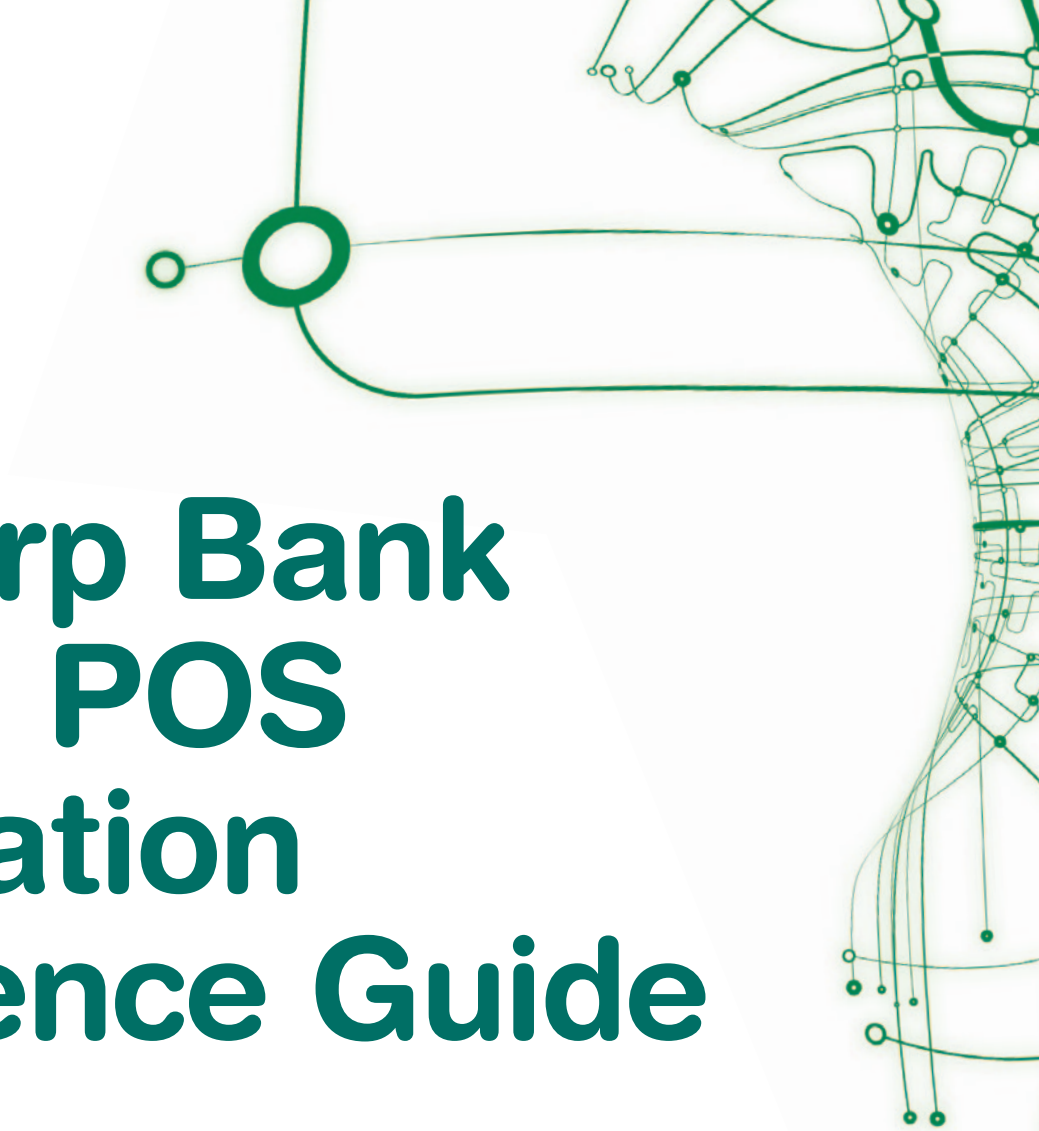


Suncorp Bank Virtual POS Integration Reference Guide

August 2013

SUNCORP BANK
Business

Copyright

License Agreement

Trademarks

Suncorp Bank
GPO Box 1453
Brisbane QLD 4001
Phone 13 11 75
www.suncorpbank.com.au

Contents

About Virtual POS

Suncorp Bank Virtual POS enables merchants to use payment enabled websites, e-commerce or other applications by providing a low effort integration solution. It is suitable for most website hosting environments as merchants can integrate payment capabilities into their application without installing or configuring any payments software.

This guide describes how to payment enable your e-commerce application or online store by using the functionality of the Virtual POS.

It details the basic and supplementary fields for the different types of transactions, and includes additional material such as valid codes, error codes and security guidelines.

Where to Get Help

If you need assistance with Virtual POS integration, please contact your support organisation's help desk, the details of which you will be given once you sign up to the MiGS service via Suncorp Bank.

Basic Transaction Fields

This section describes the commands, field types and valid values for basic transactions in Virtual POS.

Field Types

Virtual POS uses three different types of fields: **Alpha, Alphanumeric** and **Numeric** as described in the table below.

Field Types	Description
Alpha	Alphabetical characters only, in the range **A** to **Z** and **a** to **z** of the base US ASCII characters. The US ASCII ranges for these characters are decimal 65 to 90 inclusive, and decimal 97 to 122 inclusive.
Alphanumeric	Any of the base US ASCII characters in the range decimal 32 to 126, except the | character, decimal 124.
Numeric	Numeric characters only in the range **0** to **9** in the base US ASCII characters. The US ASCII ranges for these characters are decimal 48 to 57 inclusive.

Input Requirements

Virtual POS requires a number of inputs to perform a basic transaction. The values of these inputs are passed from the merchant software into the Payment Server via the Virtual POS interface.

For 3-Party, the appropriate suffix must be appended to the Virtual POS URL, https://migs.mastercard.com.au/

3-Party Payment Model

The 3-Party Payment Model can be only used for payments where a web browser is involved.

- Data is sent via HTTP GET or POST to https://migs.mastercard.com.au/vpcpay
- Supports either HTTP GET or POST requests. POST must be used when sensitive data is present in the request. This includes one or more of the following fields:
- vpc_CardNum
- vpc_CardSecurityCode
- vpc_CardTrack1
- vpc_CardTrack2
- vpc_User
- vpc_Password.

Note: Sensitive data must never form part of the URL for HTTP GET or POST requests. It must always be sent via POST parameters. A failure to conform to this rule will result in a HTTP Response code of 400 (Bad Request), and the transaction will fail to proceed.

Input Fields for Basic 3-Party Transactions

Data is sent from the merchant application to the Payment Server via Virtual POS, a basic transaction requiring a number of data fields as per the table below.

A fully qualified URL (https://migs.mastercard.com.au/vpcpay) must be included in the merchant's application code to send transaction information to the Virtual POS.

Basic 3-Party Input Fields			
The following data fields must be included in a Transaction Request when using a 3-Party transaction.			
Field Name			
Field Description			
Required/Optional	Field Type	Min, Max or Set Field Length	Sample Data
vpc_Version			
The version of Virtual POS API being used. The current version is 1.			
Required	Alphanumeric	1,8	1
vpc_Command			
Indicates the transaction type. This must be equal to 'pay' for 3-Party payment.			
Required	Alphanumeric	1,16	pay
vpc_AccessCode			
Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id. The access code is provided when the merchant profile is registered with Suncorp Bank.			
Required	Alphanumeric	8	6AQ89F3
vpc_MerchTxnRef			
A unique value created by the merchant. **Usage Notes:** The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly. Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt. This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server. **Note**: If "Enforce Unique Merchant Transaction Reference" privilege is enabled by Suncorp Bank, this value must be unique across all the merchant's transactions.			
Required	Alphanumeric	1,40	ORDER958743-1
vpc_Merchant			
The unique Merchant Id assigned to a merchant by Suncorp Bank. The Merchant ID identifies the merchant account against which settlements will be made.			
Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo			
The merchant's identifier used to identify the order on the Payment Server. For example, a shopping cart number, an order number, or an invoice number. This identifier will be displayed in the Transaction Search results in the Merchant Administration portal on the Payment Server. **Note**: if 'Enforce Unique Order Reference" privilege is enabled by Suncorp Bank, this value must be unique across all the merchant's orders.			
Required	Alphanumeric	1,100,34	ORDER958743
vpc_Amount			

Basic 3-Party Input Fields			
The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, $12.50 is expressed as 1250. This value cannot be negative or zero. The maximum valid value is 2147483647.			
Required	Numeric	1,12	1250
vpc_Currency			
The currency of the order expressed as an ISO 4217 alphanumeric code. This field is case-sensitive and must include uppercase characters only.			
Optional	Alpha	3	AUD
vpc_Locale			
Specifies the language used on the Payment Server pages that are displayed to the cardholder, in 3-Party transactions. Please check with Suncorp Bank for the correct value to use.			
Required	Alphanumeric	2,5	en
vpc_ReturnURL			
URL supplied by the merchant in a 3-Party transaction. It is used by the Payment Server to redirect the cardholder's browser back to the merchant's website. The Payment Server sends the encrypted Digital Receipt with this URL for decryption. It must be a fully qualified URL starting with HTTP:// or HTTPS:// and if typed into a browser with Internet access, would take the browser to that web page. It is recommended that the browser is returned to an SSL secured page. This will prevent the browser pop-up indicating that the cardholder is being returned to an unsecure site. If the cardholder clicks 'No' to continue, then neither the merchant nor the cardholder will obtain any receipt details.			
Required	Alphanumeric	1,255	https://merchants_site/receipt.asp
vpc_SecureHash			
A secure hash which allows Virtual POS to authenticate the merchant and check the integrity of the Transaction Request. Secure hash provides better security to merchants than Access Code. For more details see *Generating a Secure Hash* on page 28 and remember to ***always store the Secure Hash secret securely*** (see page 29). **Note**: The secure secret is provided by Suncorp Bank.			
Optional	Alphanumeric	64	9FF46885DCA8563ACFC62058E0FC447BD2C033D505BD8202F681DCAD7CED4DD2
vpc_SecureHashType			
The type of hash algorithm used to generate the secure hash of the Transaction Request and the Transaction Response. It is strongly recommended that you generate your secure hash using SHA256 HMAC, in which case vpc_SecureHashType=SHA256 For more details see *Generating a Secure Hash* on page 28.			
Optional	Alphanumeric	6	SHA256
vpc_ReturnAuthResponseData			
Specifies whether the authorisation response data must be included in the Transaction Response. Valid values for this field are: Y - indicates that the authorisation response data may be included in the Transaction Response, depending on the card type and acquirer used. N - indicates that the authorisation response data must not be included in the Transaction Response. This is the default value. For information on authorisation response data, see *Authorisation Response Data* on page 35.			
Optional	Alpha	1	Y

Basic Output Fields

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

Terminology: Returned Input fields are shown as "Input" in the table.

Basic Output Fields			
The following data fields must be included in a Transaction Request for 3-Party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data
vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_MerchTxnRef			
The value of the vpc_MerchTxnRef input field returned in the Transaction Response. This field may not be returned in a transaction that fails due to an error condition.			
Input	Alphanumeric	0,40	ORDER958743-1
vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo			
The value of the vpc_OrderInfo input field returned in the Transaction Response.			
Input	Alphanumeric	1,34	ORDER958743
vpc_Amount			
The value of the vpc_Amount input field returned in the Transaction Response.			
Input	Numeric	1,10	1250
vpc_Currency			
The value of the vpc_Currency input field returned in the Transaction Response. This field is returned only if vpc_Currency was included in the Transaction Request.			
Input	Alpha	3	AUD
vpc_Message			
This is a message to indicate what sort of errors the transaction encountered.			
Output	Alphanumeric	10,255	Merchant [TESTCORE23] does not exist.
vpc_TxnResponseCode			
A response code that is generated by the Payment Server to indicate the status of the transaction. A vpc_TxnResponseCode of “0” (zero) indicates that the transaction was processed successfully and approved by the acquiring bank. Any other value indicates that the transaction was declined (it went through to the banking network) or the transaction failed (it never made it to the banking network). For a list of values, see page 30.			
Output	Alphanumeric	1	0
vpc_ReceiptNo			
A unique identifier that is also known as the Reference Retrieval Number (RRN). The vpc_ReceiptNo may be passed back to the cardholder for their records if the merchant application does not generate its own receipt number. This field is not returned for transactions that result in an error condition.			
Output	Alphanumeric	0,12	012413207163

Basic Output Fields			
vpc_AcqResponseCode			
Generated by the financial institution to indicate the status of the transaction. The results can vary between institutions so it is advisable to use the vpc_TxnResponseCode as it is consistent across all acquirers. It is only included for fault finding purposes. Most Payment Providers return the vpc_AcqResponseCode as a 2-digit response. This field is not returned for transactions that result in an error condition.			
Output	Alphanumeric	2,3	00
vpc_TransactionNo			
Payment Server OrderID (or Shopping Transaction Number) is a unique number generated by the Payment Server for every transaction. It is important to ensure that the TransactionNo is stored for later retrieval. It is used in Merchant Administration and Advanced Merchant Administration as a reference to perform refund, capture and void transactions. This field is not returned for transactions that result in an error condition.			
Output	Numeric	1,19	96841
vpc_BatchNo			
A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with for settlement. It is typically a date in the format YYYYMMDD. This field will not be returned if the transaction fails due to an error condition.			
Output	Numeric	0,8	20110105
vpc_AuthorizeId			
Authorisation Identification Code issued by the Acquirer to approve or deny a transaction. This field is 6-digits maximum and is not returned for transactions that are declined or fail due to an error condition.			
Output	Alphanumeric	0,6	654321
vpc_Card			
Identifies the card type used for the transaction. For a list of card types see *Card Type Code* on page 33. This field is not returned for transactions that result in an error condition.			
Output	Alpha	0,2	MC
vpc_SecureHash			
Allows the merchant application to check the integrity of the returning Transaction Response. ***Always store the Secure Hash secret securely*** (see *Generating a Secure Hash* on page 28).			
Output	Alphanumeric	64	9FF46885DCA8563ACFC620 58E0FC447BD2C033D505B D8202F681DCAD7CED4DD2
vpc_SecureHashType			
The value of vpc_SecureHashType returned in the Transaction Response.			
Input	Alphanumeric	6	SHA256
vpc_CardNum			
The card number in 0.4 card masking format. This field is only returned if **System-Captured Masked Card in Digital Receipt** privilege is enabled for the merchant processing the transaction. See **Suncorp Bank Merchant Manager Administration User Guide.**			
Output	Alphanumeric Special	5	-1234
vpc_ReturnACI			
The ACI (Authorisation Characteristics Indicator) returned by the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	1	N

Basic Output Fields			
vpc_TransactionIdentifier			
The unique identifier for the transaction returned by the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	0, 19	ABC187659DEFGJ0
vpc_CommercialCardIndicator			
Indicates the type of commercial card as returned by the card issuer. For information, see *Authorisation Response Code* on page 35. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	1	B
vpc_CommercialCard			
Indicates if the card used is a commercial card. For more information, see *Authorisation Response Code* on page 35. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	1	Y
vpc_CardLevelIndicator			
Indicates the card level result returned by the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	2	A [Character "A" followed by a space]
vpc_FinancialNetworkCode			
Indicates the code of the financial network that was used to process the transaction with the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	0,3	MCC
vpc_MarketSpecificData			
Indicates the market or the industry associated with the payment. For example, B and H may indicate "bill payment" and "hotel" respectively depending on the acquirer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	0,1	A

Supplementary Transaction Fields

The following sections detail the additional functionality available to merchants. The basic fields for 3-Party transactions are used with the extra fields detailed in these sections.

Most functionality is available to 3-Party transactions. Functionality limited to 3-Party transactions is designated as such in the details.

Note: While these are supplementary fields, some of these fields may be mandatory for certain functions.

Card Security Code (CSC) Field

The Card Security Code (CSC) is a security feature for card not present transactions. It is also known as also known as CVV (Visa), CVC2 (MasterCard), CID/4DBC (Amex), or CVV2.

It compares the Card Security Code on the card with the records held in the card issuer's database. For example, on Visa and MasterCard credit cards, it is the three digit value printed on the signature panel on the back following the credit card account number. For American Express, the number is the 4 digit value printed on the front above the credit card account number.

Once the transaction is successfully processed and authorised, the card issuer returns a result code (CSC result code) in its authorisation response message. This verifies the CSC level of accuracy used to match the card security code.

In a standard 3-Party transaction, the merchant does not have to send the Card Security Code as the Payment Server prompts the cardholder for the information.

Enhanced Industry Data Fields

Although Enhanced Industry Data functionality was originally designed for the travel industry, this functionality allows the merchant to enter any industry related data to be stored on the Payment Server for that transaction. It includes fields:

- Ticket Number — allows the merchant to submit airline ticket number in the Transaction Request, including Capture transactions. The previous ticket number is overwritten when a new ticket number is submitted. The Payment Server does not maintain an audit record of these changes. You can view the latest ticket number in the search results of a Transaction Search using the Merchant Administration portal on the Payment Server.
- Addendum Data — allows the merchant to include industry specific data in the Transaction Request. The data can include passenger names, ticket numbers, hotel bookings, etc. The addendum data is stored in the database, which may be used in creating reports external to the Payment Server.

Both Ticket Number and Addendum Data are passed with the Transaction Request and stored on the Payment Server. The ticket number is passed to the financial institution as part of certain transactions.

Transaction Request Input Fields

Enhanced Industry Data Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/Optional	Field Type	Min, Max or Set Field Length	Sample Data
vpc_TicketNo			
The airline ticket number that is passed with the Transaction Request and stored on the Payment Server.			
Optional	Alphanumeric	0,15	A234567F
vpc_AddendumData			
Extra information about the industry, for example, passenger names, ticket numbers, hotel bookings, etc., that is passed with the Transaction Request and stored on the Payment Server. **Prerequisite**: You must enable the privilege **May Include Addendum Data** to pass Addendum data in the Transaction Request. **Note**: Though vpc_AddendumData supports 2048 characters, ensure that the Transaction Request does not exceed 2048 characters due to browser redirect limitations in 3-Party transactions.			
Optional	Alphanumeric Special	0, 2048	Scott Adam, VIP Client, Acme Hotel.

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Referral Message Fields

This response message occurs when the Acquirer needs to manually authorise the cardholder (by having the merchant contact them) as indicated by a **vpc_TxnResponseCode 'E'.** See Transaction Response Codes.

Transaction Request Input Fields

There are no supplementary input fields in the Transaction Request.

Transaction Response Output Fields

Card Present Output Fields			
In addition to the standard output fields, the following optional field is also returned in the Transaction Response.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AcquirerResponseAdvice			
Referral Message: This field is only present if vpc_TxnResponseCode is 'E'. See *Returned Response Codes* on page 30. This field is the referral message from the issuer. It may contain contact details to allow the merchant to contact the issuer directly to seek authorisation for the transaction. If Authorised the card company will provide a Manual Auth ID code that is input into the payment system using a **'Referral Transaction'**.			
Output	Alphanumeric	0,70	Please call John Doe at BankXYZ on 18004159896

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Payment Authentication

Payment Authentications are designed to reduce credit card fraud by authenticating cardholders when performing transactions over the Internet by using the 3-Domain Secure™ (3-D Secure or 3DS) protocol developed by Visa.

A 3-D Secure transaction is performed immediately before a merchant performs a payment transaction, that is, an Authorisation transaction in the Auth/Capture mode, or a Purchase transaction in the Purchase mode. Authentication ensures that the card is being used by its legitimate owner.

During a transaction, 3DS authentication allows the merchant to authenticate the cardholder by redirecting them to their card issuer where they enter a previously registered password.

Merchants using 3DS can be configured to block any transaction that fails 3DS authentication. A transaction is considered to fail 3DS authentication if it results in a Verification Security Level of '07'. A blocked transaction results in a Dialect Response Code of 'B', which is included in the DR and displayed in the Financial Transaction Details page.

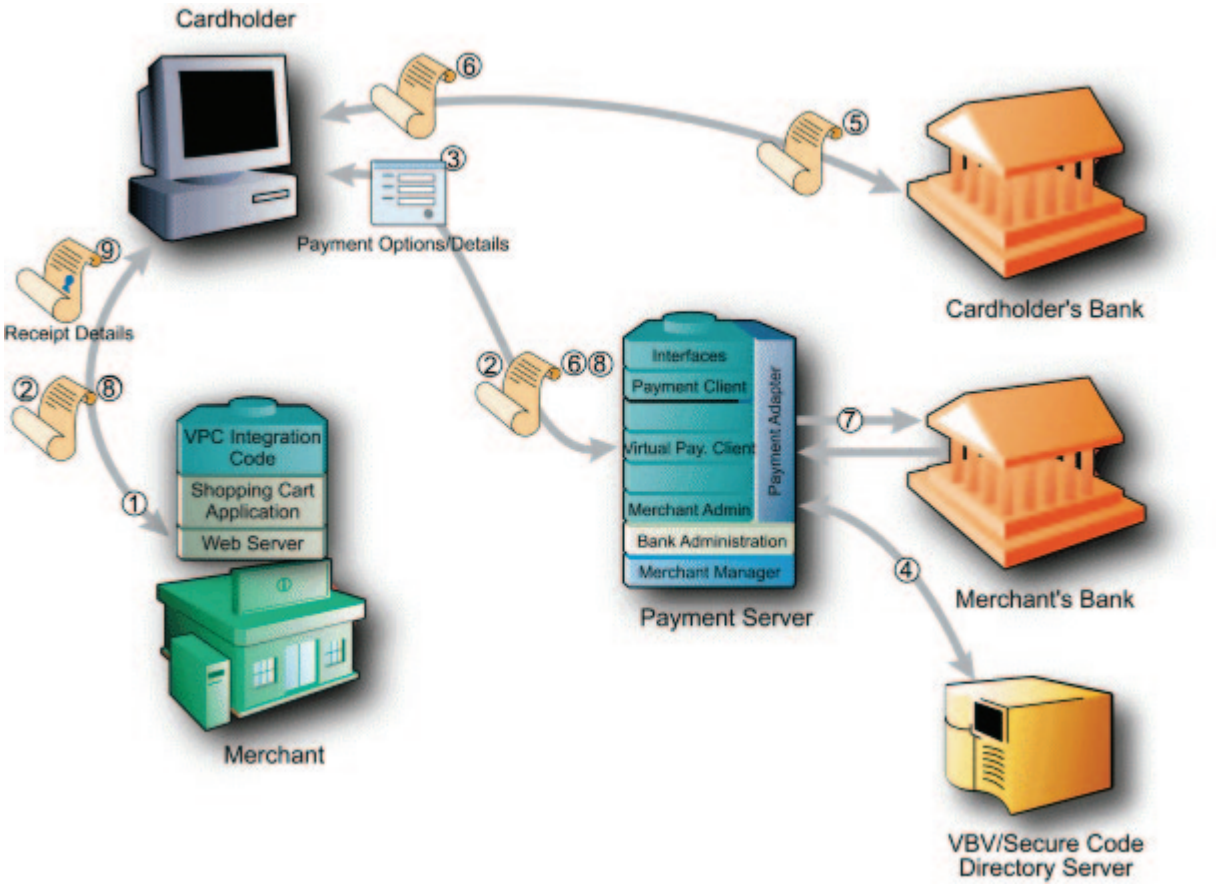
Note: For 3DS Authentication to take place, the cardholder's browser has to be redirected to their card issuing bank where they enter their secret password. This is performed by the Payment Server if the cardholder is enrolled in the 3DS schemes of Verified by Visa™, MasterCard® SecureCode™ or JCB J/Secure™.

Payment Authentication 3-D Secure transaction modes

- **Combined 3-Party Authentication and Payment transaction** - The merchant uses the Payment Server to perform the authentication and payment in the one transaction.

The **Payment Server collects the cardholder's card details** and not the merchant's application. The Payment Server redirects the cardholder to the card issuing institution to enter their 3-D Secure password. If the Authentication is performed correctly the Payment Server uses the Authentication information to perform the payment transaction.

Information Flow of a 3-D Secure Authentication/Payment transaction



If you have been enabled to use Verified by Visa, MasterCard SecureCode or JCB J/Secure, the information flow where the Payment Server collects the card details is as follows:

1 A cardholder browses the application, selects a product and enters their shipping details into the merchant's application at the checkout page.

2 The cardholder clicks a pay button and your application sends the payment Transaction Request to the Payment Server by redirecting the cardholder's Internet browser to the Payment Server.

3 The Payment Server prompts the cardholder for the card details.

4 If the card is a Visa, MasterCard or JCB card, the Payment Server then checks with the Directory Server to determine if the card is enrolled in either the Verified by VisaTM (Visa 3-Domain Secure), MasterCard® SecureCodeTM (MasterCard 3 Domain Secure) or JCB J/SecureTM (JCB 3-Domain Secure) scheme.

If the card is not enrolled in a payment authentication scheme then go to Step 7.

5 If the cardholder's card is registered in the payment authentication scheme, the Payment Server redirects the cardholder's browser to the card issuer's site for authentication. The card issuer's server displays the cardholder's secret message and the cardholder enters their secret password, which is checked against the Issuing bank's database.

6 At the completion of the authentication stage, the cardholder is redirected back to the Payment Server indicating whether or not the cardholder's password matched the password in the database.

If the cardholder was not authenticated correctly, then the payment does not take place and the cardholder is redirected back to the merchant's site with a Transaction Response containing details to indicate the authentication failed – see step 8.

7 If the cardholder was authenticated correctly, or Payment Authentication did not occur the Payment Server continues with processing the transaction with the results of the authentication attempt.

8 The Payment Server then redirects the cardholder back to merchant's site with the Transaction Response. The Transaction Response contains the result of the transaction.

9 The application processes the Transaction Response and displays the receipt.

Note: If the cardholder is enrolled in the 3-D Secure scheme but is not authenticated correctly, for example, because the cardholder may have entered their password incorrectly 3 times, then the merchant's application is sent a **vpc_TxnResponseCode** code of 'F' to indicate the cardholder failed the authentication process and the transaction does not proceed.

3-Party Authentication & Payment Transaction: (Payment Server collects card details)

The 3-Party Authentication and Payment transaction mode uses the basic 3 Party style of transaction.

Transaction Request Input Fields

There are no additional input fields in the Transaction Request to add 3-D Secure authentication to a standard 3-Party transaction.

Transaction Response Outputs

The outputs from this transaction type are as follows.

Payment Authentication Output Fields			
In addition to the standard output fields, the following fields are also returned in the Transaction Response for this 3-Party transaction.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data
vpc_3DSECI			
The 3-D Secure Electronic Commerce Indicator, which is set to '05' when the cardholder authenticates OK, and '06' when the cardholder is not enrolled. (These values may change depending on the locale or issuer). For AMEX SafeKey, an ECI value is only returned if the ACS returns a PARes value. For all other SafeKey cases, the field is not returned.			
Output	Numeric	0,2	06
vpc_3DSXID			
It is a unique transaction identifier that is generated by the Payment Server on behalf of the merchant to identify the 3DS transaction. It is a 20-byte field that is Base64 encoded to produce a 28-character value.			
Output	Alphanumeric	0,28	uyPfGlgsoFQhklklsto+IFWs92s=
vpc_3DSenrolled			
This field indicates if the card is within an enrolled range. This is the value of the VERes.enrolled field. It will take values (**Y** - Yes, **N** - No, **U** - Unavailable for Checking).			
Output	Alpha	1	N
vpc_3DSstatus			
This field is only included if payment authentication was attempted and a PARes was received by the MPI. It will take values (**Y** - Yes, **N** - No, **A** - Attempted Authentication, **U** - Unavailable for Checking).			
Output	Alpha	0,1	N
vpc_VerToken			
This value is generated by the card issuer as a token to prove that the cardholder authenticated OK. This is a base64 encoded value.			
Output	Alphanumeric	28	gIGCg4SFhoeliYqLjI2Oj5CRkpM=
vpc_VerType			
This field will either be '**3DS**' 3-D Secure incorporating Verified by Visa, MasterCard SecureCode and JCB J/Secure, or '**SPA**' - Secure Payment Authentication from MasterCard (rarely used).			
Output	Alphanumeric	0,3	3DS
vpc_VerSecurityLevel			

Payment Authentication Output Fields			
The Verification Security Level is generated at the card issuer as a token to prove that the cardholder was enrolled and authenticated OK. It is shown for all transactions except those with authentication status “Failure”. This field contains the security level to be used in the AUTH message. MasterCard '**0**' - Merchant not participating (a merchant will not see this if they are configured for MasterCard SecureCode). MasterCard '**1**' - Cardholder not participating MasterCard '**2**' - Cardholder authenticated. Visa '**05**' - Fully authenticated. Visa '**06**' - Not authenticated, (cardholder not participating). Visa '**07**' - Not authenticated. Usually due to a system problem, for example the merchant password is invalid. American Express ‘**05**’ – Fully authenticated. American Express ‘**06**’ – Not authenticated (card is enrolled but authentication failed). American Express ‘**07**’ – Not authenticated. For SafeKey,07 is only returned if the ACS returns a PARes status of ‘U’; otherwise no ECI value is returned.			
Output	Numeric	0,2	06
vpc_VerStatus			
The status codes used by the Payment Server to show whether the payment authentication was successful or not (see *Verified by Visa™, MasterCard® SecureCode™ and JCB* J/Secure™ Status *Codes on page 34*).			
Output	Alphanumeric	1	N

Advanced Merchant Administration (AMA) Transactions

Advanced Merchant Administration (AMA) is used when the volume of transactions is too great to be economically viable or too difficult to be carried out manually. AMA transactions allow the merchant to incorporate additional features such as refunds, into the merchant system.

Capture, Refund, Void Capture, Void Refund and Void Purchase return standard output fields, plus a comma (',') delimited result string containing a host of other data.

Note: Some financial institutions do not support voids.

Merchants and users who need AMA transactions must have a username and password; in addition, they must be set up with the appropriate AMA privileges to perform a particular AMA transaction.

Note: An AMA user cannot be used for Merchant Administration operations.

Basic Input Fields - AMA Transaction

Data is sent from the merchant application to the Payment Server via the Virtual POS. A basic transaction requires a number of data fields as per the table below.

The fields are sent to a fully qualified URL (https://migs.mastercard.com.au/vpcdps) via a HTTP POST operation. This URL must be included in the merchant's application code to send transaction information to Virtual POS.

AMA Input Fields			
Field Name			
Field Description			
Required/Optional	Field Type	Min, Max or Set Field Length	Sample Data
vpc_Version			
The version of the Virtual POS API being used. The current version is 1.			
Required	Alphanumeric	1,8	1
vpc_AccessCode			
Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id. The access code is provided when the merchant profile is registered with a Payment Provider.			
Required	Alphanumeric	8	6AQ89F3
vpc_MerchTxnRef			
A unique value created by the merchant. **Usage Notes**: The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing transaction receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly. Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt. This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server. **Note**: If "Enforce Unique Merchant Transaction Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's transactions.			
Required	Alphanumeric	1,40	ORDER958743-1

AMA Input Fields			
vpc_Merchant			
The unique Merchant Id assigned to a merchant by the Payment Provider. The Merchant ID identifies the merchant account against which settlements will be made.			
Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_TransNo			
This is the unique Payment Server OrderID (Shopping Transaction) number generated by the Payment Server for the initial transaction.			
Required	Numeric	1,19	10712
vpc_User			
The user name of the user who is performing the AMA transaction. Each AMA User name may be assigned different privileges to perform particular functions. For example, an AMA User can be set to only perform refunds. **Note**: An AMA user cannot be used for Merchant Administration operations.			
Required	Alphanumeric	1,20	Maryellen
vpc_Password			
The password used by the merchant to authorise Advanced Merchant Administration transactions. It must be at least 8 characters long and contain at least one non-alphabetical character.			
Required	Alphanumeric	8,25	T1m34t*A

Basic Output Fields - AMA Transaction

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

Note: The Transaction Response provided by the Payment Server may contain other fields that are not documented in this guide. Such fields may be changed, added, or removed without notice, and must NOT be relied upon by merchant integrations.

Terminology: Returned Input fields are shown as "Input" in the table.

AMA Output Fields			
The following data fields are returned in the Transaction Response.			
Field Name			
Field Description			
Required/Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Version			
The version of the Virtual POS API being used. The current version is 1.			
Input	Alphanumeric	1,8	1
vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_Locale			
Specifies the language used on the Payment Server based on the merchant configuration.			
Input	Alpha	2,5	en
vpc_MerchTxnRef			
The value of the vpc_MerchTxnRef input field returned in the Transaction Response. This field may not be returned in a transaction that fails due to an error condition.			
Input	Alphanumeric	0,40	ORDER958743-1

AMA Output Fields			
vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_Message			
This is a message to indicate what sort of errors the transaction encountered. This field is not provided if vpc_TxnResponseCode has a value of zero.			
Output	Alphanumeric	1,255	Merchant [TESTCORE23] does not exist.
vpc_TxnResponseCode			
A response code that is generated by the Payment Server to indicate the status of the transaction. A vpc_TxnResponseCode of "0" (zero) indicates that the transaction was processed successfully and approved by the acquiring bank. Any other value indicates that the transaction was declined (it went through to the banking network) or the transaction failed (it never made it to the banking network). For a list of values, see *Returned Response Codes* on page 30.			
Output	Alphanumeric	1	0
vpc_AcqResponseCode			
Generated by the financial institution to indicate the status of the transaction. The results can vary between institutions so it is advisable to use the vpc_TxnResponseCode as it is consistent across all acquirers. It is only included for fault finding purposes. Most Payment Providers return the vpc_AcqResponseCode as a 2-digit response; others return it as a 3-digit response. This field is not returned for transactions that result in an error condition.			
Output	Alphanumeric	2,3	00
vpc_TransactionNo			
Financial Transaction Number is a unique number generated by the Payment Server for this transaction. This field will not be returned if the transaction failed due to an error condition.			
Output	Numeric	1,19	96841
vpc_BatchNo			
A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with. Batches of transactions are settled by the acquirer at intervals determined by them. This is an acquirer specific field, for example, it could be a date in the format YYYYMMDD. This field will not be returned if the transaction fails due to an error condition.			
Output	Numeric	0,8	20110105
vpc_AuthorizeId			
Authorisation Identification Code issued by the Acquirer to indicate the approval of a transaction. This field is 6-digits maximum and is not returned for transactions that are declined or fail due to an error condition. **Note**: This field may or may not be returned for some acquirers or combination of transactions even if the transaction is successful.			
Output	Alphanumeric	0,6	654321
vpc_ReceiptNo			
A unique identifier that is also known as the Reference Retrieval Number (RRN). The vpc_ReceiptNo may be passed back to the cardholder for their records if the merchant application does not generate its own receipt number. This field is not returned for transactions that result in an error condition.			
Output	Alphanumeric	0,12	RP12345

AMA Output Fields			
vpc_Amount			
The value of the vpc_Amount input field returned in the Transaction Response. For Void transactions, vpc_Amount indicates the amount associated with the Order to be voided.			
Input	Numeric	1,10	1250
vpc_Card			
Identifies the card type used for the transaction. For a list of card types see *Card Type Codes* on page 33. This field is not returned for transactions that result in an error condition.			
Output	Alpha	0,2	MC
vpc_Currency			
The value of the vpc_Currency input field returned in the Transaction Response. This field is returned only if vpc_Currency was included in the Transaction Request.			
Input	Alpha	3	AUD
vpc_ShopTransactionNo			
This is the unique Payment Server Order Number (Shopping Transaction Number) generated by the Payment Server for the initial transaction.			
Input	Numeric	0,19	96841
vpc_TicketNumber			
The ticket number was originally aimed at the airline industry, however it can be used for any relevant information about this transaction you want stored. The ticket number is stored on the Payment Server database for that transaction and returned in the Transaction Response for capture transactions. This field is only returned if <Input_TicketNumber> was supplied in the initial transaction.			
Output	Alphanumeric	0,15	VIP Client
vpc_AcqResponseText			
The response from the acquirer in the text form. This field is used instead of vpc_AcqResponseCode for acquirers that return text instead of a single code.			
Optional	Alphanumeric	0,255	Success : Pending: Authorisation
vpc_TerminalID			
Specifies the terminal ID used to process the transaction with the acquirer.			
Optional	Alphanumeric	4,8	123456

AMA Capture Transaction

The AMA Capture command allows a merchant to capture the funds from a previous authorisation transaction.

Transaction Request Input Fields

Capture Input Fields			
The following additional data fields must be included in a Transaction Request when performing a Capture transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to 'capture' for a capture transaction.			
Required	Alphanumeric	1,16	capture
vpc_Amount			
The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, $12.50 is expressed as 1250. This value cannot be negative or zero. The maximum valid value is 2147483647.			
Required	Numeric	1,12	1250
vpc_Currency			
The currency of the order expressed as an ISO 4217 alpha code. This field is case-sensitive and must include uppercase characters only. This value must match the currency of the existing order that is being identified by vpc_TransNo.			
Output	Alpha	3	AUD

Transaction Response Output Fields

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

AMA Output Fields			
The following additional data fields are returned in a Transaction Response for standard transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	1,10	1295

AMA Refund Transaction

AMA Refund allows you to refund funds for a previous purchase or capture transaction from the merchant's account back to the cardholder's account.

Transaction Request Input Fields

Refund Input Fields			
The following additional fields must be included in a Transaction Request when performing a Refund transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data
vpc_Command			
Indicates the transaction type. This must be equal to '**refund**' for a refund transaction.			
Required	Alphanumeric	1,16	refund
vpc_Amount			
The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, $12.50 is expressed as 1250. This value cannot be negative or zero. The maximum valid value is 2147483647.			
Required	Numeric	1,12	1250
vpc_Currency			
The currency of the order expressed as an ISO 4217 alpha code. This field is case-sensitive and must include uppercase characters only. This value must match the currency of the existing order that is being identified by vpc_TransNo.			
Optional	Alpha	3	AUD

Transaction Response Output Fields

AMA Output Fields			
The following additional data fields are returned in a Transaction Response for standard transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data
vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	1,10	1295

AMA Void Capture Transaction

AMA Void Capture allows a merchant to void the funds from a previous capture transaction in Auth/Capture mode that has not been processed by the acquiring institution.

Transaction Request Input Fields

Void Capture Input Fields			
The following additional data fields must be included in a Transaction Request when using for a Void Capture transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**voidCapture**' for a void capture transaction.			
Required	Alphanumeric	1,16	voidCapture
vpc_Currency			
The currency of the order expressed as an ISO 4217 alpha code. This field is case-sensitive and must include uppercase characters only. This value must match the currency of the existing order that is being identified by vpc_TransNo.			
Optional	Alpha	3	AUD

Transaction Request Output Fields

AMA Output Fields			
The following additional data fields are returned in a Transaction Response for Void Capture transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	1,10	1295

AMA Void Purchase Transaction

AMA Void Purchase allows a purchase merchant to void a purchase transaction that has not been processed by the acquiring institution. It is not available for Auth/Capture mode merchants.

Transaction Request Input Fields

Void Purchase Input Fields			
The following additional data fields must be included in a Transaction Request when using for a Void Purchase transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to 'voidPurchase' for this transaction type.			
Required	Alphanumeric	1,16	voidPurchase
vpc_Currency			
The currency of the order expressed as an ISO 4217 alpha code. This field is case-sensitive and must include uppercase characters only. This value must match the currency of the existing order that is being identified by vpc_TransNo.			
Optional	Alpha	3	AUD

Transaction Response Output Fields

Void Purchase Input Fields			
The following additional data fields are returned in a Transaction Response for Void Purchase transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual POS.			
Output	Numeric	1,10	1295

AMA QueryDR

The AMA QueryDR command allows a merchant to search for the current or the most recent transaction receipt. It also queries for unknown transactions (a transaction request for which a response was never received) and failed transactions.

The search is performed on the key - **vpc_MerchTxnRef**, so the **vpc_MerchTxnRef** field must be a unique value.

If more than one Transaction Response exists with the same **vpc_MerchTxnRef**, the most recent Transaction Response is returned. For QueryDR to return the current transaction, the transaction response code of the original Transaction Response must be "P-Pending" or "M-Submitted".

If you want to use QueryDR to return digital receipts, it must be done in under five days or no results matching the criteria will be returned. This is because the database only contains data up to five days old.

Transaction Request Input Fields

QueryDR Input Fields			
The following additional data fields must be included in a Transaction Request when using a QueryDR check.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**queryDR**' for a QueryDR function.			
Required	Alphanumeric	1,16	queryDR

Transaction Response Output Fields

A QueryDR can be performed on a base transaction, or on AMA transactions such as a Capture, Refund or Void. Both of these transaction types return different fields.

QueryDR Output Fields			
The following additional data fields are returned in a Transaction Response for a QueryDR transaction.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_DRExists			
This key is used to determine if the QueryDR command returned any search results. If the value is “Y”, there is one transaction with a MerchTxnRef number that matched the search criteria. If the value is “N”, then there is no matching MerchTxnRef number result for the search criteria.			
Output	Alpha	1	Y
vpc_FoundMultipleDRs			
This is used after the previous command to determine if there are multiple results. If the value is “Y”, there are multiple transactions with the MerchTxnRef number that matches the search criteria. If the value is “N”, there could be zero or at most, one transaction with the MerchTxnRef number that matches the search criteria.			
Output	Alpha	1	N
If an original receipt exists, the QueryDR will return all the *Basic Output Fields - AMA Transaction* on page 18 in addition to vpc_DRExists and vpc_FoundMultipleDRs. If the transaction to be queried is a subsequent or AMA transaction such as Capture, Refund, or Void then the following additional fields are returned.			
vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual POS.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual POS.			

QueryDR Output Fields			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual POS.			
Output	Numeric	1,10	1295
If an original receipt doesn't exist, the QueryDR will return the following fields in addition to vpc_DRExists and vpc_FoundMultipleDRs.			
vpc_Version			
The version of the Virtual POS API being used. The current version is 1.			
Input	Alphanumeric	1,8	1
vpc_Amount			
The value of the vpc_Amount input field returned in the Transaction Response.			
Input	Numeric	1,10	1250
vpc_BatchNo			
A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with. Batches of transactions are settled by the acquirer at intervals determined by them. This is an acquirer specific field, for example, it could be a date in the format YYYYMMDD. This field will not be returned if the transaction fails due to an error condition.			
Output	Numeric	0,8	20110105
vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_Locale			
The value of the vpc_Locale input field returned in the Transaction Response.			
Input	Alpha	2,5	en
vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_TransactionNo			
Financial Transaction Number is a unique number generated by the Payment Server for this transaction. This field will not be returned if the transaction failed due to an error condition.			
Output	Numeric	1,19	96841

Generating a Secure Hash

Note: Although the vpc_SecureHashType field is denoted as 'optional', new merchant integrations are required to generate a secure hash using the SHA-256 HMAC algorithm.

Creating a SHA-256 HMAC Secure Hash

The merchant code creates the Secure Hash value on the Transaction Request data. The Payment Server creates another Secure Hash value and sends it back to the merchant in the Transaction Response.

The Secure Hash is a hexadecimal encoded SHA-256 HMAC of a concatenation of VPC and User Defined parameters. The concatenation of parameters takes the form of a set of name-value pairs, similar to the parameter string for an HTTP GET call.

Merchant Supplied Parameters

For information that you want to return to your integration in the Transaction Response, you may either:

- Include it in an appropriate VPC parameter such as vpc_MerchTxnRef field or vpc_ReturnURL in the Transaction Request;
- Provide User Defined parameters in the Transaction Request. User Defined parameters are identified by having a parameter name starting with "user_". These fields should be used in the SHA-256 HMAC calculation;
- Provide other Merchant Supplied parameters. Other Merchant Supplied parameters (that do not begin with "user_") are not included in the SHA-256 HMAC calculation.

Note: All field names are restricted to the character set defined by the regular expression [A Z, a z, 0 9]. Currently, merchant-supplied parameters are supported by 3-Party integrations only.

SHA-256 HMAC Calculation

The SHA-256 HMAC is calculated as follows:

1. The SHA-256 HMAC calculation includes all VPC and User Defined fields, that is, all fields beginning with "vpc_" and "user_", except the vpc_SecureHash and vpc_SecureHashType parameters.

   The field names are sorted in ascending of parameter name. Specifically, the sort order is:

- Ascending order of parameter name using the ASCII collating sequence, for example, "Card" comes before "card"
- Where one string is an exact substring of another, the smaller string should be ordered before the longer, for example, "Card" should come before "CardNum".

2. Construct a string by concatenating the string form of the sorted field name-value pairs. The string form of a name-value pair is the name followed by the value.

- The field name and the value in each field name-value pair are joined using "=" as the separator.
- The resulting joined field name-value pairs are themselves joined using "&" as the separator.

3. Create a SHA-256 HMAC of the resultant string using the hex decoded value of your merchant secret as the key. The SHA-256 HMAC algorithm is defined in Federal Information Processing Standard 180-2. We strongly recommend that you use one of the numerous implementations available in most programming languages.

Note: It is critical that you use the hex decoded value of the secret as the key. For example, in PHP you can use the pack ('H*',SecureSecret) function. In C# you will need to create and parse a byte array as demonstrated in the example code.

4. Encode the HMAC in hexadecimal, and include it in the request as the value for the vpc_SecureHash field.

   For example, if your merchant secret is: BB48A64077A1CBF08FF0D91C5A9FE42B

   and the Transaction Request includes only the following parameters:

Field Name	Example Value
vpc_Version	2
vpc_Command	pay
vpc_MerchTxnRef	txn 1
vpc_CardNum	345678901234564
vpc_CardExp	1705
vpc_Merchant	TESTMERCHANT
vpc_AccessCode	75A6GH9
vpc_Amount	1000
user_SessionId	567890

The concatenated value is as follows:

```
user_SessionId=567890&vpc_AccessCode=75A6GH9&vpc_Amount=1000&vpc_CardExp=1705&vpc_CardNum=345678901234564&vpc_
Command=pay&vpc_MerchTxnRef=txn1&vpc_Merchant=TNSITESTMERCHANT&vpc_Version=1
```

Note: The last character of each field value (other than the last) is followed directly by "&". The concatenated value must be represented in the UTF-8 character encoding format.

Note: The values in all name value pairs should not be URL encoded for the purpose of hashing.

The Secure Hash value is:

```
3812B7C7D21726AAC9633E1D42BD43A73A329F8906C248EFAF9CEC354F8B0C08
```

and the resultant Request is (note the Secure Hash and Secure Hash Type fields):

```
user_SessionId=567890&vpc_AccessCode=75A6GH9&vpc_Amount=1000&vpc_CardExp=1705&vpc_CardNum=345678901234564&vpc_
Command=pay&vpc_MerchTxnRef=txn1&vpc_Merchant=TNSITESTMERCHANT&vpc_Version=1&vpc_SecureHash=7C6866D0B1DF14FE03FA
4168F3328C2D33E192E7CA5D08F5D4533F044A866D41&vpc_SecureHashType=SHA256
```

Note: Non-VPC fields (fields that do not begin with "vpc_") are returned ONLY for 3-Party integrations.

In the Transaction Response,
- the values for these fields cannot exceed 255 characters

- the maximum number of fields returned is 5

- the maximum length of the response string in the URL is 2048 characters.

The Payment Server also includes the vpc_SecureHash in the Transaction Response so you can check the integrity of the receipt data. You do this by calculating the secure hash using the above method, then comparing your calculation with the value you received from the Payment Server. If the values match, then you can be assured that we received the data you sent, and you received the data we sent.

Secure Hash Matching Error

Our Secure Hash method provides very good detection of attempts at fraud. However it is your responsibility to keep the key secret and to check the response. If the calculated and received values of the secure hash do not match, then you are at serious risk of eShoplifting. That is, providing your goods or service without being paid.

This could be due to:

- Fraud by your customer;
- Fraud by a man-in-the-middle attack (you are especially vulnerable to this if you do not use SSL between the customer's browser and your website);
- Malicious corruption of the customer's web browser or computer.

It is extremely unlikely that the reason was corruption by the network. There is only a very small chance that a network packet will be corrupted and not corrected by the IP or TCP protocols.

Therefore you should take secure hash errors seriously, and when detected, take action that you think is appropriate to protect your business.

To simplify the calculation, the fields in the returned data in the Transaction Response are sorted in the order required for the Secure Hash calculation.

Store Secure Hash Secret Securely

You must keep your Secure Hash Secret stored securely. Do not store your secret within the source code of an ASP, JSP, or other website page as it is common for web server vulnerabilities to be discovered where source code of such pages can be viewed.

You should store your Secure Hash Secret in a secured database, or in a file that is not directly accessible by your web server and has suitable system security permissions.

You should change your Secure Hash Secret regularly in accordance with your company's security policy, and at any time when you believe that its security may have been compromised.

You can change your Secure Hash Secret in Merchant Administration in the Setup menu option on the Configuration Details page. For more information, please refer to your Suncorp Bank Merchant Administration User Guide.

Returned Response Codes

The **vpc_TxnResponseCode** is a response code generated by the Payment Server that indicates the result of attempting to perform a transaction. This response code can also be used to detect an error.

Any response code other than '0' is a declined/failed transaction. If the transaction is an error condition it will be contained in the vpc_Message field.

Switch to Acquirer connectivity is where the Payment Gateway sends an authorisation request to the card schemes or card issuers via the acquirer.

Switch to Issuer connectivity allows the Payment Gateway to connect to the card schemes or card issuers without sending an authorisation request via the acquirer. The acquirer does not see the authorisation.

The response codes generated by the Payment Server are:

Vpc_Txn Response Code	Description	S2I	Description
?	Response Unknown	-	Response Unknown
0	Transaction Successful	00	Approved or completed successfully
		08	Honour with identification
		16	Approved, update Track #3
1	Transaction could not be processed	09	Request in progress
		10	Approved for partial amount
		11	Approved VIP
		12	Invalid transaction
		13	Invalid amount
		17	Customer cancellation
		18	Customer dispute
		20	Invalid response
		21	No action taken
		22	Suspected malfunction
		23	Unacceptable transaction fee
		24	File update not supported by receiver
		26	Duplicate file update record, old record replaced
		27	File update field edit error
		28	File update file locked out
		29	File update not successful, contact acquirer
		30	Format error
		32	Completed partially
		35	Card acceptor contact acquirer
		37	Card acceptor call acquirer security
		38	Allowable PIN tries exceeded
		40	Request function not supported
		42	No universal account
		44	No investment account
		45-50	Reserved for ISO use
		52	No cheque account
		53	No savings account
		55	Incorrect PIN
		56	No card record

Vpc_Txn Response Code	Description	S2I	Description
1	Transaction could not be processed	58	Transaction not permitted to acquirer
		60	Card acceptor contact acquirer
		62	Restricted card
		63	Security violation
		64	Original amount incorrect
		66	Card acceptor call acquirer's security department
		67	Hard capture (requires that the card be picked up at ATM)
		69-74	Reserved for ISO use
		75	Allowable number of PIN tries exceeded
		76-89	Reserved for private use
		93	Transaction cannot be completed, violation of law
		94	Duplicate transmission
		95	Reconcile error
		96	System malfunction
		97	Advises that reconciliation totals have been reset
2	Transaction Declined - Contact Issuing Bank	02	Refer to card issuer's special conditions
		03	Invalid merchant
		04	Pick up card
		05	Do not honour
		06	Error
		07	Pick up card, special condition
		14	Invalid card number
		15	No such Issuer
		19	Re-enter transaction
		25	Unable to locate record on file
		31	Bank not supported by switch
		34	Suspected fraud
		36	Restricted card
		39	No credit account
		41	Lost card
		43	Stolen card, pick up
		57	Transaction not permitted to card holder
		59	Suspected fraud
		61	Exceeds withdrawal amount limits
		62	Restricted card
		65	Exceeds withdrawal frequency limit
		81	Reserved for private use.
		90	Cut-off is in process (switch ending a day's business and starting the next. Transaction can be sent again in a few minutes.)
		91	Issuer or switch inoperative
		92	Financial institution or intermediate network facility cannot be found for routing
		98	MAC error
		99	Reserved for National Use
3	Transaction Declined - No reply from Bank	68	Response received too late

Vpc_Txn Response Code	Description	S2I	Description
4	Transaction Declined - Expired Card	33	Expired card
		54	Expired card
5	Transaction Declined - Insufficient credit	51	Not sufficient funds
E	Transaction Declined - Refer to card issuer	01	Refer to card issuer

Card Security Code Response Code

The Card Security Code (CSC) is a 3 or 4 digit numeric identifier printed on either the signature panel on the back of the card or on the front of the card. For example, MasterCard and Visa use a 3 digit CSC on the signature panel on the back of the card and American Express has a 4 digit CSC on the front of the card.

It is a security feature used for card not present transactions that compares the Card Security Code entered by the cardholder with the records held in the card issuer's database. Once the transaction is successfully processed and authorised, the card issuer returns a result code (CSC result code) in its authorisation response message verifying the level of accuracy of the card security code provided.

By default the Payment Server only accepts a transaction when the CSC result code returned from the issuer is in the range of M to S. Depending on the Payment Provider, the merchant can nominate a new CSC card acceptance level range. For example if they decide they can accept an order with a CSC card result code of U, the Payment Server accepts transactions in a new range from M to U, instead of S.

The CSC result codes are:

Code	Description
M	Valid or matched CSC
S	Merchant indicates CSC not present on card
P	CSC Not Processed
U	Card issuer is not registered and/or certified
N	Code invalid or not matched

Card Type Code

The Card Type Code is a two-character field that identifies the card type that was used for the transaction.

The Card Type Field values are shown in the following table.

Code	Description
AE	American Express
DC	Diners Club
JC	JCB Card
MC	MasterCard
VC	Visa Card

Verified by Visa™, MasterCard® SecureCode™ and JCB J/Secure™ Status Codes

All authentication transactions use a vpc_VerStatus response code value to show whether the card authentication was successful or not. The vpc_VerStatus response code values are shown in the following table:

vpc_VerStatus response code values

Code	Description
Y	Success - The cardholder was successfully authenticated.
M	Success - The cardholder is not enrolled, but their card issuer attempted processing.
E	Not Enrolled - The cardholder is not enrolled.
F	Failed - An error exists in the request format from the Merchant.
N	Failed - Verification Failed.
S	Failed - The signature on the response received from the Issuer could not be validated. This should be considered a failure.
P	Failed - Error receiving input from Issuer.
I	Failed - Internal Error.
U	Undetermined - The verification was unable to be completed. This can be caused by network or system failures.
T	Undetermined - The cardholder session timed out and the cardholder's browser never returned from the Issuer site.
A	Undetermined - Authentication of Merchant ID and Password to the Directory Failed.
D	Undetermined - Error communicating with the Directory Server.
C	Undetermined - Card brand not supported.

The following vpc_VerStatus response codes are returned if "Use new 3DS response codes for Virtual POS" is enabled for the merchant profile.

Code	Description
Y	Success - The cardholder was successfully authenticated.
M	Success - The cardholder is not enrolled, but their card issuer attempted processing.
E	Undetermined - The Directory Server returned an Enrollment Status of "N" WITHOUT an Invalid Request element. This may indicate that the card cannot use 3DS.
F	Failed - An error exists in the request format from the Merchant.
N	Failed - Verification Failed.
S	Failed - The signature on the response received from the Issuer could not be validated. This should be considered a failure.
P	Failed - Error receiving input from Issuer.
I	Failed - Internal Error.
T	Undetermined - The cardholder session timed out and the cardholder's browser never returned from the Issuer site.
A	Undetermined - Authentication of Merchant ID and Password to the Directory Failed.
D	Undetermined - Error communicating with the Directory Server.
C	Undetermined - Card Type not supported.
Z	Undetermined - The Directory Server returned an Enrolment Status of "N" WITH an Invalid Request element. The Invalid Request indicates that the Directory Server rejected the contents of at least one field in the request, i.e., the request was invalid.
B	Undetermined - The Directory Server returned an Enrolment Status of "U" WITHOUT an Invalid Request element.
V	Undetermined - The Directory Server returned an Enrolment Status of "U" WITH an Invalid Request element.
W	Undetermined - Unable to parse VERes received from the Directory Server.
X	Undetermined - The Access Control Server returned an Authentication Status of "U" (Authentication not available) with error details provided.
U	Undetermined - The Access Control Server returned an Authentication Status of "U" (Authentication not available) with no error details provided.

Authorisation Response Data

Authorisation response data is additional data returned by the issuer during the authorisation process of a transaction. This data should be included in capture requests processed through an external system where applicable. When captures are processed through the Payment Server, this data is automatically included with the capture request as needed.

You can control the receipt of authorisation response data in the Transaction Response using the field vpc_ReturnAuthResponseData in the Transaction Request for both authorisation and purchase transactions. The received response data varies based on the card schemes, as shown in the following table:

Note: A tick (✓) indicates the field is returned for that card scheme.

Code	Visa	MasterCard	American Express
vpc_ReturnACI	✓	✗	✗
vpc_TransactionIdentifier	✓	✓	✓
vpc_CommercialCardIndicator	✓	✓	✗
vpc_CardLevelIndicator	✓	✗	✗
vpc_FinancialNetworkCode	✗	✓	✗
vpc_MarketSpecificData	✓	✗	✗

The Commercial Card field, vpc_CommercialCard, generated by the Payment Server, indicates if the card was identified by the issuer as a commercial card, based on the response returned from the issuer in the Commercial Card Indicator field, vpc_CommercialCardIndicator, as shown in the following table:

vpc_CommercialCardIndicator		vpc_CommercialCard	
Code	**Description**	**Code**	**Description**
0 (zero)	Decline or not a Commercial Card	N	Not a Commercial Card
B	Business Card	Y	Commercial Card
R	Corporate Card	Y	Commercial Card
S	Purchasing Card	Y	Commercial Card
1	Consumer Card	N	Not a Commercial Card
2	Commercial Card	Y	Commercial Card
3	Both	U	Undetermined
Other	Undefined	U	Undetermined

Note: Codes 1-3 are returned only for MasterCard cards. Codes 0-S are returned for Visa cards.

Error Codes

In an unsuccessful transaction with a vpc_TxnResponseCode of "7", an error description may be contained in the field **vpc_Message** to describe the reason for the error.

The format of the error message is:

E**<error number>-<Date/Time Stamp MMDDHHMM>: <error description>**

For example: Where the error code is "5431" and the error description is "Invalid Field : CardNum", the full error message returned is;

"E5431-08131458: Invalid Field : CardNum"

The common errors that a merchant may encounter are listed in the table below followed by a complete list of error codes that may be returned.

Error Codes and Their Descriptions for the Most Commonly Encountered Errors

Error Number	Description
5001	Invalid Digital Order
5004	Invalid Digital Order: invalid session ID
5005	Invalid Digital Order: invalid Merchant Id
5006	Invalid Digital Order: invalid purchase amount
5007	Invalid Digital Order: invalid locale
5050	Invalid Permission
5061	Unsupported payment method
5065	Runtime exception
5121	Try to access an invalid key file
5134	RSA Decrypt Failed
5135	RSA Encrypt Failed
5231	Retrieved Digital Receipt Error
5423	Bad User Name or Password
5425	Invalid Recurring Transaction Number
5426	Invalid Permission
5433	Invalid Permission
5435	Max No of Deferred Payment reached
5436	Invalid recurring transaction number

The complete list of Error Codes and their descriptions are:

Error Number	Description
5000	Undefined error
5001	Invalid Digital Order
5002	Invalid Digital Order: not enough fields
5003	Invalid Digital Order: too many fields
5004	Invalid Digital Order: invalid session ID
5005	Invalid Digital Order: invalid Merchant Id
5006	Invalid Digital Order: invalid purchase amount
5007	Invalid Digital Order: invalid locale
5008	Invalid Digital Order: outdated version
5009	Invalid Digital Order: bad or too many Transaction Request parameters. It could be one of the following: • Invalid Digital Order: Invalid PAN Entry Mode • Invalid Digital Order: Invalid PIN Entry Capability • Bad Credit Payment Type • Bad Account Balance Type • Unsupported Transaction Type • Invalid Digital Order: Invalid Payment Method • Invalid Digital Order: Invalid PIN field • Invalid Digital Order: Invalid KSN field • Invalid Digital Order: Invalid STAN field • Invalid Digital Order: Invalid PhysicalTerminalId field • Invalid Digital Order: Invalid POSEntryMode field • PIN Entry Capability Terminal Cannot Accept PIN • PIN Entry Capability Terminal PIN pad down • Authorisation Code must be provided • Authorisation Code must be numeric and 1 to 6 characters in length

Error Number	Description
5010	Bad DCC Base Amount
5011	Bad DCC Base Currency
5012	Bad DCC Exchange Rate
5013	Bad DCC Offer State
5014	DCC Offer State Unsupported
5015	Missing or Invalid Currency
5016	Missing or Invalid Merchant Transaction Reference
5020	Invalid Digital Receipt
5021	Invalid Digital Receipt: not enough fields
5022	Invalid Digital Receipt: too many fields
5023	Invalid Digital Receipt: invalid session ID
5024	Invalid Digital Receipt: invalid Merchant Id
5025	Invalid Digital Receipt: invalid purchase amount
5026	Invalid Digital Receipt: invalid locale
5027	Error in generating Digital Receipt ID
5028	Invalid Digital Receipt Delivery URL
5029	Invalid Digital Receipt Delivery IO
5030	Invalid Transaction log string
5031	Invalid Transaction log string: not enough fields
5032	Invalid Transaction log string: too many fields
5033	Invalid Transaction log string: invalid purchase amount
5034	Invalid Transaction log string: invalid locale
5035	Transaction Log File error
5040	Invalid QsiFinTrans message
5041	Unsupported acquirer
5042	Unsupported transport
5043	Unsupported message format
5044	Invalid Merchant transaction mode
5045	Unsupported transaction counter
5046	SecureCGIParam verification of digital signature failed
5047	Failed to read a QsiSigner object back from a serialized file!
5048	Failed to create a DCOM object
5049	Receipt is invalid.
5050	Invalid Permission
5051	Unsatisfied DLL link error
5052	Invalid Merchant Id
5053	Transmission error from QSIFinTrans
5054	Parser error
5055	Acquirer Response Error
5056	Trace file I/O error
5057	Invalid cookie
5058	RMI exception
5059	Invalid session
5060	Invalid locale
5061	Unsupported payment method
5065	Runtime exception

Error Number	Description
5066	Bad parameter name or value
5070	File backup error
5071	File save error
5072	File IO error
5073	File not found error
5074	File not found
5080	SQL Error
5081	SQL Error : Cannot locate the database
5082	SQL Error : Cannot connect to the database
5083	SQL Error : Incorrect row count
5084	SQL Error : Invalid value format
5085	SQL Error : Bad line count
5086	Duplicate primary agent
5087	Unknown database type
5090	Illegal user name
5091	Illegal password error
5101	Could not create and load the specified KeyStore object. If you are using a QSIDB KeyStore the database connection may have failed
5103	Could not create the specified javax.crypto.Cipher object. You may not have a provider installed to create this type of Cipher object or the Cipher object that is specified in your config file is incorrect
5104	Error in call to javax.crypto.Cipher.doFinal. Either the input was too large or the padding was bad
5106	The Message type specified is not supported. Check the com.qsipayments.technology.security. MessageCrypto.properties file to ensure that the MsgType is valid
5108	The message received has a bad format
5109	Error verifying signature
5110	Error creating a signature
5161	Customer Reference too long
5175	Card track data exceeded the allowed lengths
5120	Unable to generate new keys
5121	Try to access an invalid key file
5122	Not able to store the security keys
5122	Not able to store the security keys
5123	Not able to retrieve the security keys
5124	Encryption format invalid for Digital Order
5125	Encryption signature invalid for Digital Order
5126	Invalid transaction mode
5127	Unable to find user keys
5128	Bad key Id
5129	Credit Card No Decryption failed
5130	Credit Card Encryption failed
5131	Problem with Crypto Algorithm
5132	Key used is invalid
5133	Signature Key used is invalid
5134	RSA Decrypt Failed
5135	RSA Encrypt Failed
5136	The keys stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid
5137	The private key stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid

Error Number	Description
5138	The public key stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid
5140	Invalid Acquirer
5141	Generic error for a financial transaction
5142	Generic reconciliation error for a transaction
5143	Transaction counter exceeds predefined value
5144	Generic terminal pooling error
5145	Generic terminal error
5146	Terminal near full
5147	Terminal Full
5148	Attempted to call a method that required a reconciliation to be in progress but this was not the case
5150	Invalid credit card: incorrect issue number length
5151	Invalid Credit Card Specifications
5152	Invalid Credit Card information contained in the database
5153	Invalid Card Number Length
5154	Invalid Card Number
5155	Invalid Card Number Prefix
5156	Invalid Card Number Check Digit
5157	Invalid Card Expiry Date
5158	Invalid Card Expiry Date Length
5162	Invalid Card Initialisation file
5166	Invalid Credit Card: incorrect secure code number length
5170	Unable to delete terminal
5171	Unable to create terminal
5161	Customer Reference too long
5175	Card track data exceeded the allowed lengths
5176	Bad Card Track, invalid card track sentinels
5185	Invalid Acknowledgement
5200	Payment Client Creation Failed
5201	Creating Digital Order Failed
5202	Creating Digital Receipt Failed
5204	Executing Administration Capture Failed
5205	Executing Administration Refund Failed
5206	Executing Administration Void Capture Failed
5207	Executing Administration Void Refund Failed
5208	Executing Administration Financial Transaction History Failed
5209	Executing Administration Shopping Transaction History Failed
5210	PaymentClient Access to QueryDR Denied
5220	Executing Administration Reconciliation Failed
5221	Executing Administration Reconciliation Item Detail Failed
5222	Executing Administration Reconciliation History Failed
5230	Retrieving Digital Receipt Failed
5231	Retrieved Digital Receipt Error
5232	Digital Order Command Error
5233	Digital Order Internal Error
5234	MOTO Internal Error
5235	Digital Receipt Internal Error
5336	Administration Internal Error

Error Number	Description
5400	Digital Order is null
5401	Null Parameter
5402	Command Missing
5403	Digital Order is null
5410	Unknown Field
5411	Unknown Administration Method
5412	Invalid Field
5413	Missing Field
5414	Capture Error
5415	Refund Error
5416	VoidCapture Error
5417	VoidRefund Error
5418	Financial Transaction History Error
5419	Shopping Transaction History Error
5420	Reconciliation Error
5421	Reconciliation Detail Error
5422	Reconciliation History Error
5423	Bad User Name or Password
5424	Administration Internal Error
5425	Invalid Recurring Transaction Number
5426	Invalid Permission
5427	Purchase Error
5428	VoidPurchase Error
5429	QueryDR Error
5430	Missing Field
5431	Invalid Field Digital.TRANS_NO must be provided to indicate which existing order this transaction is to be performed against
5432	Internal Error
5433	Invalid Permission
5434	Deferred Payment service currently unavailable
5435	Max No of Deferred Payment reached
5436	Invalid recurring transaction number
5450	DirectPaymentSend: Null digital order
5451	DirectPaymentSend: Internal error
5500	Error in card detail
5501	Errors exists in card details
5600	Transaction retry count exceeded
5601	Instantiation of AcquirerController for this transaction failed.
5602	An I/O error occurred
5603	Could not get a valid terminal
5604	Unable to create the ProtocolReconciliationController for the protocol
5661	Illegal Acquirer Object Exception
5670	Message Exception
5671	Malformed Message Exception
5672	Illegal Message Object Exception
5680	Transport Exception

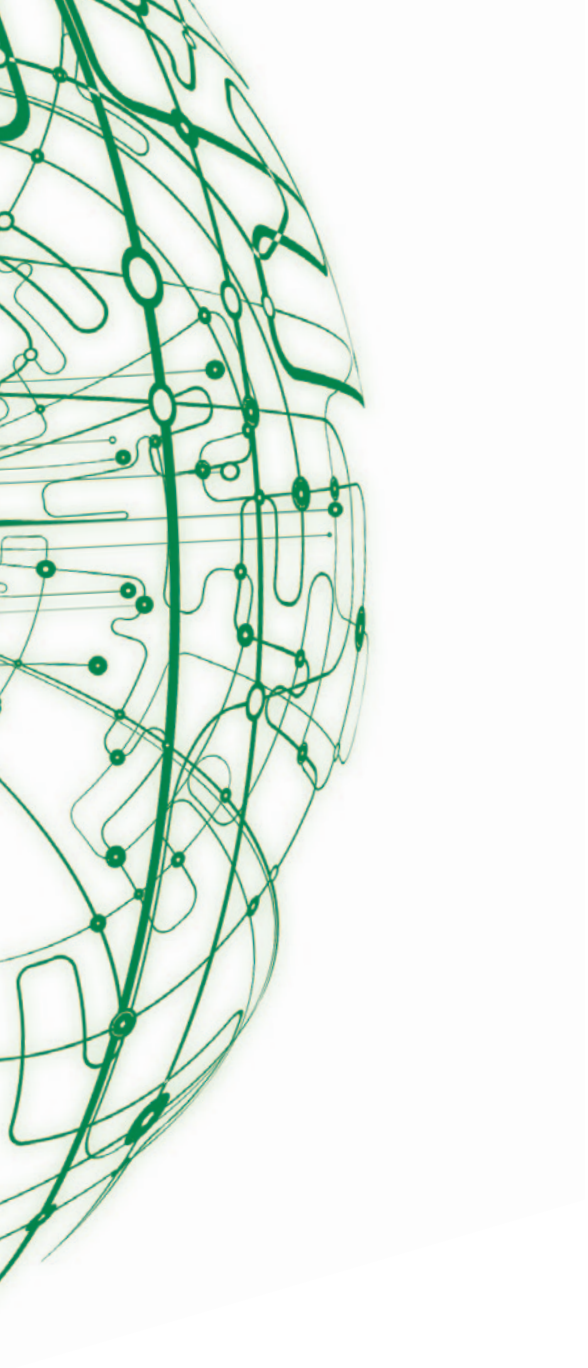
Error Number	Description
5681	Transport type not found
5682	Transport connection error
5683	Transport IO error
5684	Illegal Transport Object Exception
5690	Permanent Socket Transport connected
5691	Permanent Socket Transport JII class exception
5692	Permanent Socket Transport mismatched message received
5693	Permanent Socket Transport malformed message received
5694	Permanent Socket Transport unavailable
5695	Permanent Socket Transport disconnected
5696	The connection has been closed prematurely
5730	Host Socket unavailable
5750	Message header not identified
5751	Message length field was invalid
5752	Start of text marker (STX) not found where expected
5753	End of text marker (ETX) not found where expected
5754	Message checksum (LRC) did not match
5800	Init service started
5801	Init service stopped
5802	Invalid entry
5803	Duplicate entry
5804	Parse error
5805	Executing task
5806	Cannot execute task
5807	Terminating task
5808	Task killed
5809	Respawning task
5810	Cron service started
5811	Cron service stopped
5812	Parse error
5813	Invalid entry
5910	Null pointer caught
5911	URL Decode Exception occurred
5930	Invalid card type for excessive refunds
5931	Agent not authorized to perform excessive refunds for this amount
5932	Too many excessive refunds apply to this shopping transaction already
5933	Merchant agent is not authorized to perform excessive refunds
5934	Merchant is not authorized to perform excessive refunds
5935	Merchant cannot perform excessive refunds due to its transaction type
6010	Bad format in Rulefile
6100	Invalid host name
7000	XML parser [Fatal Error]
7001	XML parser [Error]
7002	XML parser [Warning]
7003	XML Parameter is invalid
7004	XML Parameter had an invalid index. Check input .html file
7005	XML [Bad Provider Class]

Error Number	Description
7050	SleepTimer: Time value is not in a valid format (ignored this time value)
7100	No valid times and/or interval specified in StatementProcessing.properties file. Execution terminated
7101	Status file for this data file was never created – deleting
7102	Error loading Statement.properties file
7104	Can't find file
7106	IOException thrown attempting to create or write to file
7107	Overwriting file
7108	SecurityException thrown when attempting to create output file
7109	Invalid Merchant Id. This Advice element will not be processed
7110	Can't create file name from the given date string
7111	Duplicate Advice element found in input document and skipped. Check input document
7112	Invalid payment type specified. This file will be skipped
7113	Null directory: can't create output file
7114	Validation of input file provided by host failed
7120	IOException thrown attempting to create or write to file
7121	IOException thrown while attempting to create a ZIP archive
7122	An inaccessible output directory was specified in the configuration file
7200	PRE Issue Id Error
7201	No Login User Object stored in session.
7202	Error Occurred while creating the merchant on the Payment Server.
7203	Logging out
7204	Error occurred while instantiating Payment.
7205	Error occurred while instantiating SSL Payment
7207	Error occurred while sending email
7208	Invalid Access. User is trying to access a page illegally.
7209	Invalid User Input.
7300	Error parsing meta data file
7301	Invalid field
7302	Field validator not present
7303	Validation of field failed
7304	Field not present in arbitrary data
7305	Mandatory field missing
7306	Date mask is invalid
7307	Error creating field validator
7308	Failed to update arbitrary data
7400	Invalid transaction type
7500	Record has changed since last read
8000	Invalid Local Tax Flag
8001	Local Tax Amount Equal to or Greater then Initial Transaction Amount
8002	Purchaser Postcode Too Long
8003	Invalid Local Tax Flag and Local Tax Flag Amount Combination
8004	Invalid Local Tax Amount
8015	Payment method must be EBT for a balance inquiry
8015	Invalid Digital Order: Invalid PaymentMethod
8016	Invalid Digital Order: Invalid PIN field
8017	Invalid Digital Order: Invalid KSN field
8019	Invalid Digital Order: Invalid PhysicalTerminalID field

Error Number	Description
8020	Invalid Digital Order: Invalid POSEntryMode field
8021	Invalid Digital Order: Invalid AdditionalAmount field
9000	Acquirer did not respond
9150	Missing or Invalid Secure Hash
9151	Invalid Secure Hash Type, or Secure Hash Type not allowed for this merchant
9152	Missing or Invalid Access Code
9153	Request contains more than one instance of the same field [FieldName]
9154	General merchant configuration error preventing request from being processed
9200	Missing or Invalid Template Number

Glossary

Term	Description
Access Code	An identifier that is used to authenticate you as the merchant while you are using the Virtual POS. The access code is generated and allocated to you by Merchant Administrator.
Acquirer Bank	Where your business account is maintained and settlement payments are deposited. This is normally the same bank with which you maintain your merchant facility for your online credit card payments.
Bank	The bank or financial institution with which you have a merchant facility that allows you to accept online credit card payments.
Capture	A transaction that uses the information from an authorisation transaction to initiate a transfer of funds from the cardholder's account to the merchant's account.
Card Token	The identifier for the stored card details that may be used later to refer to the card details to perform a payment.
Financial Institution (FI)	See Bank.
Issuing Bank	The bank or financial institution that issues credit cards to customers.
Merchant Administration	Allows you to monitor and manage your electronic transactions through a series of easy to use, secure web pages.
Payment Provider	Acts as a gateway between your application or website and the financial institution. It uses the Payment Server to take payment details (Transaction Request) from your cardholder and checks the details with the cardholder's bank. It then sends the Transaction Response back to your application. Approval or rejection of the transaction is completed within seconds, so your application can determine whether or not to proceed with the cardholder's order.
Payment Server	Facilitates the processing of secure payments in real-time over the Internet between your application/website and the Payment Provider. All communications between the cardholder, your application, the Payment Server and the Payment Provider is encrypted, making the whole procedure not only simple and quick, but also secure.
Purchase	A single transaction that immediately debits the funds from a cardholder's credit card account.
RRN	The Reference Retrieval Number is a unique number generated by the Payment Provider for a specific merchant ID. It is used to retrieve original transaction data and it is useful when your application does not provide a receipt number.
Switch to Acquirer	Switch to Acquirer connectivity is where the Payment Gateway sends an authorisation request to the card schemes or card issuers via the acquirer.
Switch to Issuer	Switch to Issuer connectivity allows the Payment Gateway to connect to the card schemes or card issuers without sending an authorisation request via the acquirer. The acquirer does not see the authorisation.
Transaction Request	Also called the Digital Order (DO) and is a request from the Virtual POS to the Payment Server to provide transaction information.
Transaction Response	Also called the Digital Receipt (DR) and is a response from the Payment Server to the Virtual POS to indicate the outcome of the transaction.
Virtual POS	The interface that provides a secure method of communication between your application and the Payment Server, which facilitates the processing of payments with your financial institution. It allows a merchant application to directly connect using HTTPS protocol in the merchant's choice of programming language.
VPC	Virtual POS
Transaction	A combination of a Transaction Request and a Transaction Response. For each customer purchase or order, merchants may issue several transactions.



Suncorp-Metway Limited ABN 66 010 831 722

Contact us for more information or to change your details:

Call 13 11 75

www suncorpbank.com.au

Visit your local branch or agency

Mail to GPO Box 1453, Brisbane QLD 4001

Fax 07 3031 2250

SUNCORP BANK
Business

13672 01/08/13 A