more than money

nab

NAB TRANSACT

Direct Post v2.1.2 – Integration Guide

CONTENTS

1 INTRODUCTION

1.1. What is Direct Post?

Direct Post is a payment service that integrates seamlessly with an existing website both functionally and aesthetically by accepting customer data directly from a form on your web site. Unlike an API, Direct Post uses a browser redirect model, where data is transmitted directly from a customer's web browser to NAB Transact and not to your own or a third party server.

Once the bank has processed the transaction, Direct Post redirects the customer back to a result page on your web site for order completion and fulfillment. NAB Transact can optionally send the result parameters to a back-end Callback URL on your website in order to enable seamless tracking of payments and orders, and to separate your systemic update from the browser process.

1.2. Requirements for Implementation

This guide covers the technical requirements for integrating Direct Post with your website, therefore an understanding of web programming, such as PHP or .NET, is required.

In order to process payments using Direct Post, you must have a NAB Merchant facility and NAB Transact eCommerce account. The following section of your NAB Transact activation email outlines the details you should be using in your implementation:

Getting Started

Live Direct Post and API Implementation

- **Merchant ID (or "EPS_MERCHANT"): <Your Merchant ID>**
- **Live Transaction Password: <Your live transaction password>**

Test Direct Post and API Implementation

- **Merchant ID (or "EPS_MERCHANT"): <Your Merchant ID>**
- **Test Transaction Password: <Your test transaction password>**

1.2.1. Public Test Account Details

Don't have a NAB Transact account? You can use our test account details in order to test your implementation.

Merchant ID: XYZ0010
Transaction Password: abcd1234

NAB Transact Portal – Test Login URL https://demo.transact.nab.com.au/nabtransact

NAB Transact Portal – Public Test Login Details

Client ID: XYZ
Username: demo
Password: abcd1234

1.3. Card Types Accepted

Direct Post accepts the following card types by default via your NAB merchant facility:

- Visa
- MasterCard

You may also accept the following card types by applying for these independently via the contacts shown:

American Express: 1300 363 614

Diners Club: 1300 360 500

JCB: 1300 363 614

UnionPay Online Payments (UPOP): Please refer to the NAB Transact UPOP Getting Started Guide by going to the Product Documentation & Downloads link under the User Administration & Documentation column of your NAB Transact login homepage.

1.4. Technical Overview

Direct Post is an online, secure credit card transaction system that integrates into a web programming environment, such as PHP or .NET, via the following steps that ensure transaction amount and response integrity.

Step 1: Generate a Fingerprint

A Fingerprint is generated in your web site code by a SHA1 hash comprising your seven digit NAB Transact Merchant ID, transaction password, the transaction type, transaction reference, payment amount and timestamp. This value is then presented in your payment form as a hidden field.

Step 2: Customer Submits Card Details to Direct Post

Your customer enters in their credit card details on a secure HTML form on your web site. The form is then submitted directly to Direct Post, which reduces the scope of your compliance with Payment Card Industry Data Security Standards (PCI DSS).

When accepting card details on your website, you will require an SSL certificate. It is your responsibility to obtain and configure the SSL certificate.

Step 3 (optional): Result Data Sent to a Callback URL

You can choose to pass result parameters in the background to a URL on your website, known as the Callback URL. This separates the browser redirect from your systemic update, ensuring that your website receives result data.

Step 4: Redirect to Result Page

Upon completion of the transaction, Direct Post redirects to your nominated Result URL and passes result parameters, including a result Fingerprint to protect the transaction result. Your system checks the Fingerprint, updates your database and displays the receipt to the customer.

1.5. Technical Overview for UPOP

UPOP uses a secure page, hosted by UnionPay and presented to customers by NAB Transact Direct Post.

Step 1: Generate a Fingerprint

A Fingerprint is generated in your web site code by a SHA1 hash comprising your seven digit NAB Transact Merchant ID, transaction password, the payment amount, transaction reference and timestamp. This value is then presented in your payment form as a hidden field.

Step 2: Customer Submits Payment Details to Direct Post

Your customer selects the payment option of UPOP. Card details are not submitted at this time. Payment details (amount, transaction reference, and fingerprint) are submitted to Direct Post via hidden fields, along with a payment choice of UPOP. The UPOP payment page will then be presented to the customer.

Step 3: Customer Submits Card Details to UPOP

Customer is presented with the secure UPOP hosted payment page by NAB Transact Direct Post. The customer enters their card details directly into the UPOP presented payment page and then submits the form for processing.

Step 4: Redirect to Result Page

Upon completion of the transaction, Direct Post redirects to your Result URL and passes result parameters, including a result Fingerprint to protect the transaction result. Your system checks the Fingerprint, updates your database and displays the receipt to the customer.

2 IMPLEMENTATION

2.1. General Information

2.1.1. Case Sensitivity

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

2.1.2. HTML Forms

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.

Direct Post only accepts POST data from an HTML form submitted by your customer on your website to initiate a transaction. Ensure that the "method" attribute is set to "post".

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

2.1.3. Acceptable Form Input Tags

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 sent to and 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. Form inputs follow the structure:

<input type="field_type" name="field_name" value="field_value">

2.2. Transaction URLs

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

2.2.1. Test URL

Test transactions are created by an HTML form submitted by your customer on your web site to:

```
<form method="post" action="https://demo.transact.nab.com.au/directpostv2/authorise">
```

2.2.2. Live URL

Live 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/live/directpostv2/authorise">
```

2.3. Standard Fields

The following form fields must be sent to NAB Transact for payment processing.

2.3.1. Merchant ID - EPS_MERCHANT

CLASS	Mandatory
FORMAT	Alpha-numeric, length 7
DESCRIPTION	Consists of your three digit NAB Transact Client ID used to login to the NAB Transact Management Portal, the two digit sub-account ID, and the two digit NAB Gateway ID. This merchant identifier value is not the same as the merchant number provided by your bank.

Your NAB Transact Merchant ID will be supplied to you by the NAB Transact Service Centre when your account is activated.

TYPICAL USE	**<input type="hidden" name="EPS_MERCHANT" value="XYZ0010">**

2.3.2. Transaction Type - EPS_TXNTYPE

CLASS Mandatory

FORMAT Numeric

DESCRIPTION Used to determine the processing type for an individual transaction and is included within the fingerprint. This is used to switch between payments, preauthorisations and the added features of Risk Management and 3D Secure. Payments and preauthorisations are described in the following sections.

Other transaction types are listed in Appendix 2: Transaction Types.

2.3.2.1. Payment

Payments are real-time, immediately authorised card transactions. Transaction information is passed from a payment form to your NAB Transact account for immediate processing. The transaction type for payments is equal to 0.

TYPICAL USE **<input type="hidden" name="EPS_TXNTYPE" value="0">**

2.3.2.2. Preauthorisation

A preauthorisation is a transaction that reserves funds on a credit card. This can then be completed at a later date so that the credit card is charged and you receive the funds. If the preauthorisation is never completed, it expires, usually after approximately five working days. After this, the reserved funds are again made available to the card holder.

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

To preauthorise an amount, submit all the fields exactly as they were for the PAYMENT (0) transaction type above, including the card details, but set the EPS_TXNTYPE field to 1 instead of 0.

TYPICAL USE **<input type="hidden" name="EPS_TXNTYPE" value="1">**

Once submitted, the result will be returned to your "EPS_RESULTURL" or, if applicable, your "EPS_CALLBACKURL", including the 'preauthid' field:

Example: Extra result field from a PREAUTH transaction

preauthid=516376

This field can then be used to complete the preauthorisation via the XML/API or Batch solutions.

2.3.3. Payment Reference - EPS_REFERENCEID

CLASS Mandatory

FORMAT String, min length 1, max length 60

*For UPOP only: Alpha-numeric, min length 8, max length 32, must be unique.

DESCRIPTION A string that identifies the transaction. This string is stored by NAB Transact as the Transaction Reference.

This field is typically a shopping cart id or invoice number and is used to match the transaction in NAB Transact to your application to aid in reconciliation.

TYPICAL USE **<input type="hidden" name="EPS_REFERENCEID" value="My Reference">**

2.3.4. Transaction Amount - EPS_AMOUNT

CLASS Mandatory, for all transaction types of Payment and Preauthorisation. Not required for Store Only transactions.

FORMAT Numeric, two decimal places, from 0.01 to 99999999.99

DESCRIPTION The total amount of the purchase transaction. This value must be a positive decimal value of dollars and cents e.g. $1.00 will be passed as $1.00. Please be careful to correctly specify the amount as Direct Post has no method of determining whether an amount has been correctly specified. By default, the currency is AUD (Australian Dollars).

Example: Setting the transaction amount

Scenario: A customer chooses items from your shopping cart totalling AUD $53.00.

TYPICAL USE **<input type="hidden" name="EPS_AMOUNT" value="53.00">**

2.3.5. GMT Timestamp - EPS_TIMESTAMP

CLASS	Mandatory
FORMAT	String, format "YYYYMMDDHHMMSS" in GMT (UTC).
DESCRIPTION	The GMT time used for Fingerprint generation. This value must be the same when submitted to generate a fingerprint as submitted with the transaction. NAB Transact validates the time within five minutes of current time. The time component must be in 24 hour time format. 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 Fingerprint. It is currently 22:24:53 on 20/05/2014 in Sydney (+10 hours from GMT). The time in GMT is 12:24:53 on the same day.

TYPICAL USE **<input type="hidden" name="EPS_TIMESTAMP" value="20140520222453">**

2.3.6. Fingerprint - EPS_FINGERPRINT

CLASS	Mandatory
FORMAT	String, length up to 60
DESCRIPTION	The Fingerprint is a protected 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 transaction details when submitting their card information. To generate a fingerprint, your system will need to create a SHA1 hash of the following mandatory request fields: EPS_MERCHANT|TransactionPassword|EPS_TXNTYPE|EPS_REFERENCEID|EPS_AMOUNT|EPS_TIMESTAMP Where the EPS_ prefixed fields are sent in the request and the Transaction Password is obtained from NAB Transact, which may be changed via the NAB Transact Management Portal.

Example: Setting the fingerprint

Fields joined with a | separator:

XYZ0010|abcd1234|0|Test Reference|1.00|20140224221931

SHA1 the above string: 7be3248e35ad189193d8ecd4273ad3b9fd069e90

<input type="hidden" name="EPS_FINGERPRINT" value="7be3248e35ad189193d8ecd4273ad3b9fd069e90">

TYPICAL USE **<input type="hidden" name="EPS_FINGERPRINT" value="7be3248e35ad189193d8ecd4273ad3b9fd069e90">**

This field is then submitted, along with the other Direct Post mandatory fields, to the customer payment page hosted on your website.

For methods of generating a SHA1 hash in your language please visit: http://code.wikia.com/wiki/SHA_checksum

2.3.7. Transaction Result URL - EPS_RESULTURL

CLASS	Mandatory
FORMAT	String, fully-qualified URL
DESCRIPTION	Used to set the secure page on your web site that must receive and interpret the transaction result and display the result to the customer. When a transaction is complete (approved or declined), Direct Post redirects the browser to this result page with the transaction result in a series of POST or GET fields. These fields are described in Section 2.4.

POST: NAB Transact retrieves the result data from the nominated Result URL on your website and renders the result page without redirecting to your Result URL.

GET: See Section 6.3 to redirect NAB Transact to your Result URL, and append the result parameters to your Result URL as a GET string based on RFC 2616 standards after being redirected. Please handle both GET and POST methods in this instance.

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 URL must also:

- 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.
- Be written as a fully-qualified URL. i.e. "https://...".
- Be a secure URL (unless you are submitting to the test environment) from a trusted SSL provider (not self-signed)

The result includes a Fingerprint that you can verify to check the integrity of the transaction result.

TYPICAL USE	**<input type="hidden" name="EPS_RESULTURL" value="http://www.myserver.com.au/result.asp">**

2.3.8. 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" and "EPS_EXPIRY YEAR" are all required for the transaction. The field “EPS_CCV” is required for all financial transactions. “EPS_CCV” is not required for the Store Only transaction type.

Visa and MasterCard have the card number and expiry date on the front, and a security number referred to as a CCV2 printed on the signature strip on the back of the card, appearing as a three digit number. For American Express cards, this is a four digit value printed on the front of the card.

2.3.8.1. EPS_EXPIRYMONTH

Payments are real-time, immediately authorised card transactions. Transaction information is passed from a payment form to your NAB Transact account for immediate processing. The transaction type for payments is equal to 0.

CLASS	Mandatory
FORMAT	String, min length 1, max length 2
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.

Notes:
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.
A leading zero is allowed.

*For UPOP payments this field must be NULL. Expiry date will be collected by the UPOP payment page.

TYPICAL USE	**<input type="text" name="EPS_EXPIRYMONTH" value="06">**

2.3.8.2. EPS_EXPIRYYEAR

CLASS	Mandatory
FORMAT	String, length 2 or 4
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.

Notes:
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.
Four digit years are accepted, with the first two digits ignored. E.g. 2016 will be treated as 16.

*For UPOP payments, this field must be NULL. Expiry date will be collected by the UPOP payment page.

TYPICAL USE	**<input type="text" name="EPS_EXPIRY YEAR" value="16">**

2.3.8.3. EPS_CCV

CLASS	Mandatory for financial transactions. Not Required for Store Only transactions.
FORMAT	Numeric, length 3 or 4
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.

Notes:
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 (CVV2) or a Card Verification Code (CVC), most notably in information provided by banks or card providers.

*For UPOP payments this field must be NULL. The CCV will be collected by the UPOP payment page.

TYPICAL USE **<input type="text" name="EPS_CCV" value="999">**

Example: Allow a customer to enter their card information

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

```
<input type="text" name="EPS_CARDNUMBER">
<select name="EPS_EXPIRYMONTH">
        <option value="01">01
        <option value="02">02
        <option value="03">03
        <option value="04">04
        <option value="05">05
        <option value="06">06
        <option value="07">07
        <option value="08">08
        <option value="09">09
        <option value="10">10
        <option value="11">11
        <option value="12">12
</select>
<select name="EPS_EXPIRYYEAR">
        <option value="2014">2014
        <option value="2015">2015
        <option value="2016">2016
        <option value="2017">2017
        <option value="2018">2018
</select>
<input type="text" name="EPS_CCV">
```

2.4. Transaction Result

After the transaction has been processed, a set of result parameters will be returned to the URL you defined in EPS_RESULTURL. You may then use these parameters within your defined Result URL program to update your system and display the desired outcome to the customer. It is recommended, however, that you use the Callback URL for your system update in order to separate your system update from the browser process. Refer to Section 2.6.2 for more information.

2.4.1. Merchant ID - EPS_MERCHANT

Result parameters are returned using the POST or GET methods with parameter names as described below. Some parameters will only be returned if a particular feature is used.

2.4.2. Standard Result Fields

2.4.2.1. summarycode

The one digit summary of the transaction result

1 = Approved

2 = Declined by the bank

3 = Declined for any other reason

Use "rescode" and "restext" for more detail of the transaction result.

2.4.2.2. 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 the Product Documentation & Downloads section of the NAB Transact login, located under the User Administration & Documentation column of the homepage.

2.4.2.3. restext

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

2.4.2.4. refid

The value of the EPS_REFERENCEID parameter from the transaction request. This value is returned to your processing system to allow matching of the original transaction request

2.4.2.5. txnid

The bank transaction ID. This 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 processing refunds.

2.4.2.6. settdate

The bank settlement date. 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 9.55pm AEST), then roll to the following business day. The settlement date is returned in the format "YYYYMMDD".

2.4.2.7. preauthid

The bank pre-authorisation ID returned by the payment gateway. This value is used when sending a pre-authorisation complete transaction via the XML API or Batch solutions.

2.4.2.8. pan

The first six and last three digits of the credit card number used in the payment request. E.g. 444433...111

2.4.2.9. expirydate

The four digit expiry date entered by the customer. E.g. 0813

2.4.2.10. merchant

The EPS_MERCHANT value used for the transaction.

2.4.2.11. timestamp

The GMT (UTC) time used for the response fingerprint of the format "YYYYMMDDHHMMSS". This value must be used when generating a string to compare to the response "fingerprint" value to validate the response. The time component must be in 24 hour time format.

2.4.2.12. fingerprint

A string used to validate the transaction output.

A SHA1 hash of the following fields in order, separated by "|":
merchant, transaction password, reference, amount, timestamp, summarycode

For example:
SHA1 hash the following pipe-separated fields:
XYZ0010|abcd1234|MyReference|10.00|20140525100000|1

Result: ca35bc8e6e44e887489e662c90f78ae3cdd77240

It is recommended that your system generates a fingerprint of the above values in order to ensure that this matches the fingerprint value returned in this field.

2.4.2.13. callback_status_code

The HTTP status code of the callback to the EPS_CALLBACKURL.

This can be used to determine if Direct Post was able to successfully contact your web server. See Section 2.6.2 for more information about implementing the Callback URL.

2.5. Example Payment Request and Response

Form fields required to make a card payment

Hidden fields:

```
<input type="hidden" name="EPS_MERCHANT" value="XYZ0010">
<input type="hidden" name="EPS_TXNTYPE" value="0">
<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="20140224221931">
<input type="hidden" name="EPS_FINGERPRINT" value="7be3248e35ad189193d8ecd4273ad3b9fd069e90">
<input type="hidden" name="EPS_RESULTURL" value="https://www.resulturl.com>"
```

Customer-entered fields:

```
<input type="text" name="EPS_CARDNUMBER" value="4444333322221111">
<input type="text" name="EPS_EXPIRYMONTH" value="05">
<input type="text" name="EPS_EXPIRYYEAR" value="2018">
<input type="text" name="EPS_CCV" value="123">
```

Typical approved response data for this transaction would be:

```
timestamp=20140224221931
callback_status_code=200
fingerprint=c83c01cb8c74e20212074d04c68e1e4b782e484a
txnid=726337
merchant=XYZ0010
restext=Approved
rescode=00
expirydate=052018
settdate=20140610
refid= Test Reference
pan=444433...111
summarycode=1
```

2.6. Optional Features

2.6.1. Currency - EPS_CURRENCY

If your account supports multicurrency, you may optionally set the currency of the transaction to one other than AUD

Set EPS_CURRENCY to any ISO three letter currency value that your account is enabled for

TYPICAL USE	**<input type="hidden" name="EPS_CURRENCY" value="USD">**

2.6.1.1. Getting configured for Multicurrency

If you would like your NAB Transact account to be configured for multicurrency, please contact your business banker or the NAB Merchant Sales team on 1300 338 767 option 1.

2.6.2. Callback URL - EPS_CALLBACKURL

CLASS	Optional
FORMAT	String, fully-qualified URL

DESCRIPTION	The URL on the merchant web site that accepts transaction result data as POST elements for the purpose of updating a client database or system with the transaction response, and to enable separation of the browser process from the update process. Result data fields are described in Section 2.4.

Notes:

- Set EPS_CALLBACKURL similarly to the EPS_RESULTURL.
- The result page may be almost any form of web page, including static HTML pages, CGI scripts, ASP pages, JSP pages, PHP scripts.
- The EPS_CALLBACKURL 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.
- The result fields may include a callback_status_code – the HTTP response code from your URL.
- Note that your callback URL must not contain multiple redirects or flash content or other content that may prevent Direct Post from successfully making a connection.

TYPICAL USE	**<input type="hidden" name="EPS_CALLBACKURL" value="http://myserver.com.au/result.asp">**

2.6.3. Result Page Redirect - EPS_REDIRECT

CLASS	Optional
FORMAT	String, values "FALSE" or "TRUE"
DEFAULT	FALSE
DESCRIPTION	Directs the system to redirect to the EPS_RESULTURL page to display the result to the customer, where r esult parameters are appended to the URL as a GET string. Validate the result fingerprint to ensure integrity of the bank response. Use the EPS_CALLBACK parameter if separate database update and page redirect URLs are required.

TYPICAL USE	**<input type="hidden" name="EPS_REDIRECT" value="TRUE">**

2.6.4. Pass through data

Additional fields such as session information or data can be passed to the gateway and returned with your result and callback data. This option can be enabled by setting EPS_CALLBACKPARAMS and EPS_RESULTPARAMS to TRUE. Additional parameters are either posted to the URL (if EPS_REDIRECT is false or omitted) or are appended to the URL as a GET string after the transaction result parameters (if EPS_ REDIRECT is true).

These must be unreserved fields. Reserved fields begin with "EPS_".

2.6.4.1. EPS_RESULTPARAMS

CLASS	Optional
FORMAT	String, values "FALSE" or "TRUE"
DESCRIPTION	Directs the system to append unreserved input fields to the EPS_RESULTURL. Additional parameters either posted to the URL (if EPS_REDIRECT is false or omitted) or are appended to the URL as a GET string after the transaction result parameters (if EPS_REDIRECT is true). Reserved fields begin with "EPS_".

TYPICAL USE	**<input type="hidden" name="EPS_RESULTPARAMS" value="true">**

2.6.4.2. EPS_CALLBACKPARAMS

CLASS	Optional
FORMAT	String, values "FALSE" or "TRUE"
DEFAULT	FALSE
DESCRIPTION	Directs the system to append unreserved input fields to the EPS_CALLBACKURL. Additional parameters posted to the URL in addition to the transaction result parameters. Reserved fields begin with "EPS_".

TYPICAL USE	**<input type="hidden" name="EPS_CALLBACKPARAMS" value="true">**

2.6.5. Risk Management

The Risk Management feature can assist merchants in evaluating the risk of a transaction based on rules set within the NAB Transact management portal.

Once you have enabled these rules, you can set the field "EPS_TXNTYPE" to include the Risk Management option and pass a series of additional payment parameters to the system to help validate your customer.

Note: Risk Management cannot eliminate fraud. It observes transaction patterns and conservatively judges whether a transaction is of higher risk. You should always use your own judgement before sending goods or supplying services based on the result of any transaction.

Example – Payment with Risk Management	
TYPICAL USE	**<input type="hidden" name="EPS_TXNTYPE" value="2">**

Please see 4.2 Appendix 2: Transaction Types for other Transaction Types that include Risk Management.

2.6.5.1. Risk Management Request Fields

Each Risk Management payment request must be submitted with a transaction type of 2. In addition, each request will require further fields submitted in order to evaluate against the configured ruleset.

Mandatory, along with the appropriate Transaction Type:

EPS_IP

CLASS	Mandatory when EPS_TXNTYPE includes Risk Management
FORMAT	String, length up to 15
DESCRIPTION	Payee's IPV4 IP Address – should be obtained from the card holder's browser. Typically a programmatic environment variable such as remote IP.

TYPICAL USE	**<input type="hidden" name="EPS_IP" value="203.123.456.789">**

Optional:

EPS_ZIPCODE

CLASS	Optional
FORMAT	String, length less than 30
DESCRIPTION	Payee's zip/post code

TYPICAL USE	**<input type="text" name="EPS_ZIPCODE">**

EPS_TOWN

CLASS	Optional
FORMAT	String, length less than 30
DESCRIPTION	Payee's town

TYPICAL USE	**<input type="text" name="EPS_TOWN">**

EPS_BILLINGCOUNTRY

CLASS	Optional
FORMAT	String, length 2, ISO 4217 currency code
DESCRIPTION	Payee's Country two letter code

TYPICAL USE	**<input type="text" name="EPS_BILLINGCOUNTRY">**

EPS_DELIVERYCOUNTRY

CLASS	Optional

FORMAT	String, length 2, ISO 4217 currency code
DESCRIPTION	Order delivery country two letter code
TYPICAL USE	**<input type="text" name="EPS_DELIVERYCOUNTRY">**

EPS_EMAILADDRESS

CLASS	Optional
FORMAT	String, length less than 30
DESCRIPTION	Payee's email address
TYPICAL USE	**<input type="text" name="EPS_EMAILADDRESS">**

Example: Sending Risk Management parameters with a transaction. Required (in addition to other required payment fields):

```
<input type="hidden" name="EPS_TXNTYPE" value="2">
<input type="hidden" name="EPS_IP" value="203.123.456.789"> Optional (any combination is acceptable):
<input type="hidden" name="EPS_ZIPCODE" value="2345">
<input type="hidden" name="EPS_TOWN" value="Melbourne">
<input type="hidden" name="EPS_BILLINGCOUNTRY" value="AU">
<input type="hidden" name="EPS_DELIVERYCOUNTRY" value="AU">
<input type="hidden" name="EPS_EMAILADDRESS" value="john@email.com">
```

2.6.5.2. Risk Management Result Fields

If the transaction passes Risk Management, you will receive the following result parameters:

rescode = Bank response code

restext = Bank response text

...

afrescode = 000

afrestext = Fraud check passed

If the transaction does not pass Risk Management you will receive:

rescode = Error code

restext = Error text

...

afrescode = Value other than 000

afrestext = Associated Risk Management result text

2.6.6. 3D Secure

3D Secure is 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.

To utilise this service, your merchant facility and NAB Transact account must be enabled for this. Once you have been enabled, you can instruct the system to use 3D Secure through Direct Post by changing the value of the mandatory EPS_TXNTYPE field. See section 4.2 Appendix 2: Transaction Types for more information.

You must also include the following fields in your payment requests:

2.6.6.1. 3D_XID

CLASS	Mandatory when EPS_TXNT YPE includes 3D Secure
FORMAT	String, length 20
DESCRIPTION	3D Secure Transaction ID string. MUST uniquely reference this transaction and MUST be 20 characters in length. Any ASCII characters may be used to build this string

Example: 3D_XID set as a timestamp padded with 0s for uniqueness: "20140614112034872000".

TYPICAL USE **<input type="hidden" name="3D_XID" value="20140614112034872000">**

2.6.6.2. EPS_MERCHANTNUM

CLASS	Mandatory when EPS_TXNT YPE includes 3D Secure
FORMAT	String, length less than 20
DESCRIPTION	Your online merchant number specified by your bank which has been registered for Verified by Visa or SecureCode, or both. This will be your eight digit NAB EB number, e.g. "22123456".

TYPICAL USE **<input type="HIDDEN" name="EPS_MERCHANTNUM" value="22123456">**

2.6.7. UPOP Payments

UnionPay Online Payment (UPOP) is the way that China UnionPay cardholders pay for goods and services online. UPOP uses a secure page hosted by UnionPay and is presented to customers by NAB Transact Direct Post. The UPOP payment page will directly accept the card number, expiry date and card security code.

This is an additional service that can be added to your NAB Transact account.

Once active, you can instruct the system to submit UPOP payments by setting the EPS_PAYMENTCHOICE to "UPOP".

EPS_PAYMENTCHOICE

CLASS	Optional
FORMAT	String, max length 30
DESCRIPTION	Field is used to select additional payment types. For UnionPay Online Payments this must be set to "UPOP". Else this field must be NULL or omitted.

TYPICAL USE **<input type="hidden" name="EPS_PAYMENTCHOICE" value="UPOP">**

Note the following additional integration requirements when submitting UPOP payments:

EPS_TXNTYPE of "0" (Payment) is the only accepted payment type for UPOP.

EPS_CARDNUMBER, EPS_EXPIRYMONTH, EPS_EXPIRYYEAR and EPS_CCV are to be left NULL. The cardholder will enter these details into the UPOP payment page directly. EXAMPLE: <input type="hidden" name="EPS_CARDNUMBER" value="">

EPS_REFERENCEID must be unique

EPS_REFERENCEID must be alpha-numeric and 8 to 32 characters in length

AUD and CNY are the only accepted currencies for UPOP

NAB Transact Risk Management and 3D Secure (Verified by Visa and MasterCard SecureCode) cannot be used in conjunction with UPOP payments.

2.6.8. Tokenization

Using NAB Transact's Customer Management, you can store your customer's card details in NAB Transact's secure database after a Direct Post transaction has been submitted and get back a Token. A Token is a string that represents a stored card number. If the card number changes, so does the token, therefore card numbers and tokens cannot be edited, they may only be added or deleted.

Once the customer's card details have been stored, you can perform subsequent transaction requests via the NAB Transact XML API or Batch solutions, using the Token in the requests to represent the stored card details. These types of payment requests are known as Triggered Payments.

You can also optionally use the Store Only method to store the customer's details without charging their card.

To enable card storage for either storage type, you will need to send through the following parameters in your requests:

EPS_STORE

CLASS	Mandatory for Card Storage
FORMAT	String, values "FALSE" or "TRUE"
DESCRIPTION	Directs the system whether to securely store the payer's card details in the NAB Transact database
DEFAULT	FALSE
DESCRIPTION	Set the value to TRUE to enable card storage

TYPICAL USE **<input type="hidden" name="EPS_STORE" value="true">**

EPS_STORETYPE

CLASS	Mandatory when the value is set to "TOKEN"
FORMAT	String, value "TOKEN"
DESCRIPTION	Defines the storage method used for a card

TYPICAL USE **<input type="hidden" name="EPS_STORETYPE" value="TOKEN">**

Direct Post will return the token in the result parameters.

Example: Set card storage with type Token by passing through the following extra parameters:

TYPICAL USE **<input type="HIDDEN" name="EPS_STORE" value="true">**

<input type="HIDDEN" name="EPS_STORETYPE" value="TOKEN">

2.6.8.1. Card Storage Result Fields

When EPS_STORE=TRUE, the following result fields are returned in addition to the standard result fields.

strescode
The primary indicator of the storage response.
Storage code Returns "00" if the CRN or Token was successfully stored. Returns a different string if the storage failed. The "strestext" describes the failure reason.

strestext
Storage response text. Contains a description of the storage result.

token
The system-generated token will be returned in this field. If the card has never been stored before, this will be a new value. If the card has been stored previously, the stored value will be returned.

fingerprint
If you choose to use the default Pay and Store method of card storage i.e. charging your customer's card when their details are stored, the standard fingerprint will be returned, as per the specifications outlined in Section 2.4.2.12.
If you choose to store your customer's card details using the Store Only method, the result fingerprint will be a SHA1 hash of the following fields in order, separated by "|":
EPS_MERCHANT|TransactionPassword|EPS_STORETYPE|EPS_REFERENCEID, timestamp, summarycode

Example: XYZ0010|abcd1234|token|Test Reference|20140711004448|1

Example Fingerprint Value: 640326582f556903cd2f65a761184944a7702b9d

It is recommended that your system generates a fingerprint of the above values in order to ensure that this matches the fingerprint value returned in this field.

2.6.8.2. Store Only
When you choose to store a customer's card details in NAB Transact when a Direct Post transaction is processed, you can optionally choose to Tokenize their card details without charging their card. This is known as the Store Only method.

When you use Store Only, the amount is not required. If you include the amount, this is ignored and is not stored against the customer's details.

To use Store Only, you must:

- Pass through the EPS_TXNTYPE value of 8 in your requests. This value is defined further in Section 2.3.2.

TYPICAL USE **<input type="HIDDEN" name="EPS_TXNTYPE" value="8">**

- Generate a fingerprint and pass this through as the EPS_FINGERPRINT value in your requests. This is a protected record of the transaction details and prevents a customer modifying the details when submitting their card information. Your system will need to create a SHA1 hash of the following fields in order, separated by "|". These fields are different to the standard fingerprint fields described in Section 2.3.6.

EPS_MERCHANT|TransactionPassword|EPS_TXNTYPE|EPS_STORETYPE|EPS_REFERENCEID|EPS_TIMESTAMP

Example:

XYZ0010|abcd1234|8|token|Test Reference|20140711004448

TYPICAL USE **<input type="HIDDEN" name="EPS_FINGERPRINT" value=" 7be3c767b1194fb49f717abd294111ea238c74a5">**

When you use Store Only, the following financial transaction result fields are not returned:

- rescode
- restext
- txnid
- settdate
- preauthid

2.7. Testing
As you build your system, you can test functionality when necessary by submitting parameters to the test URL found in Section 2.2 'Transaction URLs'. You can generate a fingerprint and then complete the transaction by using the card details listed below.

You must also ensure that you use your 7 digit Merchant ID and your Test Transaction Password supplied to you in your activation email, or NAB Transact's test details. Section 1.2.1 details these requirements.

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 / 17 (or any date in the future)

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. See the examples below.

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

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)

2.8. Troubleshooting

You may experience one of the following issues when integrating and testing NAB Transact Direct Post. In addition to this section, help is available from our Support team by calling 1300 369 852 option 1 or emailing support@transact.nab.com.au.

2.8.1. Invalid Fingerprint

This error can be returned by NAB Transact after the payment page form post is submitted from your website. This may be caused by:

- The Merchant ID or Transaction Password used in the fingerprint or form post being incorrect.
  Please refer to the following section of your NAB Transact Activation email to verify these details.

Getting Started

Live Direct Post and API Implementation

- **Merchant ID (or "EPS_MERCHANT"): <Your Merchant ID>**
- **Live Transaction Password: <Your live transaction password>**

Test Direct Post and API Implementation

- **Merchant ID (or "EPS_MERCHANT"): <Your Merchant ID>**
- **Test Transaction Password: <Your test transaction password>**

- The requests from your website are being sent to the incorrect payment URL. If you are submitting payments to the test URL, ensure that you use your test transaction password. If you are submitting payments to the live URL, ensure you are using your live transaction password. The Merchant ID remains the same for both environments.
- There is a discrepancy between the values of the fields included in the fingerprint, and the values of the fields included in the form post. All fields included in the fingerprint must be valid and match the hidden fields that are sent in the payment form post, with the exception of the transaction password which should only be included in the fingerprint.

2.8.2. Invalid Parameter

This error can be returned by NAB Transact when a parameter in the payment form post is invalid. The response will specify which particular parameter is invalid. Proper validation must exist on your website for all customer-facing fields on your payment page to ensure the payment can be processed. For Invalid Fingerprint error troubleshooting, please refer to the above section.

Example:

An invalid Expiry date of 12/2013 is entered by the customer and passed from the payment form to NAB Transact. A response of 'Invalid parameter EPS_EXPIRYYEAR' is then returned by NAB Transact.

2.8.3. Blank Result URL page

A blank result page can be caused by NAB Transact being unable to retrieve the POST result data from your nominated Result URL and render the data to the NAB Transact result page. This may be due to an invalid EPS_RESULTURL value being submitted.

To troubleshoot this issue, investigation will need to be performed by your web developer as to why NAB Transact cannot retrieve the result data from your nominated Result URL. Requirements for the Result URL are outlined in Section 2.3.7.

Alternatively, you can use the GET method to retrieve the result data by passing through the field of EPS_REDIRECT with each payment request and setting the value to 'TRUE'. This tells NAB Transact to redirect the customer's browser to your Result URL, append the result data to your Result URL as a query string, and display the result on your result page.

2.8.4. Declined test payment

When submitting to the test environment, a payment can decline if your test does not include a cent amount of 00, 08, 11 or 16 e.g. $1.00, $1.08, $1.11, $1.16. Each declined response code will equal the cent amount passed through.

Example:

You send through an amount of $10.05 when testing. A declined response code of 05, and its associated response text, 'Do Not Honor', will be returned.

Please ensure you send through the correct cent amounts to simulate an approved response.

2.8.5. Invalid Merchant

This error can be returned by NAB Transact when an invalid Merchant ID and/or Transaction Password is included in the fingerprint when implementing Direct Post v1. It is recommended that Direct Post v2 is implemented to utilize all Direct Post features.

2.8.6. Result data not received or displayed

Your website may be experiencing an issue with either the result page not being rendered via the Result URL field using GET or POST, or result data not being returned in the background to your nominated Callback URL.

This may be due to an issue with your SSL certificate implementation.

The Direct Post interface uses Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) to communicate with the NAB Transact

Payment Gateway. HTTPS mechanism uses SSL to encrypt and decrypt the request and response payload. NAB Transact uses the SSL certificate issued by VeriSign, Inc. Your website's application should have access to the VeriSign Root Certificate to communicate with the NAB Transact Payment Gateway. Majority of the Application Servers, Run Time Environments and Operating Systems are shipped with VeriSign Root Certificate. VeriSign Root Certificate can be downloaded from http://www.verisign.com/support/roots.html

Please refer to VeriSign® SSL FAQs located at

http://www.verisign.com.au/repository/faq/rootCA_faq.shtml for more information.

Notes:

- Third party websites are available for you to check the status of your SSL certificate. If no issues are found, there may be an issue with NAB Transact's payment server not supporting your SSL's Certificate Authority (CA).
- Your web host cannot use Server Name Indicators (SNIs) for determining which SSL certificate to serve. This is not supported by NAB Transact's systems.

2.8.7. 03 – Invalid Merchant

This response code can be returned when a customer is attempting to make a payment using their American Express or Diners card details and you do not accept these card types. If you do not yet accept these card types, please ensure only Visa and Mastercard is enabled on your website. You can accept these card types by establishing a separate merchant facility with the relevant card provider. Contact details for each provider are shown on page 1.

3 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.

CVV
Cardholder Security Code. This is an extra code printed on the back of a Visa, MasterCard, or Diners card, 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 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 Direct Post.

HTML
Hypertext Markup Language. The language interpreted by web browsers. This is the language used to create your Direct Post 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 Direct Post from your order form.

J Secure
JCB's brand name for its version of 3D Secure. Refer also to 3D Secure.

Log Date/Time
The date and time that the transaction was processed via Direct Post. Log Date and Time helps to tie a transaction back to your business system and assists in searching (via the NAB Transact Management Portal) for transactions which occurred during a specific period. Refer also to Settlement Date.

Client ID
Your NAB Transact Client ID used to specify which account payments are made through.

Merchant Number
Your bank's merchant number.

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.

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 not transfer those funds to the merchant's account until a follow up Complete transaction is performed. Refer also to Complete and Payment.

Response Code
A numeric code associated with a transaction to indicate a specific transaction's processing result. Transactions which are successfully passed through the banking system are returned with a two digit response code allocated by the banking system. Transactions which were rejected during Risk Management processing or which encountered technical problems and therefore were not successfully returned by the banking system will be allocated a 3 digit response code by NAB Transact. A full list of response codes can be found within the Product Documentation & Downloads section of the NAB Transact login, located under the User Administration & Documentation column on the homepage.

Settlement Date
The date which funds associated with successful transactions are transferred to your settlement account. Settlement is usually same day for transactions which have been processed by your bank before 6-10:00 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 Socket 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 NAB Transact login password, however, it can be changed via your NAB Transact 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 Log In. Transaction Reference (or any part of it) is an important search criterion within the NAB Transact Log In.

Transaction Source
The point of origin of a transaction. The transaction details of each Direct Post transaction within the NAB Transact login will show the source as Direct Post.

Transaction Type
The type of processing requested by this transaction. Valid Transaction Types are Payment and Pre-authorisation. Each of these is individually explained in more detail in this Glossary.

UPOP
UnionPay Online Payment (UPOP) is the way that China UnionPay cardholders pay for goods and services online. UPOP works like a digital wallet and uses a secure page hosted by UnionPay and presented to customers by NAB Transact Direct Post. The UPOP payment page will directly accept the card number, expiry date and card security code. Alternatively, the UnionPay customer can choose other ways to authorise their payment (such as a link to their Internet Banking service).

Verified by Visa
Visa's brand name for its version of 3D Secure. Refer also to 3D Secure.

4 APPENDICES

4.1. Appendix 1: Summary of Accepted Input Fields

Mandatory	Optional	Risk Management	3DSecure
EPS_MERCHANT	EPS_CURRENCY	EPS_IP	3D_XID
EPS_TXNTYPE	EPS_REDIRECT		EPS_MERCHANTNUM
EPS_AMOUNT*	EPS_CALLBACKURL	**Risk Management (Optional)**	
EPS_REFERENCEID	EPS_RESULTPARAMS	EPS_FIRSTNAME	
EPS_TIMESTAMP	EPS_CALLBACKPARAMS	EPS_LASTNAME	
EPS_FINGERPRINT	EPS_PAYMENTCHOICE	EPS_ZIPCODE	
EPS_CARDNUMBER+	EPS_STORE	EPS_TOWN	
EPS_EXPIRYMONTH+	EPS_STORETYPE	EPS_BILLINGCOUNTRY	
EPS_EXPIRYYEAR+		EPS_DELIVERYCOUNTRY	
EPS_CCV*		EPS_EMAILADDRESS	
EPS_RESULTURL			

* Not required for Store Only transactions.
+ Not required for UPOP transactions.

4.2. Appendix 2: Transaction Types

Transaction type codes define the type of financial transaction processed by NAB Transact, and may be one of the following, depending on the type of transaction.

Code	Type	Description
0	PAYMENT	A card payment/purchase transaction. Note: This is the only accepted type for UPOP payments
1	PREAUTH	Used to pre-authorise an amount on a card. The result parameters include the "preauthid" which must be stored and used when completing the pre-authorisation
2	PAYMENT with Risk Management	A card payment/purchase transaction with the optional Risk Management service
3	PREAUTH with Risk Management	A card preauthorisation transaction with the optional Risk Management service
4	PAYMENT with 3D Secure	A card payment/purchase transaction with the optional 3D Secure service
5	PREAUTH with 3D Secure	A card preauthorisation transaction with the optional 3D Secure service
6	PAYMENT with Risk Management and 3D Secure	A card payment/purchase transaction with the optional Risk Management and 3D Secure services
7	PREAUTH with Risk Management and 3D Secure	A card preauthorisation transaction with the optional Risk Management and 3D Secure services
8	STORE Only	A store only card storage request where the card is not charged