

5.   VOUCHERING

5.1.   The Vouchers can be bought from specific outlets and can used by a Customer for the payment of goods and/or service purchased online from you.

5.2.   We do not take any liability for the validity and settlement of Vouchers.

5.3.   Processing Vouchers

5.3.1.   Upon checkout, a Customer has the option to pay for the goods and/or services purchased from you by using a Voucher.

5.3.2.   Upon selecting to pay using a Voucher, the Customer will be prompted to enter the Voucher number.

5.3.3.   Once the Voucher number is entered, we will route the Voucher Transaction to the applicable Alternative Service Provider for balance enquiry and Voucher verification.

5.3.4.   Once the Voucher has been verified, the Alternative Service Provider will send an OTP to the Voucher holder for Authorization.

5.3.5.   The Customer will enter the OTP and the Voucher Transaction will be approved.

5.3.6.   We will facilitate the Transaction by routing the Transaction to the Alternative Service Provider for authorization and settlement.

5.3.7.   The Alternative Service Provider will settle you directly for the Vouchers redeemed on your website.

6. QR CODE

6.1. By processing QR Code Transactions you agree that you will inform your Customers on how to initiate a payment using a QR Code. To initiate payment using a QR Code, a Customer must scan the QR Code with a banking or QR Code third party mobile application and follow the instructions/prompts on the mobile application.

6.2. Once the QR Code is scanned, the Transaction will be submitted to us for onward submission to the Alternative Service Provider and/or Bank (as applicable), for settlement and approval.

6.3. The Bank will settle you directly for any Transaction processed using the QR Code Solution.

7. BULK CARD COLLECTION SOLUTION

7.1. By using the Bulk Card Collection Solution, you agree:

7.1.1. to enter your Customer's Card number, expiry date and CVV number into the secure online payment page we provide to you as part of the PPS Services;

7.1.2. you have the authority or mandate (by agreement) from your Customer to process a Bulk Card Collection Solution Transaction.

7.1.3. you have obtained Authorisation for the first Transaction in the series of Transactions;

7.1.4. to store the Authorisation of the first Transaction, together with the authority or mandate from your Customer to debit your Customer's account. You will be required to produce this as evidence in the event that your Customer disputes the Transaction;

7.1.5. that subsequent authorisation requests in the recurring series will be processed using the Card on File Solution and processed as a RPI Transactions that will not contain a CVV number.

7.2. Bulk Card Collection Solution Transactions are Card Transactions where the initial Transaction is sent as a normal Card Transaction, containing the following: Card number; reference; start and end date; amount, frequency (daily, weekly, monthly, quarterly, bi-annually, yearly).

7.3. We automatically generate the subsequent Transactions.

7.4. Processing Bulk Card Collection Solution Transactions

7.4.1. The Customer selects to pay for goods and/or services by way of the Bulk Card Collection Solution and proceeds to checkout. You will open a secure payment page, either supplied by the Hosted Payment Page or the Payment Gateway.

7.4.2. The Transaction will be processed in a 3D Secure compliant manner and the Customer will be prompted to insert it OTP in the window provided.

7.4.3. We will route the Transaction to the Bank for authorization.

7.4.4. The Issuing Bank approves/declines the 3DSecure request and sends it back to the Hosted Payment Page, or your payment page when using our Payment Gateway.

7.4.5. Settlement is either initiated by you or is done automatically depending on your settings.

7.4.6. The Bank will settle you directly.

7.5. Card on File Solution

7.5.1. The Card on File Solution provides a Customer the option to pay for goods and/or services purchased from you using the Card on File as a Payment Instrument.

7.6. Processing of Card on File Transactions

7.6.1. The Customer purchases goods and/or services online from you and selects to pay using the Card on File Solution.

7.6.2. The first Transaction must be processed as a standard Real Time Payment with 3D Secure verification.

7.6.3. The Card Token will be returned to you as part of the successful Transaction response message. This token would be required for future Transactions.

7.6.4. Post the initial Transaction, you must assemble a batch file containing multiple Card on File Transactions. These records contain:

7.6.5. Card Token, amount; action date; merchant category code; optional (expiry date, hashed PAN, Transaction description).

7.6.6. Post the submission, a batch ID will be returned to you.

7.6.7. Once the batch file is received, we will route the Transaction to the Bank for approval.

7.6.8. You can view the response received from the Issuing Bank on the Client Portal.

7.6.9. You will be settled directly by the Bank.

C. ALTERNATIVE PAYMENT METHODS

8. TOKENIZATION SOLUTION

8.1. By selecting Tokenization on the Application Form, you agree that you will accept payment for goods and/or services on your website by allowing Customers to pay with a token.

8.2. Once Adumo Online Token is selected, the Transaction will be submitted to us for onward submission to Bank for settlement and approval.

8.3. The Bank will settle you directly for all Tokenised Transactions processed by you.

8.4. Processing Tokenization Transactions

8.4.1. A Customer selects Adumo Online Tokenization upon check out.

8.4.2. We will request the Customer to log in and select the Card it wants to use, or if not previously registered to register the Card.

8.4.3. A 3D Secure verification will be performed on the selected Card if required, and an authentication message will be sent to the Customer.

8.4.4. We will submit the Transaction for authorization and settlement to the Bank.

8.4.5. The Bank will settle you directly for Transactions processed using the Tokenization Solution.

D. LIST OF CARD ASSOCIATIONS, BANKS, THIRD PARTIES AND SERVICE PROVIDERS

- The following table contains a list of third parties and Alternative Service Providers that are used to process the Transactions and enable the Solutions.
- The table below specifies whether you (D) are required to enter into a direct contract with the third party or Alternative Service Provider, or if it is our responsibility to enter into an agreement with the third party or Alternative Service Provider for the provision of the Solution to you.
- If you are required to contract the third party directly, you must enter into an agreement directly with the relevant Alternative Service Provider, or bank and provide us with the Merchant Identifiers (MIDs) to populate in every Transaction.
- Where indicated that we are required to enter into an agreement with the Alternative Service Provider or Bank for the provision of the Solution, the Banks and Alternative Service Providers have duly authorised us to conclude an agreement with you for the acceptance and processing of Solutions offered by them.

Name	Payment Stream	Who completes Application for Services?	Country	Type of Service
ABSA ISO	Payment Instruments acceptance	AO	RSA	Acquiring Bank
ABSA	Payment Instruments acceptance	D	RSA	Acquiring Bank
FNB	Payment Instruments acceptance	D	RSA	Acquiring Bank

Standard Bank	Payment Instruments acceptance	D	RSA	Acquiring Bank
Nedbank	Payment Instruments acceptance	D	RSA	Acquiring Bank
Bank Windhoek	Payment Instruments acceptance	D	Namibia	Acquiring Bank
ABSA Africa	Payment Instruments acceptance	D	Across Africa	Acquiring Bank
Mastercard	Mastercard Payment Instruments	N/A	Worldwide	Card Association
VISA	VISA Payment Instruments	N/A	Worldwide	Card Association
BankServAfrica	Payment Instruments	AO	RSA	3D Secure Service Provider
Cardinal Commerce	Non-RSA Merchant - Card	AO	Rest of Africa	3D Secure Service Provider
American Express & AMEX Safekey	American Express Payment Instruments acceptance	D	Worldwide	Card processor and 3D Secure Service Provider
Diners Club & ProtectBuy	Diners Club Cards	D	Worldwide	Card processor and 3D Secure Service Provider
FinGO Systems (Pty) Ltd	Debit Order Solution	D	RSA	Alternative Service Provider
Mobicred (Pty) Ltd	Mobicred Solution	AO	RSA	Alternative Service Provider
Planet	Multi-Currency Solution	AO	RSA	Alternative Service Provider
Ahead start (Pty) Limited - Callpay	EFT Solution	AO	RSA	Alternative Service Provider
Ozow (Pty) Ltd	EFT Solution	AO	RSA	Alternative Service Provider
Cellulant Kenya Ltd	Mobile Money Solution	AO	Africa	Alternative Service Provider

OTT Mobile Technologies	Voucher Solution	AO	RSA	Alternative Service Provider
Masterpass	QR-Code Solution	D	RSA	Alternative Service Provider
Zapper	QR-Code Solution	D	RSA	Alternative Service Provider