PayWay

PayWay Net Developer's Guide

Version 5.0 17 Jul 2011

Release Date	Version	Description
12 Mar 2007	1.0	Initial Version
18 Nov 2007	2.0	Expand HTTP Parameter descriptions and add appendices.
17 Apr 2008	2.1	Added return_linl_url_pre_payment and return_link_text_pre_payment parameters
23 May 2008	2.2	New security features
29 Sep 2008	3.0	Reviewed and updated documentation to reflect current functionality
15 Nov 2009	4.7	Re-wrote and condensed document
17 Jul 2011	5.0	Added PayPal.
22 Jul 2012	5.7	Described how to ask for hidden fields in browser redirect
16 Aug 2012	5.11	Described how to ask for fields in default server to server notification
20 Jun 2013	5.13	Added details of test cards for Fraud Guard

Table of Contents

1 Introduction

PayWay Net is a secure, flexible online payment system. It can be used as a stand-alone bill payment website or integrated with your website. You can offer your customers credit card payments[1] and PayPal payments[2].

NOTE: We advise against embedding PayWay payment pages into frames or iframes. If this is done, the customer's browser may treat the PayWay session cookies as 'third party' (PayWay has a P3P default policy but some browsers do not support this standard). So, unless the customer's browser is set to allow 'third party' cookies (or supports P3P) this will cause issues. Typical issues are no PayWay page being displayed or the customer receiving a timeout.

1.1 Shopping Cart Quick Start

- Obtain your PayWay Login and initial password
- Sign-in to PayWay and click on **Setup Net**
- Customise look and feel by uploading style-sheet and images

If your shopping cart does not have a PayWay module available:

- Download sample code and step through setup wizard
- Implement secure token request
- Refer to Appendices of this document for parameters
- Commence testing with `merchant_id=TEST` and/or paypal_email=test@example.com
- When ready, Go Live as described in Chapter 6

1.2 Your PayWay Login Name and Password

You will require a login to PayWay to:-

- Download Documentation,
- Download Sample Code,
- Configure PayWay Net,
- Link a PayPal account to your PayWay facility,
- View test payments you have conducted.

TIP: If you are a web developer, you may need to ask the business owner to give you access to PayWay. To do this, the business owner must sign-in to PayWay and choose **Administration** and then **Manage Users**.

Visit **www.payway.com.au** and click on **Sign In**. On first sign in, you will be asked to change your password and answer security questions. Keep a copy of your username and password in a secure location. If you require a password reset, you can do this online by answering your security questions.

Choose **Setup Net** in the menu to access documentation, samples and configuration.

[1] Requires that you be approved for a Westpac Merchant Facility.
[2] Requires that you setup a PayPal Business or PayPal Premium account.

1.3 Free Test Facility

For a free test facility (or to purchase PayWay Net), contact your Relationship Manager or a Customer Care Banking Representative:

- Phone: 1300 368 098
- Email: prioritysegments@westpac.com.au
- Apply online: Visit www.payway.com.au and click **Apply Now**

Provide your company name, preferred login name and email address.

1.4 Sample Code

We have provided sample code for:

- pure HTML,
- JSP,
- PHP,
- C# .NET

To access the sample code, sign-in to PayWay and click on **Setup Net** and then click **Downloads**.

1.5 PayWay Payment Cards

If you are using PayWay Payment Cards, you do not need to configure PayWay Net. PayWay Net will be automatically setup to work with the information printed on the payment cards when you complete the **Setup Payment Cards** wizard.

2 Configuring PayWay Net

PayWay Net is configured through the **Setup Net** pages. Access these using your PayWay login (see section 1.2).

Once logged in to the PayWay website, your **Biller Code** will appear on the *top-right* of each page. Your biller code is included when you send information to PayWay Net or is entered by your customer if you have no website.

From there, choose the level of integration you want to use and click the "Next" button down the bottom right. These pages will allow you to configure your payment gateway, and provide helpful tips on each of the configuration options.

The integration options are repeated here:

2.1 Bill Payments - No Website

Required Technologies: None

Select this option if you do not have your own website, but you would like to allow your customers to make payments over the Internet. Payments will be made using the PayWay website. This option requires no knowledge of HTML or website concepts.

2.2 Bill Payments - Simple Link

Required Technologies: Web Site including creating links to PayWay
Example Code: HTML

Select this option if you have your own website and can update it to have a html link or button that will take your customer to the PayWay website so that they can make a payment.

This option requires basic knowledge of HTML and website concepts.

2.3 Bill Payments/Shopping Cart

Required Technologies (depending on options you select):

- A dynamic back-end which can send a HTTPS POST directly to PayWay server,
- The ability to make an outbound HTTPS connection to PayWay through your proxy and firewall (for secure token request),
- A valid SSL certificate issued by a trusted certificate authority (for server to server payment notification),
- A dynamic back-end which can receive and parse HTTPS requests with parameters or can parse XML (for customising receipt page),
- The ability to decrypt and verify data encrypted using AES with Cipher Block Chaining (for customising receipt page)

Example Code: JSP, C# .NET, PHP

Select this option if you have your own website which includes a commercial shopping cart application, shopping cart-like functionality, or captures customer information that you wish to display on the payment pages.

This option allows the highest level of integration with the PayWay Net webpages and requires advanced knowledge of HTML and website concepts.

In addition to the options available to simple link customers, you can pass parameters for information fields to display to the customer, hidden fields to be displayed on internal invoices and products in the shopping cart (chapter 3).

You can request a server-to-server payment notification for straight-through processing (chapter 4), and customise the receipt page (chapter 5). Look and feel can be changed by uploading images and a custom style sheet to PayWay.

2.4 Linking a PayPal Account

If you wish to accept live payments via PayPal you will require a PayPal Business or Premier account. You can use an existing one or create a new one.

Your PayPal Business or Premier account is linked to PayWay as follows:-

1. Sign-in to PayWay

2. Click on **Administration** and then **Manage PayPal Accounts**

3. Click **Link Another PayPal Account**

4. Enter the email address of your account and click **Next**

   You will be redirected to PayPal.

5. Sign in to PayPal using your PayPal email address and password

6. Click **Grant Permissions** to allow PayWay to use your PayPal account

   This informs PayPal that you allow PayWay to process on your behalf.

7. In order to enable PayPal, add the parameter `paypal_email` with the value of the email address you linked above when sending parameters from your website to PayWay.

3 Sending Parameters to PayWay

3.1 Sending Parameters via Form Inputs

The HTML sample code provides an example of how to send POST parameters to PayWay. These are used to specify information to display to the customer, hidden data that you would like posted back to your server and products in the shopping cart.

Example Code: HTML

In addition to the parameters you post to configure each transaction, you must always post your Biller Code as the value of a parameter named `biller_code`. If you are using Shopping Cart configuration, you must also pass either your Merchant ID as the value of the `merchant_id` parameter, or your PayPal email address as the value of `paypal_email`.

3.1.1 Security risk of passing parameters as form inputs

Using HTTPS only secures the communication channel between the browser and the web-server. The customer is in full control of their computer and can easily use software such as browser plug-ins to modify data. Parameters that you send from your server to browser for it to post to PayWay could be tampered with. This would allow a fraudster to order many items from your website and then modify the total payment amount to $1.00.

This security risk may be addressed by:-

- Verifying transaction details after the payment has occurred,
- Reconciling transactions at end of day before shipping goods,
- Using a secure token request.

If you are setting up a bill payment or donation website, then modification of the payment amount does not represent a security risk so long as you update your system with the actual amount paid.

3.2 Sending Parameters via Secure Token Request

Tokens allow you to send parameters directly from your server to PayWay, bypassing the security risk described above.

3.2.1 Pre-Requisites

In order to use secure token requests, your website must have:-

- a dynamic back-end which can send a HTTPS POST directly to the PayWay server,
- the ability to make an outbound HTTPS connection to PayWay through your proxy and firewall

Example Code: JSP, C# .Net, PHP.

3.2.2 Secure Token Request

Under a secure token scenario, the shopping cart parameters are passed directly from your server to PayWay. This means that the customer cannot tamper with parameters.

The secure token request works as follows:

1. Your customer's browser requests the checkout page from your server
2. Your server sends a token request directly to PayWay. The token contains all fields from your shopping cart (e.g. total payment amount, products)
3. PayWay stores the cart details and responds with a security token
4. Your site returns a HTML page to the browser including a form containing only your biller code and the token. The HTML form instructs the browser to POST directly to the PayWay server when submitted
5. The customer's browser displays the HTML form to the customer
6. The customer submits the HTML form, and the browser sends it directly to PayWay
7. PayWay looks up the shopping cart details based on the token and the payment flow continues.

3.2.3 What is a token?

After registering the shopping cart parameters with the PayWay server through a token request, you will receive a randomly generated string of characters which is called a token. When the customer arrives at the PayWay website via their browser, PayWay looks-up the shopping cart details from the token. Tokens are valid for 1 hour after they have been created, and can only be used once each.

3.2.4 How do I request a token?

Refer to the sample code for how to request a token. Your server makes an outbound HTTPS connection to the PayWay server. You must provide a `biller_code`, `username` and `password` as parameters in your token request. Tokens are only accepted for a list of IP addresses that you configure in Setup Net wizard.

3.3 Parameters

The built-in parameters you can pass to PayWay are listed in Appendix A – PayWay Request Parameters and shown in the example code. You can create your own parameters for information fields, hidden fields and products.

3.3.1 Information Fields

Information fields are additional fields that you wish to display on the payment pages. You provide a list of information fields using built-in parameters `information_fields` and `suppress_field_names` as follows:

Parameter Name	Parameter Value
information_fields	`Name,Address,Address2`
suppress_field_names	`Address2`
Name	`Bob`
Address	`15 Bob Street`
Address2	`Bobsville`

These parameters will appear in a tabular format as transaction details on the payment page. If you do not wish to display the label of an information field (say, for Address2) you can suppress field names. This is done with `suppress_field_names`, in the same format as `information_fields`.

3.3.2 Hidden Fields

Hidden fields contain information that is not displayed to the customer[3] but may be returned to your website via:

- server to server payment notification,
- browser redirect after payment (if specified in URL).

Hidden fields are visible when you sign-in to PayWay and view transactions.

You can instruct PayWay to hide fields using the `hidden_fields` parameters as shown in the example below. In this example, `PromotionCode` and `PartnerCode` are hidden fields.

Parameter Name	Parameter Value
hidden_fields	`PromotionCode,PartnerCode`
PromotionCode	`A93DS`
PartnerCode	`TYE`

3.3.3 Product Fields

Parameters which are not built-in parameters and not listed as hidden fields or information fields will be interpreted as product fields.

TIP: If you make a mistake on a field name it will appear as a product. If you see products appearing that you don't remember specifying, check for the product name in your form.

TIP: Use each product name only once.

[3] However, your customers may be able to see this information using "View Source" in their browser if you are not using secure token requests to pass the parameters to PayWay.

The format of product fields is as follows:-

Parameter name	Parameter Value
The name of product	*[<quantity>,]<price>*
DVD	5,20.5
OLED TV	9999.99

These examples:

- Add 5 DVDs worth $20.50 each to the transaction.
- Add one OLED TV worth $9999.99 to the transaction.

TIP: Ensure you do not format the amount or quantity with commas as this will result in incorrect interpretation of the field by PayWay.

PayWay will calculate the total product costs based on all products. There are options for calculating and displaying GST using `gst_rate`, `gst_added` and `gst_exempt_fields`. See Appendix A – PayWay request parameters.

3.4 Customising Credit Card Details Entry Page (Advanced)

Generally, credit card details are input by the customer on the PayWay website. This is the simplest method. The page can be branded by uploading a style sheet and logos and content can be modified via information and product fields.

If this level of customisation is not sufficient, you can design your own page requesting credit card details so long as:

- You pass the shopping cart parameters via a token request,
- The credit card details are posted directly to PayWay and not your server

This works as follows:

1. Your customer's browser requests the credit card input page from your server.
2. Your server sends a token request directly to PayWay. The token contains all parameters from your shopping cart (e.g. total payment amount, products)
3. PayWay stores the cart details and responds with a security token
4. Your server responds with a HTML form to the browser. The HTML form includes fields for entering credit card details as well as hidden input fields for the `token` and `biller_code`. The HTML form instructs the browser to post directly to the PayWay server when submitted.
5. The customer's browser displays the HTML form to the customer
6. The customer enters their credit card details and submits the form
7. The browser sends the credit card details and the token directly to PayWay over an SSL connection

8. PayWay looks up the shopping cart details based on the token and processes a transaction against the credit card details in the POST

9. PayWay displays the receipt page (or redirects to your receipt page, see chapter 5).

TIP: Because the customer will still see a PayWay page if they enter incorrect card details, it is recommended that you upload a customised style sheet and a logo on the Biller Code page of PayWay Net Shopping Cart setup.

This mode of integration is not available when you are conducting a PayPal transaction.

3.4.1 Credit Card Details and PCI-DSS Obligations

The credit card details ***must*** be submitted ***directly*** to the PayWay `MakePayment` page. If credit card details enter your network then your organisation's obligations under the Payment Card Industry Data Security Standard requirements are increased. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. For more on PCI DSS, please see: **https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml**

TIP: If you are developing in .NET, you will need to write in-line ASP code on the hand-off page to prevent the HTML designer from rendering pages which post card details back to your server.

4 Receiving Payment Notification

PayWay Net can notify you with the result of each individual payment to allow you to process the order. This notification can be sent:-

- Via email to your nominated email address,
- Directly from PayWay to your server over HTTPS for straight-through processing.

Configure these options using the **Setup Net** menu option.
The remainder of this chapter discusses the HTTPS payment notification option.

4.1 Pre-Requisites

In order to use server to server payment notification, your website must have:

- a valid SSL certificate issued by a trusted certificate authority,
- a dynamic back-end which can receive and parse HTTPS requests with parameters or can parse XML.

Example code is provided for: JSP, C# .NET and PHP

4.2 Security

It is important for you to verify that the notification originated from the PayWay server and not a fraudster. To allow you to verify this, a username and password are included in each notification.

Your website must check the username and password on each notification to ensure that the request came from the PayWay server. If the username or password is not correct, you must ignore the notification.

To find your PayWay Net server to server payment notification username and password refer to the Configuration section below. This is not the same password that you use to sign-in to the PayWay website.

Why is an SSL certificate required for server to server payment notification?
Sending the notification over SSL ensures that the encrypted notification cannot be read by a malicious third-party on the Internet. As your SSL certificate was issued by a trusted certificate authority, it also guarantees that PayWay server is connecting to your web-server (and not another fraudulent server as in the case of DNS poisoning attacks).

4.3 Configuration

To configure server to server payment notifications use the **Setup Net** pages in PayWay. You must be using the Billing Payments/Shopping Cart configuration. Enter your URL under the **Server-to-Server Payment Notification** section. Your server to server payment notification username and password are shown on the next page.

PayWay will send parameters listed in Appendix B – Payment Notification Parameters. This configuration is recommended.

If you leave the Notification Post Type blank, PayWay will send parameters that you request in your URL. See 10.2 Default Post Type.

4.4 Processing the Payment Notification

The page you write to receive the payment notification request must return an HTTP status of 200 (success), or PayWay will post the same notification to you again. You should only return a status of 200 if you have successfully processed the response and saved the payment to your database.

You should check that your server has not previously processed a notification for the given receipt number.

If after three retries your server does not return a 200 response we will send you an email notification and stop retrying that particular payment notification.

5 Browser Return Links and Redirect

The purpose of Browser Returns Links and Redirect is to display appropriate web pages to your customer. PayWay Net can be configured with:-

- A button linking back to your website if the customer decides to continue shopping rather than completing the payment,
- A button linking back to your website on the payment receipt page,
- To redirect the browser to your website instead of displaying a payment receipt page (advanced).

When redirecting after payment, PayWay will provide an encrypted list of ampersand delimited parameters and instruct the customer's browser to pass them to your site. The encrypted parameters include details about the outcome of the transaction.

Use this method to display a customised receipt page.

Do not use this as a method to track payments. It is more difficult to implement than server-to-server messaging. It is also far less reliable. Anything that causes the customer's browser not to redirect would prevent your site from receiving payment notification. The browser could also send more than one request to your server.

5.1 Pre-Requisites

To create a customised receipt based on the outcome of the transaction, your website must have:-

- a dynamic back-end which can receive a parse GET parameters,
- the ability to decrypt and verify data encrypted using AES with Cipher Block Chaining.

Example Code is provided for: JSP, C# .NET, PHP.

5.2 Configuration

To configure browser redirect use the **Setup Net** pages in PayWay. You must be using the Billing Payments/Shopping Cart configuration. Enter your URL under the **Browser Return** section. If you wish to receive information and hidden fields, specify the name of the fields as shown in this example:

www.example.com?PromotionCode&Name&Address

If you wish to decrypt the payment information, step to the "Security Information" page and note the HTTP Parameter Encryption key.

5.3 Decrypting Parameters

The example code shows how to decrypt the parameters.

The parameters are encrypted using AES with Cipher Block Chaining, using PCKS-5 Padding. The decryption algorithm should be initialised with a 16 byte, zero-filled

initialization vector, and should use your encryption key (which can be found on the Security page of PayWay Net Shopping Cart setup).

Before decryption, the parameters passed with the redirect will appear as follows:

```
EncryptedParameters=QzFtdn0%2B66KJV5L8ihbr6ofdmrkEQwqMXI3ayF7UpVlRheR7r5fA6
IqBszeKFoGSyR7c7J4YsXgaOergu5SWD%2FvL%2FzPSrZER9BS7mZGckriBrhYt%2FKMAbTSS8F
XR72gWJZsul9aGyGbFripp7XxE9NQHVMWCko0NlpWe7oZ0RBIgNpIZ3JojAfX7b1j%2F5ACJ79S
VeOIK80layBwCmIPOpB%2B%2BNI6krE0wekvkkLKF7CXilj5qITvmv%2FpMqwVDchv%2FUNMfCi
4uUA4igHGhaZDQcV8U%2BcYRO8dv%2FnqVbAjkNwBqxqN3UPNFz0Tt76%2BP7H48PDpU23c61eM
7mx%2FZh%2Few5Pd0WkiCwZVkSZoov97BWdnMIw5tOAiqHvAR3%2BnfmGsx

Signature=huq1shmZ6k7L5BYxjGI2lJvQxffqa%2FogZR5oO8Ln2oc%3D
```

The signature is a base-64 encoded MD5 hash of the encrypted text, and can be used to verify that the text was transmitted correctly.

After decryption, the parameters will appear as follows:

bank_reference=1234&card_type=VI&payment_amount=100&PromotionCode=ABCD&...

For details of parameters, see Appendix C – Browser Redirect Parameters.

6 Testing and Going Live

For merchants who have selected the *"Bill Payments/Shopping Cart – I need to pass across information from my website"* configuration, we provide a test merchant which simulates responses rather than sending the transaction to the live banking network.

This test merchant is accessed through the normal production URL, but you provide a value of `TEST` for the `merchant_id` parameter.

If you are using PayPal, provide `test@example.com` for the `paypal_email` parameter.

When you are ready to go live:-

- Using **Setup Net** click the **Go Live** button,
- Modify your application to pass your live `merchant_id`, rather than TEST
- If you wish to use PayPal, link your PayPal account to PayWay (see section 2.4)
- Modify your application to pass your live `paypal_email`, rather than `test@example.com`
- If your live system is hosted separately to your test system and you are using secure token requests, you must add additional IP addresses through the Setup Net pages.

You can continue to use the TEST merchant and `test@example.com` PayPal email id after you have gone live.

6.1 Test Card Numbers

When using the test merchant, only the card numbers in Table 6.1 are valid. All other card numbers will return a response of "42 No Universal Account". Each card number will return a specific response as detailed in Table 6.1

5163200000000024	02/19	847	If Fraud Guard is active 34 otherwise 08	Fraud Guard	Declined if Fraud Guard is active
5163200000000032	02/19	847	If Fraud Guard is active 34 otherwise 05	Fraud Guard	Declined

Table 6.1, so if you want to test a card which has low funds, you would use card number 4564710000000020 with an amount higher than $10. Note that if you enter an incorrect expiry date for one of the test cards, you will get a response of 54. If you enter an incorrect CVN, you will get a response of 01 or 05 depending on the card type.

Cards listed as "Fraud Guard" will decline if you have Fraud Guard enabled on your facility.

The test merchant simulates a live gateway but may be used without any risk of transactions actually being processed through the banking system.

Card Number	Expiry	CVN	Response	Description	Transaction Status
4564710000000004	02/19	847	08	Visa Approved	Approved
5163200000000008	08/20	070	08	MC Approved	Approved
4564710000000012	02/05	963	54	Visa Expired	Declined
4564710000000020	05/20	234	51	Visa Low Funds ($10 credit limit)	Declined
5163200000000016	12/19	728	04	MC Stolen	Declined
4564720000000037	09/19	030	05	Visa invalid CVV2	Declined
376000000000006	06/20	2349	08	Amex	Approved
343400000000016	01/19	9023	62	Amex Restricted	Declined
36430000000007	06/22	348	08	Diners	Approved
36430000000015	08/21	988	43	Diners Stolen	Declined
5163200000000024	02/19	847	If Fraud Guard is active 34 otherwise 08	Fraud Guard	Declined if Fraud Guard is active
5163200000000032	02/19	847	If Fraud Guard is active 34 otherwise 05	Fraud Guard	Declined

Table 6.1 –Test card numbers

6.2 Test PayPal Transactions

You can test the integration between your website and PayWay using a simulation of PayPal provided by PayWay[4]. You can use any details for the buyer on the PayPal simulation page.

[4] PayWay does not make use of the PayPal Sandbox.

7 Card Types Accepted

PayWay Net accepts the following card types via your Westpac Merchant Facility:

- Visa
- MasterCard

You may also accept the following card types if you have a merchant facility with the charge card company. You can contact the charge card company on the number below to arrange a merchant facility:

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

Refer to the PayWay User Guide for information on setting up these in PayWay once you have established your charge card merchant facility.

8 Support

For issues relating to your Merchant agreement with Westpac, contact Merchant Business Solutions on 1800 029 749.

For issues relating to your Merchant agreement with American Express, contact Amex on 1300 363 614.

For issues relating to your Merchant agreement with Diners Club, contact Diners on 1300 360 060.

For issues relating to your PayPal agreement visit www.paypal.com.au and click on the Help Centre or Contact Us links.

For issues relating to your PayWay facility setup, contact your Implementation Manager. Any actions listed on the "Go Live" page are completed by your implementation manager.

For issues relating to PayWay Net development, email PayWay Technical Support (payway@qvalent.com) and provide:

- your client number or biller code,
- a description of the issue,
- date/time when the issued occurred,
- a receipt number and dollar value of a sample transaction,
- a screenshot if relevant,
- the web technology you are using.

9 Appendix A – PayWay Request Parameters

Name	Type	Default	Description
biller_code	Number		**Mandatory.** Your six-digit PayWay Biller Code. This identifies that the payment is for your PayWay facility. To find the value for this, sign-in to PayWay. Your biller code is a six digit number displayed in the top-right corner.
merchant_id	Number		Your Merchant Id - identifies which of your registered merchant facilities the payment is to be processed under: • Specify "TEST" for making test payments. • For an Amex/Diners transactions, you must still pass your Westpac Visa/MasterCard merchant id
paypal_email	Email		Your PayPal Email address – identifies which of your linked PayPal accounts the payment is to be processed under: • Specify "test@example.com" for making test payments • In order to conduct live payments you must link a PayPal account to your PayWay facility as described in section 2.4.
information_fields	Text		Comma-separated[5] list of input field names which contain customer specific information.
required_fields	Text		Comma-separated[2] list of input field names that must be entered by your customer before a payment can be made.
hidden_fields	Text		Comma-separated[2] list of input field names that contain customer information that you require to identify the customer or payment, but do not wish to display to the customer.
suppress_field_names	Text		Comma-separated[2] list of input information field names whose labels you do not wish to display.

[5] Do not include spaces after the commas.

Name	Type	Default	Description
receipt_address	Email Address		The customer's email address to which a payment notification email will be sent.
surcharge_rates	Text	*Use surcharges as configured via PayWay sign-in.*	In general, surcharges should be configured as follows:- • Sign-in to PayWay • Click on "Administration" in the menu • Click on "Surcharges" in the menu The field can be used if you wish to define the card scheme surcharge rates to be applied to payments on a payment by payment basis. This field may only be used as part of a Token Request. See section 3.2. The format of this field is as follows:- VI/MC=1.0,AX=1.5,DC=2.0 This would set the surcharge rate to 1% for Visa/MasterCard, 1.5% for American Express and 2.0% for Diners Club.
Payment Reference Parameters These are generally used for Bill Payments, Donations and Membership Renewals where a payment is collected against a reference number. Use `payment_reference` for a shopping cart to track the cart number.			
payment_reference	Text		Your reference number used to allocate the payment. e.g. customer number, member number, invoice number, policy number, shopping cart id etc. This appears as "Customer Reference Number" on PayWay transaction reports and is included in server to server payment notifications and browser redirects back to your site.
payment_reference_text	Text	Payment Reference	The label associated with your payment reference. Displayed on the left of payment reference field.
payment_reference_text_help	Text		The help text associated with your payment reference. Displayed on the right of the payment reference field.

Name	Type	Default	Description
payment_reference_minimum_length	Number	1	The minimum length allowed for the payment reference.
payment_reference_maximum_length	Number	20	The maximum length allowed for the payment reference.
payment_reference_check_digit_algorithm	Number		Specifies the check digit algorithm to be applied to the payment reference. Use "MOD10V01" for the Luhn algorithm (also known as Mod 10 Version 1), or "MOD10V05" for the Mod 10 Version 5 algorithm.
payment_reference_change	Boolean	false	If you are passing a payment_reference and want to allow your customer to edit the value, set this field to "true". NB. A technically adept customer could modify the payment reference if you are posting parameters via form input fields. See section 3.1.1.
payment_reference_required	Boolean	true	Flag to indicate if you require a payment reference. Set to "false" if you do not use payment references.
payment_amount	Number		Amount of the payment. If you are using surcharges, this is the amount before any surcharge is added by PayWay. A value specified for the payment_amount parameter will override PayWay's calculated payment total, though the products will still be displayed as provided. NB. A technically adept customer could modify the payment amount if you are posting parameters via form input fields. See section 3.1.1.
payment_amount_text	Text	Payment Amount	The text associated with your payment amount. Displayed on the left of payment amount field.
payment_amount_text_help	Text		The help text associated with your payment amount. Displayed on the right of the payment amount field.
payment_amount_minimum	Number	0.01	The minimum payment amount you accept.
payment_amount_maximum	Number	10000	The maximum payment amount you accept.

Name	Type	Default	Description
payment_amount_change	Boolean	false	If you are passing a payment_amount and you want to allow your customer to edit the value, set this field to "true". NB. A technically adept customer could still modify the payment amount if you are posting parameters via form input fields. See section 3.1.1.
Token Lookup Parameters This field is used to instruct PayWay to make a payment against a token requested earlier. See section 3.2.			
token	Text		This is the token returned from a token request. See 3.2.2. PayWay will look up parameters based on the values passed for this token request. The biller_code must also be provided.
Credit Card Parameters These are used to provide PayWay with the credit card details. These fields can only be provided via a HTML form post. See section 3.4. If you pass these parameters, then you must also pass the `token` parameter.			
action	Text		Specify "MakePayment" to indicate that the payment should be collected immediately. The Credit Card details must be provided in the same request.
no_credit_card	Number		The credit card number
nm_card_holder	Text		The credit card holder name
dt_expiry_month	Two digit number		The expiry month
dt_expiry_year	Four digit number		The expiry year
no_cvn	Three or four digit number		The Card Verification Number (CVN). This is also known as Card Verification Value (CVV).

Name	Type	Default	Description
Product Field Parameters These fields can be used to display a list of products.			
gst_rate	Number		Set this value if you would like PayWay to display GST against your products. Use value "10" for a GST rate of 10%.
gst_added	Boolean	false	Flag to indicate whether you have included GST in the product's unit price. • Use "true" if you have already added the GST • Use "false" if you have NOT already added the GST and want PayWay to add it.
gst_exempt_fields	Text		Comma-separated[1] list of product field names that should not have GST added.
print_zero_qty	Boolean	true	Flag to indicate if product fields with a zero quantity should be displayed. If you do not wish to display products with zero quantity, set this value to "false".
Any other name not listed in this table, or as one of the information_fields or hidden_fields.	See description		Any other field that is not listed will be interpreted as a product field. See section 3.3.3. The name of the field should be the product name which is to be displayed. The value of the field is the quantity (number of products), followed by the unit price.

Name	Type	Default	Description
Browser Return and Redirect Parameters In general, these settings should be configured through the PayWay Setup Net Wizard. See section 4.3 and 5.2. These fields are only valid when requesting a token. See section 3.2.			
return_link_url	HTTP URL		The URL that will be used when the customer clicks the link back to your website. If you wish to receive information and hidden fields, specify the name of the fields in this URL: www.example.com?PromotionCode&Name&Address
return_link_text	Text	Return to <Business>	The text that will be displayed on the payment receipt page to allow the customer to return to your website.
return_link_redirect	Boolean	false	Flag to indicate whether an automatic redirection from the payment receipt page to your website should be performed.
return_link_payment_status	Text	all	Indicates for what payment statuses (all, approved, declined) the return link will be displayed or used for redirection.
return_link_url_pre_payment	HTTP URL		The website URL will be used to allow the customer to return to your website prior to making a payment.
return_link_text_pre_payment	Text		The text that will be displayed on the button to allow the customer to return to your website prior to making a payment.
Server-to-Server Payment Notification Parameters In general, these should be configured through the PayWay Setup Net Wizard. See section See section 4.3. These fields are only valid as part of a token request. See section 3.2.			
payment_alert	Email Address		Your email address to which a payment notification email will be sent.

Name	Type	Default	Description
reply_link_url	HTTPS URL		PayWay will send the server to server payment notification to this URL. See 4.3.
reply_link_post_type	Text		Specifies the format to be sent in the server-to-server message. Valid values are: xml extended Leave this field blank for the default format, and add parameters to reply_link_url to request parameters. See Appendix B – Payment Notification Parameters.
reply_link_email	Email Address		The fallback email address that an email notification will be sent to when server-to-server messages fail after three attempts.
reply_link_payment_status	Text	all	Indicates for what payment statuses (all, approved, declined) the server-to-server messages will be sent.

10 Appendix B – Payment Notification Parameters

This appendix lists the PayWay built-in parameters that are returned as part of a server to server Payment Notification.

The parameters you will receive depend on the configuration (see 4.3). Additional parameters may be added from time to time. Your server should ignore any parameters which it does not use.

10.1 Extended and XML Post Types

Parameter Name	Post Type		Description
	Server to Server Extended	Server to Server XML	
am_payment	✓	✓	Amount of attempted transaction in dollars and cents. This includes any surcharge which has been paid.
am_surcharge	✓	✓	Amount of Surcharge in dollars and cents.
cd_response	✓	✓	The two digit response code. See Appendix E – Common Response Codes
cd_summary	✓	✓	Use this to determine if the transaction was approved. See Appendix E – Common Response Codes
dt_payment	✓	✓	The settlement date of the payment. Transactions after 6pm Sydney time are settled on the following day. See PayWay User Guide for information about bank reconciliation. Format: YYYYMMDD

Parameter Name	Post Type		Description
	Server to Server Extended	Server to Server XML	
fl_success	✓	✓	0 = declined payment 1= approved payment
nm_card_holder	✓	✓	The name of the credit card holder.
nm_card_scheme	✓	✓	One of the following card schemes: VISA MASTERCARD AMEX DINERS UNKNOWN JCB
no_receipt	✓	✓	Receipt Number for the transaction generated by PayWay.
password	✓	✓	Your server must check that this password is correct to ensure the message came from PayWay. The password is displayed in the Setup Net wizard.
payment_reference	✓	✓	The payment reference entered by the customer or passed to PayWay using the payment_reference parameter.
ti_payment	✓	✓	The date/time of the transaction on the PayWay server in Sydney time. Format: 18 Sep 2009 15:04:43
TruncatedCardNumber	✓	✓	The masked card number. e.g. 456471…004

Parameter Name	Post Type		Description
	Server to Server Extended	Server to Server XML	
tx_response	✓	✓	The description of the response code. See Appendix E – Common Response Codes
username	✓	✓	This is your PayWay client number (e.g. Q10000). This can be used if you have multiple PayWay facilities to distinguish which facility the payment is for.
PayPalEmailAddress	✓	✓	If a PayPal transaction was conducted, this parameter will provide the buyer's PayPal email address.
Parameter *Name* *Value*	✓	✓	Information and hidden fields you send to PayWay are returned to in the server-to-server post-back.

10.1.1 XML Post Type

If set to xml, the parameters will be built into an xml document and passed to your server as the body of a request of content-type application/xml.

The document will be of the form:

```
<PaymentResponse>
     <cd_source>net</cd_source>
     <no_receipt>1002431909</no_receipt>
     <payment_reference>Invoice No. 5</payment_reference>
     <cd_community>PAYWAY</cd_community>
     <cd_supplier_business>QXXXXX</cd_supplier_business>
     <am_payment>11.00</am_payment>
     <am_surcharge>1.00</am_surcharge>
     <nm_card_scheme>VISA</nm_card_scheme>
     <dt_payment>20120627</dt_payment>
     <tx_response>Approved or completed successfully</tx_response>
     <cd_summary>0</cd_summary>
     <ti_payment>27 Jun 2012 16:02:47</ti_payment>
     <cd_response>00</cd_response>
     <TruncatedCardNumber>456471...004</TruncatedCardNumber>
     <nm_card_holder>Tommy Testman</nm_card_holder>
     <fl_success>1</fl_success>
     <parameter>
          <name>test field</name>
          <value>test value</value>
     </parameter>
     <username>QXXXXX</username>
     <password>XXXXXXXXX</password>
</PaymentResponse>
```

10.2 Default Post Type

Parameters for the default post type are the same as the parameters listed in Appendix C – Browser Redirect Parameters. The parameters are sent as POST parameters. In order to request parameters, you must include them in your Notification URL as follows:

www.example.com?payment_reference&payment_status

Hidden and information fields are always included.

11 Appendix C – Browser Redirect Parameters

This appendix lists the parameters that are returned as part of the browser redirect. Parameters are passed as an encrypted string. See section 5.3.

Parameter Name	Description
bank_reference	Receipt number generated by PayWay
card_type	One of the following card schemes: VISA MASTERCARD AMEX DINERS UNKNOWN JCB
payment_amount	Total amount of attempted transaction in dollars and cents. This includes any surcharge or GST which has been included paid.
payment_date	The settlement date of the payment. Transactions after 6pm Sydney time are settled on the following day. See PayWay User Guide for information about bank reconciliation. Format: YYYYMMDD
payment_number	Receipt number generated by PayWay
payment_reference	The payment reference input by the customer or passed to PayWay using the payment_reference parameter.

Parameter Name	Description
payment_status	declined approved
payment_time	The date/time of the transaction on the PayWay server in Sydney time. Format: 18 Sep 2009 15:04:43
remote_ip	The IP address of the customer.
response_code	The two digit response code. See Appendix E – Common Response Codes
response_text	The description of the response code. See Appendix E – Common Response Codes
summary_code	Use this to determine if the transaction was successful or not. See Appendix E – Common Response Codes
information fields	Information fields you sent to PayWay (see section 3.3.1) are included if you specify them in your return URL. For example, if you have information fields named "Name" and "Address1" and "Address2", you can request these by setting the return URL to: www.example.com?Name&Address1&Address2
hidden fields	Hidden fields you sent to PayWay (see section 3.3.2) are included if you specify them in your return URL. For example, if you have a hidden fields named "PromotionCode" and "PartnerCode", you can request these by setting the return URL to: www.example.com?PromotionCode&PartnerCode

12 Appendix E – Common Response Codes

These response codes have been included for your reference and are derived from the message format defined in Australian Standard 2805.2 (1997).

The table below lists the most commonly received response codes. As a general rule you should use the summary response code, which is supplied to determine whether a transaction is approved or declined. The actual reason for a decline is often not important, and the situation can usually be resolved by verifying the card details with the customer, or asking them for a different card number.

Summary Code	Description
0	Transaction Approved
1	Transaction Declined
2	Transaction Erred
3	Transaction Rejected

Valid response codes are of a two digit alphanumeric format. If an unknown response code is returned please contact Westpac with the appropriate transaction details.

Both the response code and description of a response will be supplied.

Response Code	Description	Summary Code
00	Approved or completed successfully	0
01	Refer to card issuer	1
03	Invalid merchant	1
04	Pick-up card	1
05	Do not honour	1
08	Honour with identification	0
12	Invalid transaction	1
13	Invalid amount	1
14	Invalid card number (no such number)	1
30	Format error	1
36	Restricted card	1
41	Lost card	1
42	No universal account	1
43	Stolen card, pick up	1
51	Not sufficient funds	1
54	Expired card	1

Response Code	Description	Summary Code
61	Exceeds withdrawal amount limits	1
62	Restricted card	1
65	Exceeds withdrawal frequency limit	1
91	Issuer or switch is inoperative	1
92	Financial institution or intermediate network facility cannot be found for routing	1
94	Duplicate transmission	1
Q2	Transaction Pending	2
Q3	Payment Gateway Connection Error	3
Q4	Payment Gateway Unavailable	1
QD	Invalid Payment Amount - Payment amount less than minimum/exceeds maximum allowed limit	1
QE	Internal Error	3
QI	Transaction incomplete - contact Westpac to confirm reconciliation	2
QQ	Invalid Credit Card \ Invalid Credit Card Verification Number	1
QX	Network Error has occurred	2
QY	Card Type Not Accepted	1
QZ	Zero value transaction	0

Common Response Code Descriptions

01 - Refer to Issuer
This indicates an error or problem on the issuer's side. The problem may be related to the card holder's account. In general the reason for this response code may be any of the following:-

- Suspected Fraud
- Insufficient Funds
- Stolen Card
- Expired Card
- Invalid CVN
- Any other rule imposed by the card issuer that causes a decline (e.g. daily limit exceeded, duplicate transaction suspected, etc).

03 - Invalid Merchant
This can be returned when there is a problem with the merchant configuration. This can also be returned for AMEX transactions when there is a problem with the setup at American Express. This code can be returned from an issuing bank if they don't like the acquiring bank. An example of this would be someone trying to pay their speeding fine with an overseas credit card. The overseas issuing bank would return a 03, indicating that they wouldn't allow the transaction over the internet for an Australian bank.

04 - Pickup Card
Error code 04 normally means that the card has been reported as lost or stolen. In all cases where this response code is being returned and the customer does not know why they need to follow this up with the issuing bank.

05 - Do Not Honour
This code is usually returned from Westpac for Westpac issued cards for similar reasons that other issuers return 01. It can indicate any of the following:-

- Suspected Fraud
- Insufficient Funds
- Stolen Card
- Expired Card
- Invalid CVN
- Any other rule imposed by the card issuer that causes a decline (e.g. daily limit exceeded, duplicate transaction suspected, etc).

12 - Invalid Transaction
This code is often returned from the issuer when they do not accept the transaction. This can possibly be when a transaction for the same amount and merchant is attempted multiple times quickly for the same card. The best approach is for the card holder to contact their issuing bank.

14 - Invalid card number (no such number)
This code indicates that the card number either did not pass the check digit algorithm, or is not an account that exists at the issuing bank. Westpac returns this code if the card number passes the check digit algorithm, but is not an existing card. Westpac also returns this code if an AMEX card is used, but the merchant is not setup for AMEX cards at the Westpac end.

22 - Suspected Malfunction
Westpac returns this code if the card number does not pass the check digit algorithm. This is considered a malfunction, since Westpac expect the terminal to check the card number before transmission.

42 - No Universal Account
This error is returned from some issuers when the credit account does not exist at the issuing bank. This situation is similar to the 14 response code - the card number passes the check digit algorithm, but there is no credit account associated with the card number.

This error is also returned if you are using the TEST merchant without using one of the test card numbers. See Chapter 6.

51 – Not sufficient funds
61 – Exceeds withdrawal amount limits
This error is returned when the card holder does not have enough credit to pay the specified amount. Ask the card holder if they have another card to use for the payment.

54 – Expired Card
This error is returned when the wrong expiry date has been entered for the credit card. Check that the expiry date is correct and attempt the transaction again. If the transaction still does not work, check with the card holder to see if they have a new card with a new expiry date.

91 - Issuer or switch is inoperative
This code is used to indicate that the next party in a credit card transaction timed out and the transaction has been reversed. This may happen between PayWay and Westpac, or further down the chain.

92 - Financial institution or intermediate network facility cannot be found for routing
The card number is incorrect. The first 6 digits of the credit card number indicate which bank issued the card. These are used for routing credit card requests through the credit card network to the issuing bank. This error indicates that there is no bank that corresponds to the first 6 digits of the card number.

QI - Transaction incomplete
This response code indicates that a request message was sent to the PayWay server but no response was received within the timeout period.

QQ - Invalid Card
This error code indicates that the credit card details (card number, expiry date or CVN) are invalid. This could be because the card number does not meet check digit validation, an invalid expiry date was entered or an invalid CVN was entered.

QY - Card Type not accepted
The Merchant is not enabled for the particular Card Scheme (normally returned for American Express and Diners Club cards). To register for American Express or Diners Club, click the **Register to accept Amex or Diners through PayWay** link on the "Merchants" page. Alternatively, you may have entered a bad card number with too many or too few digits.

Other Response Codes
If you receive a numeric response code other than those listed in this section, you should check that the card details are correct. If they are, ask the card holder for an alternative credit card. If this still does not resolve the problem, the card holder should contact their issuing bank.

If you receive a response code starting with 'Q' that you do not understand, you should contact Technical Support as per Chapter 8.