NAB TRANSACT

Direct Post Integration Guide

Contents

1. Introduction

1.1 About this Guide

This guide provides technical information about installing and configuring NAB Transact Direct Post within your web site. A full description of Direct Post is provided in Section 2 of this Guide (2.2 – Technical Overview). It is recommended that someone with HTML and advanced web programming experience reads this guide and implements NAB Transact Direct Post. Talk to your web developer if you require technical assistance with programming.

This guide covers the technical requirements of integrating NAB Transact Direct Post in to your web site. An advanced understanding of web programming is required.

1.2 Card Types Accepted

Direct Post accepts the following card types by default via your NAB Transact administration and reporting tool.

- Visa
- MasterCard

You may also accept the following cards. However, these must be applied for independently via the contacts shown:

American Express	1300 363 614
Diners Club	1300 360 500
JCB	1300 363 614

1.3 Prerequisites

1.3.1 Merchant Services

- A NAB Merchant ID and an Electronic Banking (EB) number for accepting Visa and MasterCard credit card transactions over the internet.
- An agreement with American Express, Diners and/or JCB if you wish to accept these transactions.

1.3.2 NAB Transact Services

- A NAB Transact Client ID (e.g. NAB0010). This number is generated by the NAB Transact Service Centre and is provided to you upon account activation.
- A web site or web site test environment.
- Knowledge of HTML and web programming is required. Web programming can be in any language you choose, such as Java, PHP, ASP or .Net. It is beyond the scope of this document to explain all features and functionality of building a web page and handling transaction result values. Please consult your web site programmer.
- The ability to update your web site. This is typically performed by a File Transfer Program (FTP)
- Direct Post supplies the SSL encryption required for secure transmission from the payment page to National Australia Bank. It is your responsibility to provide SSL encryption from your shopping cart or application to the order form that your customer completes.

1.4 Web Site Review and Account Activation

Your account is in test mode until you have implemented the service and performed test transactions.

When you want your account sent live, please contact the NAB Transact Service Centre on 1300 138 313, Option 1. The NAB Transact Service Centre will review your web site and payment service to ensure it complies with National Australia Bank's web site requirements.

To assist the Service Centre in reviewing your site, please ensure you provide the following as a minimum:

- URL or IP-address to visit
- Any test login data required to access the payment service
- Any test purchase data required to perform a test transaction

Common mistakes that slow down account activation:

- Missing privacy policy
- Missing refund policy
- Missing shipping policy
- Missing security policy
- Missing card logos (available from the NAB Transact Technical Service Centre)
- Missing transaction currency (AUD)

2. How is NAB Transact Direct Post Implemented?

2.1 Important Information Before You Begin

- The Direct Post Interface is not an API model, it is a browser redirect model. A brief description of API is contained in Section 4 – Glossary
- Credit card numbers must be submitted by your Customers directly to the payment URLs in the documentation, and not to your own or a third party server, from an HTML form on your web site. This is a NAB web site requirement and must be met before live transaction processing can commence.
- Please ensure that you integrate with either the "Payment" or "3D Secure" methods depending on which option is available to you. This will ensure you comply with NAB's risk requirements for your account.
- You must comply with all NAB web site requirements prior to the site being activated for live transactions.

2.2 Technical Overview

NAB Transact Direct Post is an online, secure credit and charge card transaction system that integrates into a web programming environment, such as PHP or .NET, via a three-step process that ensures transaction amount and response security (Figure 1).

Step 1: Server Side Post to Protect Amount

The transaction amount is passed to Direct Post via a server-side post and a fingerprint is generated as an encrypted record of the amount to be paid. The fingerprint is then included in the next step to ensure that the payment amount cannot be changed by a customer on the payment page.

Step 2: Customer Submits Card Details Directly to Direct Post

Your customer enters their credit card details on a secure HTML form on your web site and submits them directly to NAB Transact Direct Post which in turn securely processes the transaction.

Step 3: Display Result Page

Upon completion of the transaction, Direct Post calls a unique result URL on your server and passes result parameters. Your system updates itself with the result and outputs HTML. Direct Post captures the HTML and outputs the page under its own URL. This process ensures that the customer cannot intercept result parameters.

Note: When accepting card details on your web site (See "3.3 Securing Card Information Entry") you will require an SSL certificate. It is your responsibility to obtain and configure the SSL certificate.

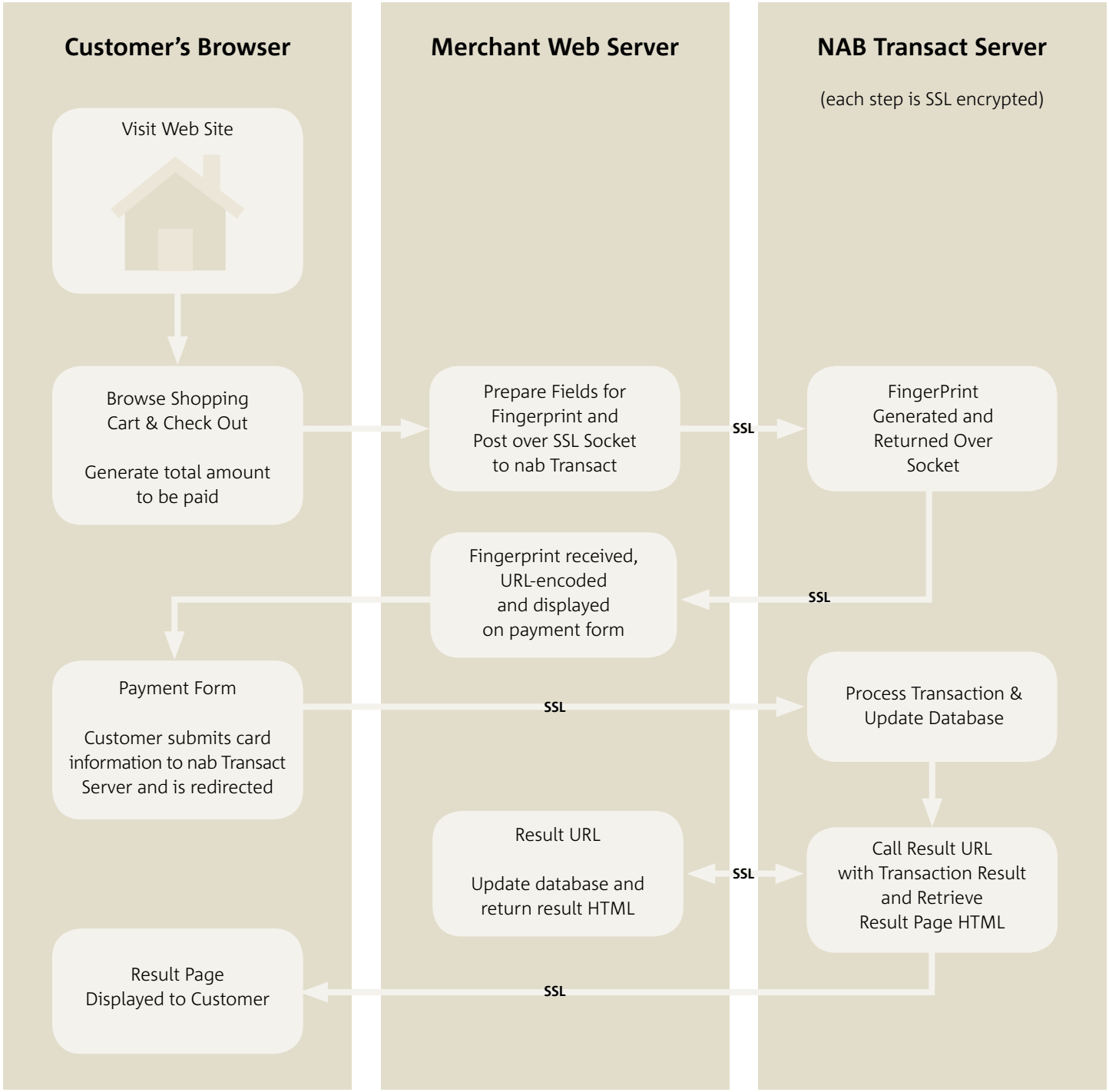

Figure 1
Direct Post Payment Process

Note that application environments that rely on cookies or other such mechanisms for passing session or state information may not be compatible with the result URL proxy system.

3. Implementation

3.1 General Information

3.1.1 Types of Information Submitted

Direct Post accepts POST data from your web server via a secure socket to generate the fingerprint, or from an HTML form submitted by your Customer on your web site to initiate a transaction.

Data submitted from a server must be URL-encoded.

3.1.2 Case Sensitivity

All field "name" and "value" attributes should be treated as case sensitive.

3.1.3 Form Tags

When using an HTML form, the following "form" tags are used to encapsulate Direct Post inputs:

```
<form method="post" action="https://...">
...
</form>
```

All INPUT fields must occur between the "form" tags for correct submission of information to the Direct Post Live and Test servers.

Ensure that the "method" attribute is set to "post".

You may also add the "name" attribute or any other form functionality that you require.

3.1.4 Test and Live Transaction URLs

Listed below are the live and test URLs for performing several functions.

- Generating fingerprints
- Processing transactions
- Processing with 3D Secure

3.1.5 Test URLs

Fingerprints are generated by server-side posts of URL-encoded data to:
https://transact.nab.com.au/test/directpost/genfingerprint

Transactions are created by an HTML form submitted by your Customer on your web site to:
<form method="post" action="https://transact.nab.com.au/test/directpost/authorise">
OR, *to utilise NAB Transact's own SSL certificate, post your entire payment page as the field EPS_HTML to:*
https://transact.nab.com.au/test/directpost/display
(see section 5.1.3.2 **EPS_HTML***)*

Antifraud-enabled merchants must use this URL:
<form method="post" action="https://transact.nab.com.au/test/directpost/authorise3d">

3.1.6 Live URLs

Note that the live transaction URLs are not yet connected to your NAB merchant service and therefore cannot be utilised prior to completion of testing.

Once testing is complete, please contact the NAB Transact Service Centre to enable live transaction processing on your account.

Fingerprints are generated by server-side posts of URL-encoded data to:
https://transact.nab.com.au/live/directpost/genfingerprint

Transactions are created by an HTML form submitted by your customer on your web site:
<form method="post" action="https://transact.nab.com.au/live/directpost/authorise">
OR, to utilise NAB Transact's own SSL certificate, post your entire payment page as the field EPS_HTML to:
https://transact.nab.com.au/live/directpost/display
(see section 5.1.3.2 EPS_HTML)

Antifraud-enabled merchants must use this URL:
<form method="post" action="https://transact.nab.com.au/live/directpost/authorise3d">

3.1.7 Acceptable Form Input Tags

Any HTML form tags may be used to submit information to NAB Transact Direct Post.

This document deals predominantly with the "input" tag, however, you may use any form tag to create the necessary name/value data pairs that form the information interpreted by Direct Post.

Most data is normally passed as "hidden" type input fields. Some fields, such as the card number, are entered by your Customer and are typically passed as "text" type input fields.

3.1.8 Result Fields

For each of the transaction methods listed below, a set of parameters will be made available to your result URL as a POST request. You may then use these parameters within your defined result URL program to display the desired outcome to the merchant.

Each transaction method will return a different subset of result parameters. Each subset is described under the sections within "3.6 Transaction Types".

The result parameters are further described in "5.2 Appendix 2: Result Fields".

3.2 How to Test

As you build your system, you can test functionality when necessary by submitting parameters to the test URL found in "3.1.4 Test and Live Transaction URLs". You can generate a fingerprint and then complete the transaction by using the card details listed below.

3.2.1 Test Card Number, Type and Expiry

Use the following information when testing transactions:

Card Number:	*4444333322221111*
Card Type:	*VISA*
Card CCV:	*123*
Card Expiry:	*08 / 08 (or any date greater then today)*

3.2.2 Simulating Approved and Declined Transactions

You can simulate approved and declined transactions by submitting alternative payment amounts.

If the payment amount ends in 00, 08, 11 or 16, the transaction will be approved once card details are submitted. All other options will cause a declined transaction.

Payment amounts to simulate approved transactions:

$1.00
$1.08
$105.00
$105.08
(or any total ending in 00, 08)

Payment amounts to simulate declined transactions:

$1.51
$1.05
$105.51
$105.05
(or any totals not ending in 00, 08)

Note that when using the live URL for payments, NAB determines the transaction result, independent of the payment amount.

3.3 Securing Card Information Entry

You must implement a Secure Sockets Layer (SSL) certificate on your web site to ensure your customers enter their card details on a secure page.

Secure pages can be identified by:

- The presence of a closed lock symbol in the browser window
- The URL being preceded by **https://nabtransact.nab.com.au**

You may use NAB Transact's inbuilt SSL Server via the EPS_HTML method (see section 5.1.3.2) or purchase your own.

SSL Certificates may be purchased from providers such as GeoTrust, Thawte or Verisign. Talk to your web site hosting company for further information

3.4 Minimum Transaction Requirements

Mandatory and Fingerprint Generation Fields must be included in every fingerprint or transaction request.

Mandatory fields must be included with every transaction request.

3.4.1 Mandatory and Fingerprint Generation Fields

Client ID and Transaction Password

The Client ID and Transaction Password input fields, "EPS_MERCHANT" and "EPS_PASSWORD", are mandatory form fields. They tell Direct Post through which account to process payments.

NAB Service Centre will supply your Client ID when your account is activated. Please contact NAB Transact Service Centre to be issued a transaction password. The Client ID will be of the format "ABC0010", where ABC is your unique three-letter account code, also used for logging in to the online NAB Transact Administration area.

Note: Your Client ID should not be confused with your eight-digit EB Number (e.g. 22123456). Your Transaction Password is for payment authentication only. It is **not** used for logging in to the online Direct Post Administration area.

Example: Form tags with EPS_MERCHANT input field
<form method="post" action="https://...">
<input type="hidden" name="EPS_MERCHANT" value="ABC0010">
<input type="hidden" name="EPS_PASSWORD" value="txnpassword">
...
</form>

Unique Payment Reference
The "EPS_REFERENCEID" mandatory field is used to tag orders with an identifier meaningful to you. This may be your invoice number, or could be a unique tracking number produced as part of your own web site.

The Reference ID is available to the Result URL and emails, and appears in the online NAB Transact Merchant Administration transaction history list.

Example: Defining a reference id
Scenario: Your Company wants to include its invoice numbers with every payment.
<input type="hidden" name="EPS_REFERENCEID" value="Invoice#642193">

Transaction Amount
The "EPS_AMOUNT" mandatory field is the amount is Australian Dollars (AUD) that will be transacted through your NAB Transact administration and reporting tool.

It is passed in a dollars and cents format. For example, $1.00 would be passed as "1.00".

Example: Setting the transaction amount
Scenario: A customer chooses items from your shopping cart totalling AUD$53.20.
<input type="hidden" name="EPS_AMOUNT" value="53.20">

GMT Timestamp
When sending a request to Direct Post to generate a fingerprint or to process a transaction, you must pass a Greenwich Mean Time (GMT) timestamp in the field "EPS_TIMESTAMP".

The timestamp sent to generate the fingerprint must exactly match the one sent with the associated transaction.

It must be of the format "YYYYMMDDHHMMSS" where:
YYYY is the current year
MM is the current two digit month 01 – 12
DD is the current two digit day 01 - 31
HH is the current two digit hour in 24-hour format 01 - 24
MM is the current two digit minute 00 – 59
SS is the current two digit second 00 – 59

Example: Setting the GMT timestamp
Scenario: Your system has generated a payment amount of AUD$53.20 which needs to be fingerprinted and returned to the browser to allow your customer to complete their card details. It is currently 22:35:05 on 20/06/2005 in Sydney (+10 hours from GMT). The time in GMT is 12:35:05 on the same day.
<input type="hidden" name="EPS_TIMESTAMP" value="20050620123505">
<input type="hidden" name="EPS_AMOUNT" value="53.20">
<input type="hidden" name="EPS_MERCHANT" value="ABC0010">
<input type="hidden" name="EPS_PASSWORD" value="txnpassword">
<input type="hidden" name="EPS_REFERENCEID" value="Test Reference">

3.4.2 Mandatory Fields

Transaction Result URL
Use the field "EPS_RESULTURL" to set the secure page on your web site that must receive and interpret the transaction result.

When a transaction is complete (approved or declined), Direct Post requests a result page from your web server with the transaction result in a series of POST fields. The HTML output of that page is then retrieved and displayed within the Direct Post secure server URL.

This protects result data from being viewed by your customer. However, note that the browser URL will change from your site to NAB Transact during this process.

The Direct Post system calls your EPS_RESULTURL directly (not from the customer's browser), therefore:

- Do not rely on session or cookie information.
- Append session id's or other required parameters to your EPS_RESULTURL (E.g. test.com.au?SESSID=jnfsdjknbsdjhfb&parameter=value).
- Do not rely on access control methods that may have been set up in the customer's browser session (The NAB Transact server will not be authorised to access any pages).
- All images referenced within the result page must be fully qualified and secure (e.g. https://www.merchant.com.au/images/image.gif).

The values of EPS_RESULTURL must:

- Be written as fully-qualified URLs. I.e. "https://...".
- Be secure URLs (unless you are testing) from a trusted provider (not self-signed)

Example: Set the Result URL
Scenario: The special result URL "result.php" has been configured to update a database and to provide HTML to NAB Transact to be displayed as a receipt page.
<input type="hidden" name="EPS_RESULTURL" value="https://www.myserver.com.au/result.php">

Fingerprint
The transaction fingerprint field, "EPS_FINGERPRINT", is used to protect the amount being paid when a customer submits card information and must be URL-encoded and included with each transaction sent to NAB Transact.

Example: Setting the fingerprint
Scenario: A customer chooses items from your shopping cart totalling AUD$53.20. This amount is used to generate the fingerprint. The fingerprint is returned and included with the payment details.
<input type="hidden" name="EPS_FINGERPRINT" value="MC0CFHsKwDfMeIXv44RO24H1deDKeTYmAhUAg3zS/srlURodH99KD2cmEs2RXcI=">

Card Information
Each transaction must include the card information submitted by a customer. This is private information and should not be visible to you or your system.

The fields, "EPS_CARDNUMBER", "EPS_EXPIRYMONTH", "EPS_EXPIRYYEAR" and "EPS_CCV" are all required for the transaction.

Visa and MasterCard have the card number and expiry date on the front, and a security number referred to as a CCV printed on the signature strip on the back of the card appearing as a three digit number.

Example: Allow a customer to enter their card information
Scenario: Your system displays a payment page to the customer, complete with amount to pay, requesting input of card information. The following input fields collect that information:

```
<input type="text" name="EPS_CARDNUMBER">
<input type="text" name="EPS_CARDTYPE" value="visa">
<select name="EPS_EXPIRYMONTH">
    <option value="1">01
    <option value="2">02
    <option value="3">03
    <option value="4">04
    <option value="5">05
    <option value="6">06
    <option value="7">07
    <option value="8">08
    <option value="9">09
    <option value="10">10
    <option value="11">11
    <option value="12">12
</select>
<select name="EPS_EXPIRYYEAR">
    <option value="2006">2006
    <option value="2007">2007
    <option value="2008">2008
    <option value="2009">2009
    <option value="2010">2010
</select>
<input type="text" name="EPS_CCV">
```

3.5 Generating the Payment Fingerprint

The Fingerprint is an encrypted record of the amount to be paid. It must be generated and then included on your customer payment HTML page as a hidden field. It prevents a customer modifying the payment amount when submitting their card information.

You must submit the required fingerprint fields to NAB Transact.

Note that the timestamp must be in Greenwich-Mean-Time (GMT).

Example: Posting information to generate a fingerprint
Note: This must be a server-side post over an SSL socket. Refer to your programming language manual for how to do this.
POST to URL: https://transact.nab.com.au/test/directpost/genfingerprint

```
EPS_MERCHANT="ABC0010"
&EPS_PASSWORD ="txnpassword"
&EPS_AMOUNT ="1.00"
&EPS_REFERENCEID ="Test Reference"
&EPS_TIMESTAMP="20050616221931"
```

If correctly submitted, this will return a Base64-encoded fingerprint string such as

```
MC0CFHsKwDfMeIXv44RO24H1deDKeTYmAhUAg3zS/srlURodH99KD2cmEs2RXcI
```

Otherwise, it will return a result of "error = error text".

Note: The Fingerprint must be URL-Encoded prior to inclusion in the payment form or you may experience "fingerprint not verified" errors occasionally.

3.6 Transaction Types

All transaction types require the generation of a fingerprint (see "3.5 Generating the Payment Fingerprint" above).

3.6.1 Payment

Authorisations and payment data is captured in real-time. Transaction information is passed from a payment form, to your NAB Transact CSSF for immediate processing.

Note: If your account is enabled for 3D Secure, you must use the Antifraud method in the next section.

Following the transaction, the Direct Post system initiates a POST request to your EPS_RESULTURL, reads the HTML output and displays the page to your customer using the Direct Post secure URL. This prevents a customer from intercepting result parameters.

Example: Form fields required to make a card payment
Note that the Fingerprint must be URL-encoded
Hidden fields:
<input type="hidden" name="EPS_MERCHANT" value="ABC0010">
<input type="hidden" name="EPS_REFERENCEID" value="Test Reference">
<input type="hidden" name="EPS_AMOUNT" value="1.00">
<input type="hidden" name="EPS_TIMESTAMP" value="200506141010">
<input type="hidden" name="EPS_FINGERPRINT" value="76f5gf5df6d57654fd4f">
<input type="hidden" name="EPS_RESULTURL" value=https://www.resulturl.com>
Customer-entered fields:
<input type="text" name="EPS_CARDNUMBER">
<input type="text" name="EPS_EXPIRYMONTH">
<input type="text" name="EPS_EXPIRYYEAR">
<input type="text" name="EPS_CCV">

A typical approved result from this transaction would be:

https://www.resulturl.com.au?
refid=Test Reference
&rescode=08
&restext=Honour with ID
&txnid=100036
&authid=151678
&settdate=20050617
&sig=MC0CFQCQnNRvziCb1o3q2XPWPljH8qbqpQIUQm9TpDX1NHutXYuxkbUk9AfV+/M=

Refer to "5.2.1 Standard Result Fields" for more information on transaction results.

3.6.2 Antifraud (3D Secure)

If your account has been enabled for Antifraud, you need to use the Antifraud URL to submit transactions. The EPS_TXNTYPE field is to be omitted for Antifraud payments.

Note: Developers should check with the merchant or the NAB Transact Service Centre to determine if this option has been paid for and enabled on the account.

Antifraud comprises 3D Secure (Verified by Visa, MasterCard SecureCode) and a system that compares millions of transactions from around the world to try and limit the effect of fraud.

Note: Antifraud cannot eliminate fraud. It observes transaction patterns and conservatively judges whether a transaction is likely to be fraudulent. You should always use your own judgement before sending goods or supplying services based on the result of any transaction.

All Antifraud parameters are described in "5.1.4 Antifraud Fields".

Example: Sending Antifraud parameters with a transaction.
Required (in addition to other required payment fields):
<input type="hidden" name="EPS_3DSECURE" value="true">
<input type="hidden" name="3D_XID" value="12345678901234567890">
<input type="hidden" name="EPS_MERCHANTNUM" value="22123456">

The field "3D_XID" must be a unique 20 character transaction reference. It can be generated using an incremental number or a timestamp and padded with zero's to 20 characters. For example: "00000000000000000001" or "Fri20050617102441000"

The field "EPS_MERCHANTNUM" is your eight-digit National Australia Bank Merchant Number. For example: "22123456".

3.6.3 Refund
To refund a payment, submit all the fields exactly as they were for the original payment, including the card details, as well as the following two fields:

Example: Additional fields required for a refund
<input type="hidden" name="EPS_TXNTYPE" value="REFUND">
<input type="hidden" name="EPS_TXNID value="100036">

Where "EPS_TXNID" is the "txnid" result field from the original payment.

Once submitted, the transaction will be processed and a result returned to your "EPS_RESULTURL" with the same parameters as a payment.

3.6.4 Pre-Authorisation

A pre-authorisation is a transaction that reserves funds on a credit card account. A merchant can then complete the transaction at a later date and receive the funds. If the pre-authorisation is never completed, it expires, usually after five days. After this, the reserved funds are again available to the card holder.

Pre-authorisations are often used by hotels to reserve funds at booking time and then completed when the guest checks out.

To pre-authorise an amount, submit all the fields exactly as they were for the PAYMENT transaction type above, including the credit card details, and set:

```
<input type="hidden" name="EPS_TXNTYPE" value="PREAUTH">
```

Once submitted, the result will be returned to your "EPS_RESULTURL" including the following field:

```
Example: Extra result field from a PREAUTH transaction
preauthid=516376
```

You may then use this "preauthid" in the pre-authorisation advice transaction type to COMPLETE the payment.

3.6.5 Pre-Authorisation Completion

This transaction type is used to complete a pre-authorisation and therefore take money from your customer's credit card account.

To provide a completion request on a pre-authorisation, submit all the fields exactly as they were for the PAYMENT transaction type, including the card details, as well as the following two fields:

```
Example: Additional fields required for a pre-auth "COMPLETE"
<input type="hidden" name="EPS_TXNTYPE value="COMPLETE">
<input type="hidden" name="EPS_PREAUTHID value="516376">
```

Where "EPS_PREAUTHID" is the "preauthid" result field from the pre-authorisation.

Once submitted, the transaction will be processed and a result returned to your "EPS_RESULTURL" with the same parameters as a payment.

3.6.6 Reversal

If you performed a transaction in error, you can remove it from the system by doing a "reversal".

Reversals differ from "refunds" in that the result of the transaction does not appear on your customer's card statement. Instead, the original transaction is removed from the system before funds are exchanged.

Reversals can only be done on transactions on the same settlement date. The settlement date is one of the result parameters returned to your result URL. It refers to the time period for which transactions are pooled for processing and settlement to your nominated bank account.

The settlement date is generally between 6pm one day and 6pm the next day. For example, a transaction at 10:00 am on 20/06/2005 would return a settlement date of "20050620", whereas a transaction at 8:00 pm on 20/06/2005 would return a settlement date of "20050621" (i.e. the next settlement period).

Reversals are run identically to "Refunds", but set:

```
<input type="hidden" name="EPS_TXNTYPE" value="REVERSAL">
```

4. Glossary

3D Secure	A method used by Visa, MasterCard and JCB to authenticate the cardholder during an online transaction. Cardholders who have enrolled in either the Verified by Visa, MasterCard SecureCode or JCB J Secure programs can be asked to supply a password during the shopping experience to validate their identity. The password request is made by the cardholder's Issuing Bank and the response is available only to that bank. Under certain circumstances, the cardholder's right to deny involvement in the transaction is removed by the application of 3D Secure. Refer also to J Secure, MasterCard SecureCode and Verified by Visa.
API	An Application Programming Interface (API) is a source code interface that an operating system or library provides to support requests for services to be made of it by computer programs.
Client ID	The Client ID is an alphanumeric code used to identify and manage a Periodic Payment. Each Client Id must be unique. Typically you will use a value such as Order Number, Invoice Number, Customer Number etc or any combination of these as your Client ID. After each instance of processing of a Periodic payment, Client ID is combined with an incrementing "processing sequence number" in the range 000001-999999 to create a unique Transaction Reference. Refer also to Transaction Reference.
Complete	The transaction which transfers funds previously reserved by a Pre-authorisation from the cardholder to the merchant. Refer also to Pre-authorisation and Payment.
CSC	Cardholder Security Code. This is an extra code printed on the back of a Visa or MasterCard, typically shown as the last three digits on the signature strip. It is used during a payment as part of the cardholder authentication process. You may also know it as the Cardholder Verification Value (CVV), Card Verification Code (CVC), or the Personal Security Code. American Express and Diner Club Cards use a 4 digit Security Code in much the same manner.
FORM	The HTML tag used to mark the start and end of the area of your payment page that passes name/value data pairs to NAB Transact.
HTML	Hypertext Markup Language. The language interpreted by web browsers. This is the language used to create your NAB Transact payment form.
Hyperlink	A shortcut to another function within the system, accessed by clicking on an underlined label.
Input Field	HTML tags that define Form input fields. Used to submit information to NAB Transact from your order form.
J Secure	JCB's brand name for it's version of 3D Secure. Refer also to 3D Secure.
Log Date/Time	The date and time that the transaction was processed via the NAB Transact service. Log Date and Time helps to tie a transaction back to your business system and assists in searching (via NAB Transact Transaction Search) for transactions which occurred during a specific period. Refer also to Settlement Date.
Merchant ID	Your NAB Transact access code ("vendor_name") for use of NAB Transact Administration tools. Also used in your payment form as your account identifier. Also used when calling NAB Transact Service Centre on 1 300 138 313
MOTO	An acronym for Mail Order/Telephone Order. MOTO is now a general term used to describe any process of processing a credit or charge card transaction by manual entry of the card details.
MasterCard SecureCode	MasterCard's brand name for it's version of 3D Secure. Refer also to 3D Secure.
Online	A cardholder initiated transaction processed via either the NAB Transact Standard or Tailored Interface.
Payment	A transaction which both reserves card holder funds and transfers those funds to the merchants account in a single step. Refer also to Pre-authorisation and Complete.

Pre-authorisation	A transaction which reserves card holder funds but does transfer not those funds to the merchants account until a follow up Complete transaction is performed. Refer also to Complete and Payment.
Periodic	Transactions processed via NAB Transact's Periodic function (Once-off, day-based or Calendar based).
Refund	A transaction which transfers funds from a merchant to a cardholder. In the NAB Transact system a Refund can only be processed if a previous Payment or Pre-authorisation/Complete transaction has been processed. The refund can only be applied to the credit or charge card used for the original transaction and although multiple partial refunds can be processed, the total of these refunds will not be permitted to exceed the amount of the original Payment or Complete transaction. Where a Refund is processed, the cardholder will see 2 transactions on their statement; one for the original Payment or Pre-authorisation/ Complete and one for the Refund.
Response Code	A numeric code associated with a transaction to indicate a specific transactions processing result. Transactions which are successfully passed through the banking system are returned with a two digit response code allocated by the banking system. A full list of Response Codes is included in this document as Appendix 2.
Reversal	A transaction which cancels the effect of a prior Payment or Pre-authorisation/Complete transaction. A Reversal can only be processed against a transaction which has not yet gone to Settlement. A Reversal must be processed prior to 6:00 pm AEST on the same day as the Payment or Pre-authorisation transaction. Where a Reversal is processed, the cardholder will not see any transactions on their statement.
Settlement Date	The date on which funds associated with successful Visa and MasterCard transactions are transferred to the merchant's account. Settlement is usually same day for transactions which have been processed by NAB Transact before 6:00 pm AEST and next day for transactions processed after that time. Settlement for American Express, Diners and JCB cards will vary depending on your relationship with these organisations. Searching by Settlement Date helps to tie a transaction back to your bank statement. Refer also to Log Date/Time.
SSL	Secure Sockets Layer. The mechanism used to encrypt form data submitted from a browser.
Transaction Password	This password is sent in transaction requests along with your Merchant ID to authenticate your account. It is not your online login password, however, it can be changed via your online login. Be aware that changing this password may prevent transactions from being processed unless you also update it in your programs.
Transaction Reference	A meaningful business reference such as customer name, customer number, order number, reservation number etc which you allocate to your transaction at the time of processing. Transactions processed by NAB Transact are immediately recorded in the secure database which is accessed by the NAB Transact Administration system. Transaction Reference (or any part of it) is an important search criterion within NAB Transact Administration.
Transaction Source	The point of origination of this transaction. Valid Transaction Sources are: Online, IVR, Batch, Periodic, and Administration. Each of these is individually explained in more detail in this Glossary.
Transaction Type	The type of processing requested by this transaction. Valid Transaction Types are: Payment, Pre-authorisation (except for 3D Secure merchants), Complete, Refund and Reversal. Each of these is individually explained in more detail in this Glossary.
Verified by Visa	Visa's brand name for it's version of 3D Secure. Refer also to 3D Secure.

5. Appendices

5.1 Appendix 1: Accepted Input Field Names

Mandatory	Additional	Antifraud (Mandatory)
EPS_MERCHANT	EPS_TXNTYPE	EPS_3DSECURE
EPS_PASSWORD	EPS_TXNID	3D_XID
EPS_RESULTURL	EPS_PREAUTHID	EPS_MERCHANTNUM
EPS_REFERENCEID		
EPS_CARDNUMBER		
EPS_CARDTYPE		
EPS_EXPIRYMONTH		
EPS_EXPIRYYEAR		
EPS_CCV		
EPS_AMOUNT		
EPS_TIMESTAMP		
EPS_FINGERPRINT		

5.1.1 Mandatory Fields (Static)

EPS_MERCHANT

CLASS:	Mandatory
DESCRIPTION:	A unique identifier for the merchant within the Payment Gateway. This merchant identifier value is an alphanumeric string allocated to the merchant by NAB Transact. This merchant identifier value is not the same as the Merchant ID number given to the merchant by National Australia Bank.
TYPICAL USE:	*<input type="hidden" name="EPS_MERCHANT" value="ABC0010">*

EPS_PASSWORD

CLASS:	Mandatory
DESCRIPTION:	The field should contain the transaction processing password supplied by NAB Transact when your account is activated. It will be supplied in the activation email.
TYPICAL USE:	*<input type="hidden" name="EPS_PASSWORD" value="password1">*

EPS_RESULTURL

CLASS:	Mandatory
DESCRIPTION:	The URL on the merchant web site that accepts transaction result data as POST elements. The result page may be almost any form of web page, including static HTML pages, CGI scripts, ASP pages, JSP pages, PHP scripts, etc, however cookies or other forms of additional information will not be passed through the Payment Gateway. The EPS_RESULTURL must be a URL for a publicly visible page on a web server within a domain that is delegated to a public IP number. Internal machine names, such as “localhost”, Windows-style machine names, and privately translated IP numbers will fail.
TYPICAL USE:	*<input type="hidden" name="EPS_RESULTURL" value="http://www.myserver.com.au/result.asp">*

5.1.2 Mandatory Fields (Variable)

EPS_REFERENCEID

CLASS:	Mandatory
DESCRIPTION:	An alphanumeric string that allows the merchant's processing system to identify an individual transaction. This string can be of any format and is stored by NAB Transact within the transaction record and returned to the merchant's processing system in the transaction result. This field is typically a shopping cart id or invoice number.
TYPICAL USE:	*<input type="hidden" name="EPS_REFERENCEID" value="My Reference">*

EPS_CARDNUMBER

CLASS:	Mandatory
DESCRIPTION:	The card number used in the transaction. This number must be greater than 12 digits, less than 19 digits and must conform to the card check digit scheme. Spaces and hyphens included in the card number value will be removed before processing.
TYPICAL USE:	*<input type="hidden" name="EPS_CARDNUMBER" value="4444333322221111">*

EPS_CARDTYPE

CLASS:	Mandatory
DESCRIPTION:	A string containing the name of the card issuer that provided the card. This may currently be one of the strings "visa", "mastercard", "amex", "dinersclub" or "jcb" in any mixture of case. If this parameter is not correctly set to one of the values listed above, the transaction will be rejected.
TYPICAL USE:	*<input type="hidden" name="EPS_CARDTYPE" value="visa">*

EPS_EXPIRYMONTH

CLASS:	Mandatory
DESCRIPTION:	The month in which the card expires. This may only contain an integer value between 1 and 12, inclusive, corresponding to the month of the year. The expiry month and expiry year together must form a date that is at least the current month. Transactions that contain an expiry date in the past will be rejected.
TYPICAL USE:	*<input type="hidden" name="EPS_EXPIRYMONTH" value="06">*

EPS_EXPIRYYEAR

CLASS:	Mandatory
DESCRIPTION:	The year in which the card expires. This should ideally be a 2 digit year value. The expiry month and expiry year together must form a date that is later than the current date. Transactions that contain an expiry date in the past will be rejected.
TYPICAL USE:	*<input type="hidden" name="EPS_EXPIRYYEAR" value="08">*

EPS_CCV

CLASS:	Mandatory
DESCRIPTION:	The Card Check Value (CCV) field should contain the three digit value that is printed on the back of the card itself, or the four digit value printed on the front of American Express cards. When sending transactions to the Payment Gateway test facility, any 3 or 4 digit value will be accepted. This field may be referred to elsewhere as a Card Verification Value (CVV) or a Card Verification Code (CVC), most notably in information provided by banks or card providers.
TYPICAL USE:	*<input type="hidden" name="EPS_CCV" value="999">*

EPS_AMOUNT

CLASS:	Mandatory
DESCRIPTION:	The total amount of the purchase transaction. This value must be a positive decimal value of dollars and cents. Please be careful to correctly specify the amount as the NAB Transact Payment Gateway has no way of determining whether an amount has been correctly specified. Null or zero and negative amounts are not acceptable and transactions containing such amount values will be rejected.
TYPICAL USE:	*<input type="hidden" name="EPS_AMOUNT" value="107.95">*

EPS_TIMESTAMP

CLASS:	Mandatory
DESCRIPTION:	A timestamp of the format "YYYYMMDDHHMMSS" in GMT. The hour component must be specified in 24-hour format. This value must be the same submitted to generate a fingerprint as to submit a card transaction.
TYPICAL USE:	*<input type="hidden" name="EPS_TIMESTAMP" value="20050620122453">*

EPS_FINGERPRINT

CLASS:	Mandatory except for generating the fingerprint
DESCRIPTION:	The value returned after submitting information to the fingerprint generation system on NAB Transact. It is a Base64-encoded string and must be included in all transaction attempts.
TYPICAL USE:	*<input type="hidden" name="EPS_FINGERPRINT" value="MCwCFCncotpMpCwMtLz8EiXz9qsi9vwvAhQzddPtwWphDTLIZ1JeUvgP+XtcxQ==">*

5.1.3 Additional Fields

Some fields are fully optional, whereas others may be required depending on the transaction type specified.

EPS_CANAME

CLASS:	Optional
DESCRIPTION	The Card Acceptor Location is normally your City/Suburb or Customer Service contact number. This field may be used to control the information on a customer's credit card statement. The maximum length available is 25 characters. Note that permission for this feature must be enabled on your account or you will receive a response of "555 – Permission denied".
TYPICAL USE:	*<input type="hidden" name="EPS_CANAME" value="www.KidsGames.com.au">* *<input type="hidden" name="EPS_CANAME" value="My Charity *NYE Ball">* *<input type="hidden" name="EPS_CANAME" value="My Charity *Donation">*

EPS_CALOCATION

CLASS:	Optional
DESCRIPTION	The Card Acceptor Location is normally your City/Suburb but can also be used to your Customer Service contact number on a customer's credit card statement. The maximum length available is 13 characters. Note that permission for this feature must be enabled on your account or you will receive a response of "555 – Permission denied".
TYPICAL USE:	*<input type="hidden" name="EPS_CALOCATION" value="Sydney">* *<input type="hidden" name="EPS_CALOCATION" value="1800-123-456">*

EPS_TXNTYPE

CLASS:	Optional
DEFAULT:	PAYMENT
DESCRIPTION	Used to determine the processing type for an individual transaction. May be one of the following: • PAYMENT: A card payment/purchase transaction. • REFUND: A card refund transaction. Must be used in conjunction with the required field "EPS_TXNID". You must also pass "EPS_REFERENCEID" matching the original payment "EPS_REFERENCEID", as well as the original card details. • REVERSAL: Used to reverse a card payment prior to bank settlement cut off. Must be used in conjunction with the required field "EPS_TXNID". You must also pass "EPS_REFERENCEID" matching the original payment "EPS_REFERENCEID", as well as the original card details. • PREAUTH: Used to pre-authorise an amount on a card. The result codes for this type include "preauthid" which must be stored and used with the type "COMPLETE" to complete the pre-authorisation • COMPLETE: Completion of a pre-authorised transaction. Must be used in conjunction with the required field "EPS_PREAUTHID" populated with the result code from the initial pre-authorisation. You must also pass "EPS_REFERENCEID" matching the original pre-authorisation "EPS_REFERENCEID", as well as the original card details. This field is omitted for Antifraud Payments.
TYPICAL USE:	*<input type="hidden" name="EPS_TXNTYPE" value="PAYMENT">*

EPS_HTML

CLASS:	Optional for all payment types
DESCRIPTION	The complete URL-encoded HTML of your payment page, including the EPS_FINGERPRINT and any other information that must be included to allow a transaction to be processed. Must be used in conjunction with the special "display" transaction URL.
TYPICAL USE:	*<form method="post" action ="https://transact.nab.com.au/test/directpost/display">* *<input type="hidden" name="EPS_HTML" value="<html> ...your page... </html>">* ... *</form>*

EPS_TXNID

CLASS:	Mandatory for Refunds and Reversals
DESCRIPTION	Used for EPS_TXNTYPE's REFUND and REVERSAL only. Must contain the “txnid” result code from the original payment.
TYPICAL USE:	*<input type="hidden" name="EPS_TXNID" value="654321">*

EPS_PREAUTHID

CLASS:	Mandatory for Preauthorisation completions (“COMPLETE” transaction type)
DESCRIPTION	Used for “EPS_TXNTYPE” COMPLETE only. Must contain the “preauthid” result code from the original payment.
TYPICAL USE:	*<input type="hidden" name="EPS_PREAUTHID" value="123456">*

5.1.4 Antifraud Fields (Mandatory)

“Antifraud” is the term that encompasses 3D Secure (Verified by Visa and MasterCard SecureCode) for the purposes of this document.

Merchants using this feature are required to include the following fields with all transactions sent to the NAB Transact system.

EPS_3DSECURE

CLASS:	Mandatory for Antifraud Payments
DESCRIPTION	Merchants using Verified by Visa or SecureCode, or both, must set this field to "true". Must also use the fields “3D_XID” and “EPS_MERCHANTNUM”. If you are not using 3D Secure, omit this field or set a value of “false”
TYPICAL USE:	*<input type="hidden" name="EPS_3DSECURE" value="true">*

3D_XID

CLASS:	Mandatory for Antifraud Payments
DESCRIPTION	3D Secure Transaction ID string. MUST uniquely reference this transaction to the merchant, and MUST be 20 characters in length. Any ASCII characters may be used to build this string. E.g. May comprise of a timestamp padded with 0s for uniqueness: “20040714112034872000”.
TYPICAL USE:	*<input type="hidden" name="3D_XID" value="20040714112034872000">*

EPS_MERCHANTNUM

CLASS:	Mandatory for Antifraud Payments
DESCRIPTION	Your online merchant number specified by National Australia Bank which has been registered for Verified by Visa or SecureCode, or both. This will be your 8 digit merchant number, e.g. "22123456".
TYPICAL USE:	*<input type="HIDDEN" name="EPS_3DSECURE" value="true">* *<input type=”HIDDEN” name=”3D_XID” value=”20050714114257796000”>* *<input type=”HIDDEN” name=”EPS_MERCHANTNUM” value=”22123456”>*

5.2 Appendix 2: Result Fields

5.2.1 Standard Result Fields

rescode
The primary indicator of the transaction result.

Bank response or internal error code numbers used to determine the transaction result. Rescode's of 00, 08 and 11 indicate approved transactions, while all other codes represent declines. A full list of response codes is available for download from your online NAB Transact login.

restext
The associated text for each "rescode". For bank response codes 00 – 99, this field is generated by NAB's payment systems. All other codes have the "restext" generated by NAB Transact.

refid
The value of the EPS_REFERENCEID parameter from the transactions request. This value is returned to the merchant's processing system to allow matching of the original transaction request.

txnid
The bank transaction ID returned by NAB Transact. This 6-digit string is unique at least per terminal, per bank and per settlement date.

This value is required to be re-entered along with other details of the original payment when conducting refunds or reversals.

settdate
The bank settlement date returned by NAB Transact. This is the date the funds will be settled into the merchant's account. The date will correspond to today's date until the bank's cut-off time (typically 6pm), then roll to the following business day. The settlement date is returned in the format "YYYYMMDD".

sig
Currently not used.

authid
The transaction id as returned by NAB Transact. This is an alphanumeric string of between 1 and 6 characters that may be quoted by the merchant or the customer in future queries regarding the particular transaction.

preauthid
The bank pre-authorisation ID returned by the payment gateway. This 6-digit string is used in the EPS_PREAUTHID field when sending COMPLETE transaction types in order to complete a pre-authorisation transaction.

5.3 Appendix 3: Response Codes

Bank Response Codes			
Code	**Response Text**	**Code**	**Response Text**
APPROVED			
00	Approved	08	Approved
11	Approved (not used)	16	Approved (not used)
DECLINED			
01	Refer to Card Issuer	41	Lost Card—Pick Up
02	Refer to Issuer's Special Conditions	42	No Universal Amount
03	Invalid Merchant	43	Stolen Card—Pick Up
04	Pick Up Card	44	No Investment Account
05	Do Not Honour	51	Insufficient Funds
06	Error	52	No Cheque Account
07	Pick Up Card, Special Conditions	53	No Savings Account
09	Request in Progress	54	Expired Card
10	Partial Amount Approved	55	Incorrect PIN
12	Invalid Transaction	56	No Card Record
13	Invalid Amount	57	Trans. not Permitted to Cardholder
14	Invalid Card Number	58	Transaction not Permitted to Terminal
15	No Such Issuer	59	Suspected Fraud
17	Customer Cancellation	60	Card Acceptor Contact Acquirer
18	Customer Dispute	61	Exceeds Withdrawal Amount Limits
19	Re-enter Transaction	62	Restricted Card
20	Invalid Response	63	Security Violation
21	No Action Taken	64	Original Amount Incorrect
22	Suspected Malfunction	65	Exceeds Withdrawal Frequency Limit
23	Unacceptable Transaction Fee	66	Card Acceptor Call Acquirer Security
24	File Update not Supported by Receiver	67	Hard Capture—Pick Up Card at ATM
25	Unable to Locate Record on File	68	Response Received Too Late
26	Duplicate File Update Record	75	Allowable PIN Tries Exceeded
27	File Update Field Edit Error	86	ATM Malfunction
28	File Update File Locked Out	87	No Envelope Inserted
29	File Update not Successful	88	Unable to Dispense
30	Format Error	89	Administration Error
31	Bank not Supported by Switch	90	Cut-off in Progress
32	Completed Partially	91	Issuer or Switch is Inoperative
33	Expired Card—Pick Up	92	Financial Institution not Found
34	Suspected Fraud—Pick Up	93	Trans Cannot be Completed
35	Contact Acquirer—Pick Up	94	Duplicate Transmission
36	Restricted Card—Pick Up	95	Reconcile Error
37	Call Acquirer Security—Pick Up	96	System Malfunction
38	Allowable PIN Tries Exceeded	97	Reconciliation Totals Reset
39	No CREDIT Account	98	MAC Error
40	Requested Function not Supported	99	Reserved for National Use

5.4 Appendix 4: NAB Transact Gateway Response Codes

The response codes returned by the NAB Transact Payment Gateway are outlined below:

Gateway Response Code	Response Text	Description
000	Normal	Message processed correctly (check transaction response for details).
504	Invalid Merchant ID	If Merchant ID does not follow the format XXXDDDD, where X is a letter and D is a digit, or Merchant ID is not found in NAB Transact database.
505	Invalid URL	The URL passed to either the Echo, Query, or Payment object is invalid.
510	Unable To Connect To Gateway	Produced by the NAB Transact Client API when unable to establish connection to the NAB Transact Payment Gateway
511	Gateway Connection Aborted During Transaction	Produced by the NAB Transact Client API when connection to the NAB Transact Payment Gateway is lost after the payment transaction has been sent
512	Transaction timed out by the Client API	Produced by the NAB Transact Client API when no response to the payment transaction has been received from the NAB Transact Payment Gateway within the predefined time period (default 80 seconds)
513	General Database Error	Unable to read information from the database.
514	Error loading properties file	The Payment Gateway encountered an error while loading configuration information for this transaction
515	Fatal Unknown Error	Transaction could not be processed by the Payment Gateway due to unknown reasons
516	Request type unavailable	The NAB Transact Payment Gateway does not support the requested transaction type
517	Message Format Error	The NAB Transact Payment Gateway could not correctly interpret the transaction message sent
524	Response not received	The client could not receive a response from the Payment Gateway .
545	System maintenance in progress	The system maintenance is in progress and the system is currently unavailable and unable to process transactions
550	Invalid password	The Client API has attempted to process a request with an invalid password.
575	Not implemented	This functionality has not yet been implemented
577	Too Many Records for Processing	The maximum number of allowed events in a single message has been exceeded.
Status Code	**Response Text**	**Description**
580	Process method has not been called	The process() method on either the Echo, Payment or Query object has not been called
595	Merchant Disabled	NAB Transact has disabled the merchant and the requests from this merchant will not be processed.

5.5 Appendix 5: Location of CVV

The Card Verification Value (CVV) is an anti-fraud measure used to prevent the fraudulent use of cards. The CVV number is printed on the physical card and is randomly assigned. The CVV number is located differently for the various card types. The location of the CVV on each card type is outlined below:

Card Type	Location
Visa	It is the last 3 digits printed on the signature strip on the back of the card.
MasterCard	It is the last 3 digits printed on the signature strip on the back of the card.
Amex	It is the 4 digits printed above card number on the front of the card.
Diners Club	It is the last 3 digits printed on the signature strip on the back of the card.
JCB	Not used