PayPal™

Website Payments Pro Developer's Guide

For Professional Use Only
Currently only available in English.

A usage Professional Uniquement
Disponible en Anglais uniquement pour l'instant.

Last Updated: February 2009

Website Payments Pro Developer's Guide

Notice of Non-Liability

PayPal Inc. is providing the information in this document to you "AS-IS" with all faults. PayPal Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. PayPal Inc. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. PayPal Inc. reserves the right to make changes to any information herein without further notice.

PayPal Inc. does not guarantee that the features described in this document will be announced or made available to anyone in the future.

Contents

Preface

Website Payments Pro Developer's Guide describes Website Payments Pro and how to integrate it into your website using the Payflow SDK. The product offers two website payment solutions: PayPal Direct Payment and PayPal Express Checkout.

Intended Audience

This guide is written for merchants who have signed up through PayPal Manager to use PayPal as their processor and Website Payments Pro as their solution for handling payment transactions on their website.

This guide assumes that its readers:

- Are experienced web or application developers
- Have a background in payments services

Scope

This guide describes the Payflow SDK programming interfaces needed to integrate Website Payments Pro into your website, along with guidelines and best practices for presenting these payment offerings.

Organisation of This Document

The guide is organised into the following chapters and appendices:

- Chapter 1, "Website Payments Pro Overview," provides a brief overview of the product.
- Chapter 2, "Installing and Configuring," describes where to get the Payflow SDK and how to install it.
- Chapter 3, "Creating a Simple Transaction Request," identifies a common set of transaction data required in all transactions and provides syntax guidelines on how to format it so that it can be understood by the Payflow server.
- Chapter 4, "Performing Direct Payment Credit Card Transactions," describes how you can implement Direct Payment credit card processing. The chapter provides a basic set of data parameters typically used in transaction requests.
- Chapter 5, "Testing Credit Card Transactions," describes testing PayPal transactions through PayPal's simulated payment network.

- Chapter 6, "PayPal Express Checkout Transaction Processing," explains how PayPal Express Checkout works and describes additional (optional) parameters you can send in PayPal Express Checkout transaction requests.
- Chapter 7, "Responses to Transaction Requests," describes parameters returned in transaction responses.
- Chapter 8, "PayPal Button Placement and Page Designs," provides guidelines on how to integrate PayPal graphics into your website.
- Chapter 9, "Implementing 3-D Secure Transactions," explains how to integrate 3-D Secure transactions for credit and debit cards.
- Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results", describes how you can use the VERBOSITY parameter to control the kind and level of information you want returned in a transaction response.
- Appendix B, "ISO Country Codes", lists the country codes you provide as transaction data in certain transactions.

Where to Go for More Information

PayPal Manager Online Help describes the use of PayPal Manager — the web-based administration tool that you can use to process transactions manually, issue credits and generate reports. PayPal Manager provides links to the PayPal website, where you can perform additional tasks such as resolving disputes. See the Manager Online Help for details.

Getting Started with PayPal Manager contains instructions on how to use PayPal Manager, including testing credit card numbers and Direct Payments.

For answers to specific questions about Payflow products, search PayPal's Knowledge Base at the following URL: http://knowledge.paypal.com/.

How to Contact Customer Service

For problems with transaction processing or your connection to the server, contact Customer Service at business-support@paypal.co.uk.

Revision History

Revision history for *Website Payments Pro Developer's Guide.*

TABLE P.1 Revision History

Date	Description
August 2009	Added chapter for 3D-Secure transactions.
February 2009	Made updates for UK currency, credit card support, and terminology. Corrected typos and other minor edits.
December 2008	Replaced Button Placement chapter with a new version. Updated Download and Install chapter.
March 2006	Integrated Express Checkout feature.
May 2006	Updated document title, product names. Reformatted in PayPal templates. Added AMEX recommendations for enhanced data for detecting fraud. Added support for multiple currencies. Edited for technical accuracy.
August 2006	Updated URLs.
September 2006	Corrected parameter name. Wrong name: COMPLETETYPE. Correct name: CAPTURECOMPLETE.
December 2006	Revised Chapter 7, "PayPal Button Placement and Page Designs." Corrected URLs to test and live servers Added error return code 51 Added SHIPTOSTREET and SHIPTOSTREET2 to Get Express Checkout Details response parameters
February 2007	Added return codes: 51, 110, 119, 120, 121, 132, 133, 200, 201, 402, 403, 404, 600, and 601. Updated description of PAYERID. Added PayPal Processor testing values.
March 2007	Corrected length of PayerID. Added note that Express Checkout does not support Payflow Recurring Billing. Corrected the bill-to country parameter name in Get Express Checkout Details response. Replaced SHIPTOCOUNTRYCODE with COUNTRY parameter. Other corrections for technical accuracy.

1 Website Payments Pro Overview

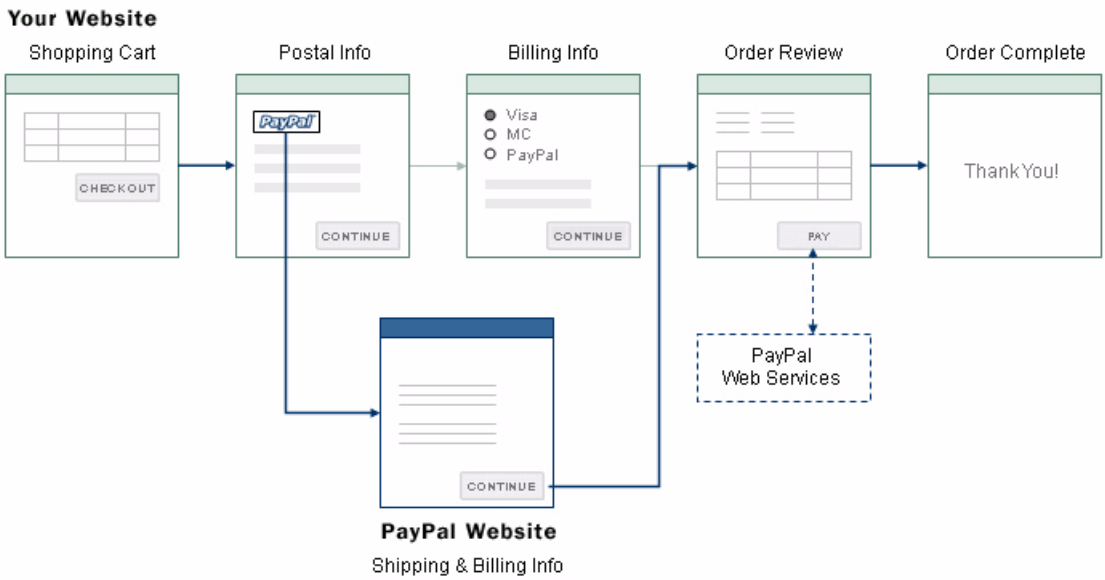
Website Payments Pro provides the payment processing capabilities of a merchant account and gateway – plus much more. It is an all-in-one payment solution that includes:

- **Direct Payment.** Direct Payment enables you to accept credit card payments directly on your website. PayPal remains invisible, so you control the customer experience.
- **PayPal Express Checkout.** PayPal Express Checkout allows PayPal account holders to check out quickly with saved information, and helps you gain incremental sales from PayPal's growing base of users.

How Website Payments Pro Works

Figure 1.1, "High-Level View," is an example of a standard checkout process. Website Payments Pro has the flexibility to work with your unique checkout process, whether it is one page or has multiple steps.

FIGURE 1.1 High-Level View



After selecting products to purchase, the customer chooses whether they want to pay using PayPal or pay using credit cards directly on your website.

If the customer pays using credit cards on your website, PayPal processes them in the background.

If the customer chooses to use PayPal, the customer is transferred to PayPal to log in and select a postal address and payment method, and is returned to your website to complete their purchase.

Once the buyer completes their order, you receive your payment.

Supported Transactions

Website Payments Pro supports the following transaction types:

Sale
Authorisation
Void
Delayed Capture
Credit

Chapter 4, "Performing Direct Payment Credit Card Transactions," describes the transaction types in detail and identifies the minimum parameters that you must send for each.

Supported Currencies

Website Payments Pro supports the following currencies:

- AUD (Australian dollar)
- CAD (Canadian dollar)
- CHF (Swiss franc)
- CZK (Czeck koruna)
- DKK (Danish krona)
- EUR (Euro)
- GBP (UK pound)
- HKD (Hong Kong dollar)
- HUF (Hungarian forint)
- JPY (Japanese Yen)
- NOK (Norwegian krona)
- NZD (New Zealand dollar)
- PLN (Polish Zloty)

- SEK (Swedish krona)
- SGD (Singapore dollar)
- USD (US dollar)

Unlike other processors that require you to set up a separate account for each currency, PayPal allows you to run transactions using any of the these currencies with a single account.

Direct Payment Overview

Direct Payment offers direct credit card payment processing capability through PayPal. For credit card transactions, customers can stay on your website as PayPal processes the payment in the background.

For each payment, Direct Payment takes the billing address, transaction amount, credit card information, and item information as inputs. Within seconds, PayPal returns a confirmation that the transaction has been processed. If you have signed up for Fraud Protection Services, Direct Payment lets you flag potentially fraudulent transactions, and provides you with industry-standard Address Verification Service and card security code (CVV2) responses for each transaction.

By integrating Direct Payment with Express Checkout as part of the Website Payments Pro solution, you can accept all major payment types, including PayPal, while working with a single provider that processes and manages all of your online payments for you.

IMPORTANT: *Direct Payment is not a standalone product. You are required to use Direct Payment and PayPal Express Checkout together as part of the Website Payments Pro solution. See "Business Rules" on page 14.*

Direct Payment is not covered by the PayPal Seller Protection Policy (SPP).

PayPal Express Checkout Overview

With PayPal Express Checkout, a customer selects his products and completes his orders on your website. Payment method along with postage and billing details are managed on PayPal's website. PayPal automatically gives you the postal address and other customer information to fulfil the order.

The more convenient it is for your customers to buy from you, the more they will buy. PayPal Express Checkout gives customers the option of paying quickly through PayPal and gives your business more benefits.

PayPal Express Checkout provides these advantages to your customers:

- Gives buyers more convenience, encouraging more sales. Customers simply log in to use information they've already entered with PayPal, so they save time by completing transactions in fewer steps.

- Helps buyers feel safer, so they buy more. Buyers prefer to pay with PayPal because their customer information is kept safe. When they're confident about the security of their information, they purchase more.

As the seller, you gain these advantages:

- Real-time notification of successful payments.
- Automation of your internal business processes.
- More advertising opportunities as buyers finish their orders on your website.
- Notification that the buyer's address is confirmed.
- Eligibility for coverage under PayPal's Seller Protection Policy.

Additional Services

If you have signed up for the Recurring Billing Service, see the *Payflow Pro Recurring Billing Service User's Guide*. It is downloadable from the PayPal Manager Documentation page. There is no charge for this service.

Business Rules

Website Payments Pro must be integrated on your website in the following ways. You must:

- Present the PayPal Express Checkout button and associated messaging before requesting postal address, billing address, and financial information. PayPal account holders should not be required to enter any of this information on your website, because the information is available from their PayPal accounts.
- Display PayPal as an option together with other payment methods wherever other payment methods are offered.
- Present the PayPal mark graphic wherever other payment marks are displayed.

For details on displaying Express Checkout graphics on your website, see Chapter 8, "PayPal Button Placement and Page Designs."

Testing

For details on testing, see the documentation at the following URL:

https://www.paypal.com/en_US/pdf/PayflowPro_Simulator_Guide.pdf

About the PayPal SDK

The SDK is available from the PayPal Manager Downloads page.

2 Installing and Configuring

The Payflow Software Development Kit (SDK) is a set of APIs that allow you to integrate Website Payments Pro (Payflow Pro) with your application or website.

IMPORTANT: *Full API documentation is included with each SDK.*

Supported Platforms

Payflow Pro is available on all major web server platforms in a variety of formats to support your integration requirements. Payflow Pro is available as a .NET or Java library, or you can build your own API by posting directly to the Payflow servers via HTTPS.

Preparing the Payflow Client Application

Follow these steps to download and install:

Step 1 Download the Payflow SDK

From the SDKs and Downloads page linked to the Library tab on PayPal Developer Central, download the Payflow SDK appropriate for your platform.

These links can be found in the PayPal Developer Central at:
https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=developer/howto_gateway_payflowpro

Step 2 Extract the files to a local directory

Step 3 Configure your firewall

If you have a stateful firewall, enable outbound traffic for SSL (port 443). The firewall keeps state on the connection, and automatically permits the inbound response from PayPal.

If you do not have a stateful firewall, enable inbound and outbound traffic for SSL (port 443). Outbound traffic permits the initial request by Payflow Pro, while inbound permits the response from PayPal.

Step 4 Set the certificate path

To enable the client to authenticate the Payflow server, you must set the path to include the **certs** directory (included with the SDK that you downloaded).

For specific information on setting the certificate path, see the readme.txt file and example applications in the SDK.

Step 5 Read the readme.txt file

The Readme.txt file includes integration information and samples that illustrate how to use the Payflow client application in your development environment.

3 Creating a Simple Transaction Request

This chapter describes how to create a simple Sale transaction request.

The chapter focuses on the common set of parameters required in all transactions, and how to set up these parameters using name-value pair strings. Additional parameters may be required, depending on the transaction type. You can also provide many optional parameters, depending on the results you want returned. For example, you can set the VERBOSITY parameter to return PayPal processor-specific details rather than normalised information.

In This Chapter

Transaction Request

Request Contents

A transaction request includes the following:

- Connection parameters.
- Parameters required by all transactions. This list includes "user information" parameters.
- Additional parameters required by the type of transaction.

Data Modes for Sending

You can send parameter data in the transaction request to the Payflow server in either of two modes:

- Name-value pair
- XMLPay

The examples in this guide are presented in name-value pair format. Name-value pair syntax guidelines are described in "PARMLIST Syntax Guidelines" on page 20.

XMLPay is an XML syntax for payment requests and associated responses in a payment-processing network. Instead of using name-value pairs, you can send to the Payflow server XML documents based on the XMLPay 2.0 schema. For details on XMLPay, see the *Website Payments Pro Payflow Edition—XMLPay Developer's Guide*. It is available from the Documentation page in PayPal Manager.

Connection Parameters

Table 3.1 describes the connection parameters. Pass them in the format and syntax required by the Payflow SDK and programming language that you are using. See your integration documentation for details.

TABLE 3.1 Connection parameters

Argument	Required	Description
HOSTADDRESS	Yes	Payflow host name. For live transactions, use **payflowpro.paypal.com** For testing purposes use **pilot-payflowpro.paypal.com**
HOSTPORT	Yes	Use port 443.
PARMLIST	Yes	The PARMLIST is the list of parameters that specify the payment information for the transaction. The quotation marks " " at the beginning and end are required. The following is an example: `"TRXTYPE=S&TENDER=C&PARTNER=PayPalUK&VENDOR=SuperMerchant&USER=SuperMerchant&PWD=SuperUserPassword&AMT=123.00"` The content of the PARMLIST varies by the type of transaction being processed. For example, a Void transaction requires a different set of parameters than a Sale.
TIMEOUT	Yes	Time-out period for the transaction. The minimum recommended time-out value is 30 seconds. The client begins tracking from the time that it sends the transaction request to the server.
PROXYADDRESS	No	Proxy server address. Use the PROXY parameters for servers behind a firewall. Your network administrator can provide the values.
PROXYPORT	No	Proxy server port.
PROXYLOGON	No	Proxy server logon ID.
PROXYPASSWORD	No	Proxy server logon password.

PARMLIST Syntax Guidelines

Follow these guidelines when creating the PARMLIST:

- Spaces are allowed in values.
- Enclose the PARMLIST in quotation marks ("").
- Do not place quotation marks ("") within the body of the PARMLIST.
- Separate all name-value pairs in the PARMLIST using an ampersand (&).
- Payflow SDKSet the VERBOSITY transaction parameter to MEDIUM (default is LOW) if you want the response to return more detailed information. For details, see Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results."

Using Special Characters in Values

Because the ampersand (&) and equal sign (=) characters have special meanings in the PARMLIST, name-value pairs like the following examples are not valid:

```
NAME=Ruff & Johnson
COMMENT1=Level=5
```

To use special characters in the value of a name-value pair, use a *length tag*. The length tag specifies the exact number of characters and spaces that appear in the value. The following name-value pairs are valid:

```
NAME[14]=Ruff & Johnson
COMMENT1[7]=Level=5
```

NOTE: Quotation marks (“ ”) are not allowed even if you use a length tag.

Values Required by All Transaction Types

All Payflow SDK transactions require the parameters described in Table 3.2.

TABLE 3.2 Required transaction parameters

Parameter	Description	Required	Type	Max. Length
USER	If you set up one or more additional users on the account, this value is the ID of the user authorised to process transactions. If, however, you have not set up additional users on the account, USER has the same value as VENDOR. The examples in this document use USER=SuperMerchant. Limitations: This value is case-sensitive.	Yes	Alphanumeric	64
VENDOR	Your merchant login ID that you created when you registered for the Website Payments Pro account. The examples in this document use VENDOR=SuperMerchant. Limitations: This value is case-sensitive.	Yes	Alphanumeric	64
PARTNER	The ID provided to you by the authorised PayPal Reseller who registered you for the Payflow SDK. If you purchased your account directly from PayPal, use PayPalUK. The examples in this document use PARTNER=PayPalUK Limitations: This value is case-sensitive.	Yes	Alphanumeric	12

TABLE 3.2 Required transaction parameters *(Continued)*

Parameter	Description	Required	Type	Max. Length
PWD	The 6 to 32-character password that you defined while registering for the account. The examples in this document use PWD=SuperUserPassword. This value is case-sensitive.	Yes	Alphanumeric	32
TENDER	The tender type (method of payment). Values are: • C = Credit card for Direct Payment transactions • P = PayPal for PayPal Express Checkout transactions	Yes	Alpha	1
TRXTYPE	A single character indicating the type of transaction to perform. Website Payments Pro supports the following values: S = Sale transaction A = Authorisation C = Credit D = Delayed Capture V = Void	Yes	Alpha	1

Sale Transaction Example

In addition to the connection parameters and the required parameters in Table 3.2, each transaction type (TRXTYPE) has additional parameter requirements and can use a number of optional ones as well.

For example, to perform a Direct Payment credit card Sale transaction, you are required to pass the following parameters:

- ACCT - The payer's credit card number
- AMT - The amount of the sale
- EXPDATE - The credit card expiry date

Typical Sale Transaction PARMLIST

The following is a typical PARMLIST string passed in a Sale transaction.

```
"TRXTYPE=S&TENDER=C&USER=SuperMerchant&PWD=SuperUserPassword&PARTNER=PayPal
UK&ACCT=5105105105105100&EXPDATE=1209&AMT=99.06&COMMENT1=Reservation&FIRSTN
AME=John&LASTNAME=Jones&STREET=123 Main St.&CITY=San
Jose&STATE=CA&ZIP=123451234&COUNTRY=US&CVV2=123&CLIENTIP=0.0.0.0"
```

Note that, besides the required Sale transaction parameters, this string includes other typical Website Payments Pro Payflow Edition parameters. These parameters are described in Chapter 4, “Performing Direct Payment Credit Card Transactions”. and in Chapter 6, “PayPal Express Checkout Transaction Processing”.

How to Format a Transaction

For details on how to format a transaction based on the above information, refer to the examples and the supporting documentation provided with your SDK.

4 Performing Direct Payment Credit Card Transactions

This chapter provides guidelines on how to implement PayPal Direct Payment transactions. Direct Payment offers you credit card payment processing capability through PayPal directly from the buyer's credit card.

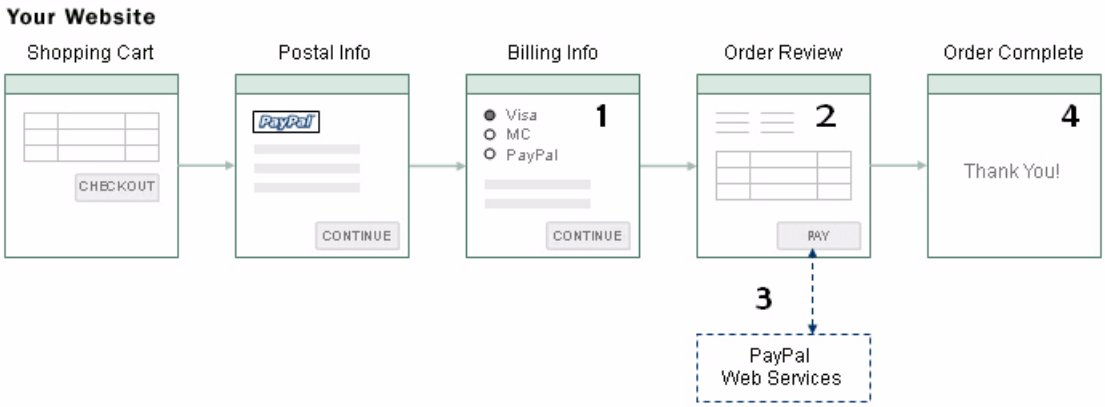
NOTE: Direct Payment is not a standalone feature. You must use Direct Payment together with PayPal Express Checkout. See Chapter 8, "PayPal Button Placement and Page Designs," for guidelines on how to display the PayPal mark logo with credit card logos.

With the exception of a few optional PayPal Express Checkout transaction parameters not covered here, this chapter describes all required Website Payments Pro Payflow Edition request parameters. Differences exist in PayPal Express Checkout transactions, however, and these are explained in Chapter 6, "PayPal Express Checkout Transaction Processing."

In This Chapter

How Direct Payment Works

Figure 3-1 shows the general flow of customer checkout with Direct Payment.



The numbered steps in the figure are described below:

1. On your website, the customer chooses to pay with a credit card and enters the credit card number and other details.
2. The customer reviews the order.
3. When your customer clicks “Pay” to place the order, you perform a transaction to request payment, and the payment transaction is initiated.
4. You transfer your customer to your order confirmation page.

The “Pay” button on your website sends the payment request to the server, including required information you collected from the customer, such as the amount of the transaction, the buyer’s credit card number, expiry date, browser IP address, and an element that specifies whether this transaction is a final sale (complete transaction amount including postage, packing and tax) or an authorisation for a final amount that you must capture later with a Delayed Capture transaction.

About Direct Payment Credit Card Processing

Direct Payment credit card processing occurs in two steps — a real-time authorisation and a capture (settlement) of the funds that were authorised. You perform these two steps either as a single Sale transaction or as two types of transactions, an Authorisation and Delayed Capture, depending on your business model.

For an Authorisation, PayPal sends the transaction information to the cardholder's issuing bank. The issuing bank checks whether the card is valid, evaluates whether sufficient credit exists, checks values such as Address Verification Service and card security codes, and returns a response: Approval, Decline, Referral, or others. For details on Address Verification Service and card security codes, see:

- "Using Address Verification Service" on page 45
- "Card Security Code Validation" on page 46

You receive the response shortly after you submit the transaction to PayPal. If the Authorisation is approved, the bank temporarily reserves credit for the amount of the transaction to prepare to capture (fulfil) the transaction. The hold on funds typically lasts for about a week.

Capturing a transaction (also known as *settling* a transaction) actually transfers the funds to PayPal. At least once a day, the Payflow server gathers all transactions that are flagged to be settled and sends them in a batch file to PayPal. PayPal charges the issuing bank and transfers the funds to your PayPal account. It typically takes a few days before the money is actually available in your PayPal account.

Considerations Regarding Your Website Integration

In the design of your website integration, you should consider whether you want to store information in your local database or use PayPal Manager reports to manage the data. You may want to store postal information in your system, or you may prefer to send the information to PayPal with the transaction and report on it later.

NOTE: PayPal recommends that you do not store credit card numbers. If you must store numbers, encrypt and store them behind properly configured firewalls. You should also consider whether and how to use the merchant-defined fields COMMENT1 and COMMENT2 to help tie PayPal reports to your orders/customers or to report on other information about the transaction.

If you want to integrate with other systems, such as order fulfilment, customer service, and so on, you may want to connect these systems directly to Website Payments Pro for capturing funds, issuing refunds/credits, and so on. Alternatively, you may prefer to perform these steps manually using PayPal Manager. Either way, PayPal recommends that you monitor transaction activity using PayPal Manager.

Parameters Used in Transactions

PayPal accepts the parameters listed in Table 4.1. The table indicates whether the parameters are required or optional.

NOTE: Unless otherwise noted, the parameters in Table 4.1 can be used in Direct Payment and PayPal Express Checkout transactions. See Chapter 6, "PayPal Express Checkout Transaction Processing," for additional (optional) PayPal Express Checkout parameters.

TABLE 4.1 Transaction parameters

Parameter	Description	Required	Type	Max. Length
ACCT	Payer's credit card or account number. It may not contain spaces, non-numeric characters, or dashes. For example, ACCT=5555555555554444	Yes[a]	Numeric	19
ACCTTYPE	Credit card type. The following card types are supported: 0 = Visa 1 = MasterCard 8 = Other 9 = Switch S = Solo **NOTE:** American Express cards are not currently processed in the UK.	No	Alpha	10
AMT	Total of this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. See CURRENCY in this table for details. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	Yes	Decimal	10
BILL-TO Address (Next five table entries)				
STREET	Cardholder's bill-to postal address (number and street name). The STREET value is verified by Address Verification System (described on page 45).	No	Alpha-numeric	100
CITY	Name of bill-to city.	No	String	40

***TABLE 4.1 Transaction parameters** (Continued)*

Parameter	Description	Required	Type	Max. Length
STATE	Name of bill-to county or province.	No	String	40
COUNTRY	Bill-to country code. See Appendix B, "ISO Country Codes."	No	Alpha	2
ZIP	Account holder's five to nine-digit bill-to ZIP code or other country-specific bill-to postcode. Do not use spaces, dashes or non-numeric characters. ZIP is verified by Address Verification System and the International Address Verification System (described on page 45).	No	String	20
BUTTONSOURCE	Identification code for use by third-party applications to identify transactions.	No	Alpha-numeric	32
CARDISSUE	Issue number of Switch or Solo card. **NOTE:** For a Switch or Solo transaction to be approved, either CARDISSUE or CARDSTART must be present.	No	Numeric	2
CARDSTART	Date that Switch or Solo card was issued in **mmyy** format. For example, 0308 represents March 2008. **NOTE:** For a Switch or Solo transaction to be approved, either CARDISSUE or CARDSTART must be present.	No	Numeric	4
CLIENTIP	IP address of payer's browser as recorded in its HTTP request to your website. **NOTE:** PayPal records this IP address as a means to detect possible fraud. Limitations: This value is in dotted quad format: *xxx.xxx.xxx.xxx*	No, but is recom-mended	String	15
COMMENT1	Merchant-defined value for reporting and auditing purposes. See "Using Address Verification Service" on page 45.	No	Alpha-numeric	128
COMMENT2	Merchant-defined value for reporting and auditing purposes.	No	Alpha-numeric	128

***TABLE 4.1 Transaction parameters** (Continued)*

Parameter	Description	Required	Type	Max. Length
CAPTURECOMPLETE	Indicates if this Delayed Capture transaction is the last capture you intend to make. The values are: • Y (default) • N **NOTE:** If CAPTURECOMPLETE is Y, any remaining amount of the original reauthorised transaction is automatically voided.	No	Alpha-numeric	12
CURRENCY	One of the following three-character currency codes: • AUD (Australian dollar) • CAD (Canadian dollar) • CHF (Swiss franc) • CZK (Czeck koruna) • DKK (Danish krona) • EUR (Euro) • GBP (UK pound) • HKD (Hong Kong dollar) • HUF (Hungarian forint) • JPY (Japanese Yen) • NOK (Norwegian krona) • NZD (New Zealand dollar) • PLN (Polish Zloty) • SEK (Swedish krona) • SGD (Singapore dollar) • USD (US dollar)	No	Alpha	3
CUSTOM	A free-form field for your own use.	No	Alpha-numeric	256
CUSTREF	Merchant-defined identifier for reporting and auditing purposes. For example, you can set CUSTREF to INVNUM.	No	Alpha-numeric	12

***TABLE 4.1 Transaction parameters** (Continued)*

Parameter	Description	Required	Type	Max. Length
CVV2	A three of four-digit code that is printed (not imprinted) on the back of a credit card. Used as partial assurance that the card is in the buyer's possession. For details, see "Card Security Code Validation" on page 46. **NOTE:** CVV2 values are normalised to Y, N and X values. The PayPal processor values are returned when you set VERBOSITY parameter to MEDIUM. For details on VERBOSITY, see Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results."	No	Alpha-numeric	4
EMAIL	Email address of payer.	No	Alpha-numeric	127
EXPDATE	Expiry date of the credit card in **mmyy** format. For example, 0308 represents March 2008.	Yes[a]	Numeric	4
FREIGHTAMT	Total postage costs for this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. See the CURRENCY entry in this table for details. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	10
HANDLINGAMT	Total packing costs for this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. See the CURRENCY entry in this table for details. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	10

***TABLE 4.1 Transaction parameters** (Continued)*

Parameter	Description	Required	Type	Max. Length
INVNUM	Your own unique or tracking number.	No	Alpha-numeric	127
ITEMAMT	Sum of cost of all items in this order. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	127
L_DESCn	Line item name. **NOTE:** You can view line item information in the Transaction Details report in your PayPal merchant account.	No	String	127
L_AMTn	Cost of line item. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. See the CURRENCY entry in this table for details. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	See description
L_QTYn	Line item quantity.	No	String	Any positive integer
L_TAXAMTn	Line item tax amount. Limitations: Any valid currency amount; CURRENCY value must be set the same as for AMT.	No	Decimal	See description
MERCHANTSESSIONID	Your customer Direct Payment session identification token. PayPal records this session token as an additional means to detect possible fraud.	No	String	64
NAME Information (Next two table entries)				
FIRSTNAME	Account holder's first name.	No, but recom-mended	Alpha	25

TABLE 4.1 Transaction parameters *(Continued)*

Parameter	Description	Required	Type	Max. Length
LASTNAME	Account holder's last name.	No, but recommended	Alpha	25
NOTIFYURL	Your URL for receiving Instant Payment Notification (IPN) about this transaction. If you do not specify NOTIFYURL in the request, the notification URL from your Merchant Profile is used, if one exists.	No	Alpha-numeric	2048
ORDERDESC	Description of items the customer is purchasing.	No	Alpha-numeric	127
ORIGID	ID of the original Direct Payment transaction that is being referenced. This ID is returned by the PNREF parameter and appears as the Transaction ID in PayPal Manager reports. Limitations: This value is case-sensitive.	Yes[a]	Alpha-numeric	12
RECURRINGTYPE	Type of transaction occurrence. The values are: F = First occurrence S = Subsequent occurrence (default)	No	Alpha	1
SHIP-TO Address Information (Next five table entries)				
SHIPTOSTREET	Post-to postal address.	No[b]	String	30
SHIPTOCITY	Name of post-to city.	No[b]	String	40
SHIPTOSTATE	Name of post-to county or province.	No[b]	String	10
SHIPTOCOUNTRY	Post-to country code. See Appendix B, "ISO Country Codes."	No[b]	Alpha	2
SHIPTOZIP	US post-to ZIP code or other country-specific postcode.	No[b]	String	20
TAXAMT	Sum of tax for all items in this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. See the CURRENCY entry in this table for details. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	10

***TABLE 4.1 Transaction parameters** (Continued)*

Parameter	Description	Required	Type	Max. Length
VERBOSITY	Either of two values: LOW or MEDIUM. LOW is the default setting — normalised values. MEDIUM returns the PayPal processor's raw response values. See Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results."	No	Alpha	

a. Some transaction types do not require this parameter. See "Values Required by All Transaction Types" on page 21.
b. If you pass in any of the post-to address parameters such as SHIPTOCITY or SHIPTOSTATE, you must pass in the complete set (that is, SHIPTOSTREET, SHIPTOCITY, SHIPTOSTATE, SHIPTOCOUNTRY and SHIPTOZIP).

Additional Parameters by Transaction Type

Each Direct Payment credit card transaction type has its own request parameter requirements. These are in addition to the parameters required by all transactions described in the following tables in Chapter 3, "Creating a Simple Transaction Request."

- Table 3.1, "Connection parameters"
- Table 3.2, "Required transaction parameters"

Transaction responses are described in Chapter 7, "Responses to Transaction Requests."

Submitting Sale Transactions

The Sale transaction (TRXTYPE=S) charges the specified amount against the account, and marks the transaction for immediate fund transfer during the next settlement period. PayPal submits each merchant's transactions for settlement on a daily basis.

When to Use a Sale Transaction

A Sale transaction is best suited to businesses that provide immediate fulfilment for their products or services. Electronic goods merchants, for example, who fulfil orders immediately can use Sale transactions. If your business does not provide immediate fulfilment, then credit card association rules recommend that you use the Authorisation and Delayed Capture model. For details, see "Submitting Authorisation/Delayed Capture Transactions" on page 35. If you need to recharge a credit card and you are not storing the credit card information in your local database, you can perform a new reference transaction based on a Sale transaction. For details, see "Recharging to the Same Credit Card (Reference Transactions)" on page 42.

Additional Parameters for Sale Transactions

To perform a Sale transaction, you are required to pass the following parameters:

ACCT
AMT
EXPDATE

Typical Sale Transaction Parameter String

The following is a typical PARMLIST string passed in a Sale transaction.

EXAMPLE 4.1 Typical Sale transaction parameter string

```
"TRXTYPE=S&TENDER=C&USER=SuperMerchant&PWD=SuperUserPassword&PARTNER=PayPal
UK&ACCT=5105105105105100&EXPDATE=1209&AMT=99.06&COMMENT1=Reservation&FIRSTN
AME=John&LASTNAME=Jones&STREET=123 Main St.&CITY=San
Jose&STATE=CA&ZIP=123451234&COUNTRY=US&CVV2=123&CLIENTIP=0.0.0.0"
```

Note that, besides the required parameters that you pass in a Sale transaction, this string includes other typical parameters. PayPal recommends that you include the account holder's FIRSTNAME and LASTNAME. PayPal also recommends including CLIENTIP to help detect possible fraud. The COMMENT1 field helps to track transaction information. The customer's postal address (STREET) and ZIP (postcode) should be passed to use the Address Verification Service (AVS). CVV2 is needed for card security code validation. For details on AVS and card security code, see the following sections:

- "Using Address Verification Service" on page 45
- "Card Security Code Validation" on page 46

The following is a typical set of Response parameters. See Chapter 7, "Responses to Transaction Requests," for details on response parameters.

EXAMPLE 4.2 Typical response parameters

```
RESULT=0&PNREF=EFIP0D391C30&RESPMSG=Approved&AVSADDR=N&AVSZIP=Y&CVV2MATCH=X
&PPREF=7XX11903GL026951F&CORRELATIONID=3a5df0066697a
```

Submitting Authorisation/Delayed Capture Transactions

An Authorisation (TRXTYPE=A) transaction places a hold on the cardholder's open-to-buy limit, lowering the cardholder's limit by the amount of the transaction. It does not transfer funds.

One or more Delayed Capture (TRXTYPE=D) transactions are performed after an Authorisation to capture the original Authorisation amount. You can perform up to ten partial captures for a single authorisation provided the buyer is in good standing. A partial capture keeps the funds in a Pending status. A Delayed Capture is scheduled for settlement during the next settlement period.

Because Visa and MasterCard regulations prohibit capturing credit card transaction funds until a product or service has been sent to the buyer, most processing networks implement an Authorisation transaction followed by one or more Delayed Capture transactions.

When to Use Authorisation/Delayed Capture Transactions

If your business does not provide immediate fulfilment of products or services, you should use this two-stage transaction model, also known as *Delayed Capture processing*, because it enables you to capture credit card transaction funds when your are ready to collect them.

If your business provides immediate fulfilment, you can use a simple Sale transaction instead. For details, see "Submitting Sale Transactions" on page 34. If you need to recharge a credit card and you are not storing the credit card information in your local database, you can perform a new reference transaction based on a Sale. For details, see "Recharging to the Same Credit Card (Reference Transactions)" on page 42.

Required Authorisation Transaction Parameters

To perform an Authorisation transaction, you are required to pass the following parameters:

ACCT
AMT
EXPDATE

Typical Authorisation Transaction Parameter String

A typical parameter string passed in an Authorisation transaction is the same as a Sale transaction string. The only difference is that the TRXTYPE value is A in an Authorisation.

EXAMPLE 4.3 Typical Authorisation parameter string

```
"TRXTYPE=A&TENDER=C&USER=SuperMerchant&PWD=SuperUserPassword&PARTNER=PayPal
UK&ACCT=5105105105105100&EXPDATE=1209&AMT=99.06&COMMENT1=Reservation&FIRSTN
AME=John&LASTNAME=Jones&STREET=123 Main St.&CITY=San
Jose&STATE=CA&ZIP=123451234&COUNTRY=US&CVV2=123&CLIENTIP=0.0.0.0"
```

Required Delayed Capture Transaction Parameters

To perform a Delayed Capture transaction, you are required to pass the following parameter:

ORIGID

Set ORIGID to the PNREF (Transaction ID in PayPal Manager reports) value returned from the original transaction. (For details on PNREF, see Chapter 7, "Responses to Transaction Requests.) In addition, if the amount of the capture differs from the amount of the Authorisation, you also must pass a value for AMT.

Fields Copied from the Authorisation Transaction into the Delayed Capture Transaction

The following fields are copied from the Authorisation transaction into a Delayed Capture transaction (if they exist in the original transaction). If you provide a new value for any of these parameters when submitting the Delayed Capture transaction, then the new value is used. (Exceptions are ACCT and EXPDATE. These parameters retain their original values.)

ACCT	AMT	CITY	COMMENT1
CLIENTIP	COMMENT2	COUNTRY	CUSTCODE
EMAIL	EXPDATE	FIRSTNAME	FREIGHTAMT
INVNUM	LASTNAME	NOTE	PHONENUM
SHIPTOCITY	SHIPTOCOUNTRY	SHIPTOFIRSTNAME	SHIPTOLASTNAME
SHIPTOSTATE	SHIPTOSTREET	SHIPTO ZIP	STATE
STREET	TAXAMT	ZIP	

Step 1 Perform the Authorisation transaction

The Authorisation transaction uses the same parameters as Sale transactions, except that the transaction type is A.

The return data for an Authorisation transaction is the same as for a Sale transaction. To capture the authorised funds, perform a Delayed Capture transaction that includes the value returned for PNREF, as described in Step 2 on page 38.

EXAMPLE 4.4 Authorisation transaction parameter string

Issue Authorisation-only Transaction

```
"TRXTYPE=A&TENDER=C&USER=SuperMerchant&VENDOR=SuperMerchant&PARTNER=PayPalU
K&PWD=SuperUserPassword&ACCT=5105105105105100&EXPDATE=1209&AMT=9.06COMMENT1
=Reservation&FIRSTNAME=John&LASTNAME=Jones&STREET=123 Main St.&CITY=San
Jose&STATE=CA&ZIP=123451234&COUNTRY=US&CVV2=123&CLIENTIP=0.0.0.0"
```

EXAMPLE 4.5 Authorisation response

(For details on response parameters, see Chapter 7, “Responses to Transaction Requests.”)

```
RESULT=0&PNREF=EFHP0D426838&RESPMSG=Approved&AVSADDR=N&AVSZIP=Y&CVV2MATCH=X
&PPREF=68W3371331353001F&CORRELATIONID=2e52df7ddf292
```

Step 2 Perform a Delayed Capture transaction

Set ORIGID to the PNREF value returned in the original Authorisation transaction response string. (There is no need to retransmit the credit card or billing address information — it is stored at PayPal.)

If the capture succeeds, the amount of the Sale is transferred to the merchant's account during the daily settlement process. If the capture does not succeed, the hold on the cardholder's open-to-buy is still in effect.

EXAMPLE 4.6 Delayed Capture transaction parameter string

```
"TRXTYPE=D&TENDER=C&USER=SuperMerchant&VENDOR=SuperMerchantPARTNER=PayPalUK
&PWD=SuperUserPassword&TENDER=C&COMMENT1=Reservation&ORIGID=EFHP0D426838"
```

EXAMPLE 4.7 Delayed Capture response

```
RESULT=0&PNREF=EFHP0D42687C&RESPMSG=Approved&PPREF=1F987159809825103&CORREL
ATIONID=b5689409e279f&FEEAMT=0.56&PAYMENTTYPE=instant&PENDINGREASON=complet
ed
```

Delayed Capture Transaction: Capturing Transactions for Lower Amounts

You can perform a Delayed Capture transaction for an amount lower than the original Authorisation amount (useful, for example, when you make a partial delivery). To perform a partial capture programmatically using the PayPal SDK, set CAPTURECOMPLETE to N in the Delayed Capture transaction request. Setting CAPTURECOMPLETE to Y voids any remaining amount of the original authorised transaction.

You can also perform Authorisations and Delayed Captures through PayPal Manager. For details, see PayPal Manager Online Help.

NOTE: The Switch and Solo card types do not support Delayed Capture transactions.

Example Partial Capture Transaction

In this example, you authorise an amount of £100 for a consignment and charge £66 for the first partial delivery using a Delayed Capture transaction. You charge the £34 for the final part of the delivery using a second Delayed Capture transaction to draw credit card and postal address information from the initial Authorisation transaction.

Step 1 Submit the Initial transaction (Authorisation in this example)

This example uses an Authorisation transaction for the full amount of a purchase of £100.

EXAMPLE 4.8 Authorisation for the full amount of the purchase

```
"TRXTYPE=A&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&ACCT=5555555555554444&EXPDATE=0308&AMT=100.00&INVNU
M=123456789&FIRSTNAME=John&LASTNAME=Jones&STREET=5199 MAPLE&ZIP=94588"
```

Note the value of the PNREF in the response.

EXAMPLE 4.9 Response to the Authorisation

```
RESULT=0&PNREF=EFHP0D426A51&RESPMSG=Approved&AVSADDR=N&AVSZIP=Y&CVV2MATCH=X
&PPREF=6FS950632E172331R&CORRELATIONID=3c1a7c1c411a
```

Step 2 Capture the authorised funds for a partial delivery of £66

When you deliver the first £66 worth of product, you use a Delayed Capture transaction to collect the £66. Set ORIGID to the value of PNREF in the original Authorisation and set CAPTURECOMPLETE to N.

EXAMPLE 4.10 Delayed Capture with CAPTURECOMPLETE=N

```
"TRXTYPE=D&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&CAPTURECOMPLETE=N&ORIGID=EFHP0D426A51&AMT=66.00"

RESULT=0&PNREF=VXYZ01234568&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N&CORRELATIONI
D=2dc60e253492e
```

Step 3 Capture the £34 balance for the rest of the consignment

Once you have sent the remainder of the product, you can collect the remaining £34 in a second Delayed Capture transaction, setting CAPTURECOMPLETE to Y.

EXAMPLE 4.11 Delayed Capture with CAPTURECOMPLETE=Y

```
"TRXTYPE=D&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&CAPTURECOMPLETE=Y&ORIGID=EFHP0D426A51&AMT=34.00"
RESULT=0&PNREF=VXYZ01234569&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N&CORRELATIONI
D=2dc60e253493e
```

Delayed Capture Transaction: Capturing Transactions for Higher Amounts

You can perform a Delayed Capture transaction for an amount higher than the original Authorisation amount, however, you are charged for an extra transaction. In addition, the cardholder's open-to-buy is reduced by the sum of the original Authorisation-only amount and the final Delayed Capture amount.

Delayed Capture Transaction: Error Handling and Retransmittal

If an error occurs while processing a Delayed Capture transaction, it is safe to retry the capture with values that allow the server to successfully process it. Conversely, if a capture for a previous Authorisation succeeds, subsequent attempts to capture it again will return an error.

Submitting Credit Transactions

The Credit transaction (TRXTYPE=C) refunds the specified amount to the cardholder.

Required Credit Transaction Parameters

Credit transactions are permitted only against existing Sale and Delayed Capture transactions. To submit a Credit transaction, you must pass the following parameter:

ORIGID

Set the value of ORIGID to the PNREF value returned for the original transaction. (PNREF is displayed as the Transaction ID in PayPal Manager reports. For details on PNREF, see Chapter 7, "Responses to Transaction Requests."). If you do not specify an amount, then the amount of the original transaction is credited to the cardholder.

Fields Copied from the Original Transaction into the Credit Transaction

The following fields are copied from the original transaction into the Credit transaction (if they exist in the original transaction). If you provide a new value for any of these parameters when submitting the Credit transaction, then the new value is used. (Exceptions are ACCT and EXPDATE. These parameters retain their original values.)

NOTE: The TAXAMT and FREIGHTAMT parameters are not copied for referenced credits.

ACCT	AMT	CITY	COMMENT1
CLIENTIP	COMMENT2	COUNTRY	CUSTCODE
EMAIL	EXPDATE	FIRSTNAME	INVNUM
LASTNAME	SHIPTOCITY	SHIPTOCOUNTRY	SHIPTOFIRSTNAME
SHIPTOLASTNAME	SHIPTOSTATE	SHIPTOSTREET	SHIPTOZIP
STATE	STREET	PHONENUM	ZIP

Credit Transaction Parameter Strings

This is an example Credit transaction string.

```
"TRXTYPE=C&TENDER=C&PARTNER=PayPalUK&VENDOR=SuperMerchant&USER=SuperMerchan
t&PWD=SuperUserPassword&ORIGID=EFHP0D426A62"
```

Submitting Void Transactions

The Void transaction (TRXTYPE=V) prevents a transaction from being settled but does not release the Authorisation (hold on funds) on the cardholder's account.

When to Use a Void Transaction

Follow these guidelines:

- You can only void Authorisation transactions.
- You can only use a Void transaction on a transaction that has not yet settled. To refund a customer's money for a settled transaction, you must submit a Credit transaction.

Required Void Transaction Parameters

To submit a Void transaction, you must pass the following parameter:

ORIGID

Set ORIGID to the PNREF (Transaction ID in PayPal Manager reports) value returned for the original transaction. (For details on PNREF, see Chapter 7, "Responses to Transaction Requests.")

Fields Copied from the Original Transaction into the Void Transaction

The following fields are copied from the original transaction into the Void transaction (if they exist in the original transaction). If you provide a new value for any of these parameters when submitting the Void transaction, then the new value is used. (Exceptions are ACCT and EXPDATE. These parameters retain their original values.)

ACCT	AMT	CITY	COMMENT1
CLIENTIP	COMMENT2	COUNTRY	CUSTCODE
EMAIL	EXPDATE	FIRSTNAME	FREIGHTAMT
INVNUM	LASTNAME	NOTE	PHONENUM
SHIPTOCITY	SHIPTOCOUNTRY	SHIPTOFIRSTNAME	SHIPTOLASTNAME
SHIPTOSTATE	SHIPTOSTREET	SHIPTOZIP	STATE
STREET	TAXAMT	ZIP	

Example Void Transaction Parameter String

This is an example Void transaction parameter string.

EXAMPLE 4.12 Void transaction parameter string

```
"TRXTYPE=V&TENDER=C&PARTNER=PayPalUK&VENDOR=SuperMerchant&USER=SuperMerchan
t&PWD=SuperUserPassword&ORIGID=EFHP0D426A68"
```

Recharging to the Same Credit Card (Reference Transactions)

If you need to recharge a credit card and you are not storing the credit card information in your local database, you can perform a *reference* transaction. A reference transaction takes the existing credit card information that is on file and reuses it.

When to Use a Reference Transaction

Say that Joe Smith purchases a holiday gift from your website shop and requests that it be sent by UPS ground service. That evening, Joe becomes concerned that the item might not arrive in time for the holiday. So he calls you to upgrade postage to second-day air. You obtain his approval for charging an extra £10 for the upgrade. In this situation, you can create a reference transaction based on the original Sale and charge an additional £10 to Joe's credit card without having to ask him again for his credit card information.

CAUTION! *As a security measure, reference transactions are disallowed by default. Only your account administrator can enable reference transactions for your account. If you attempt to perform a reference transaction in an account for which reference transactions are disallowed, RESULT code 117 is returned. See PayPal Manager online help for instructions on setting reference transactions and other security features.*

Sale and Authorisation transactions can make use of a reference transaction as a source of transaction data. PayPal looks up the reference transaction and copies its transaction data into the new Sale or Authorisation transaction.

IMPORTANT: *When PayPal looks up the reference transaction, neither the transaction being referenced nor any other transaction in the database is changed in any way. That is, a reference transaction is a read-only operation — only the new transaction is populated with data and acted upon. No linkage is maintained between the reference transaction and the new transaction.*

You can also initiate reference transactions from PayPal Manager. See *PayPal Manager Online Help* for details.

Transaction Types that Can Be Used as the Original Transaction

You can reference any of the supported transaction types shown below to supply data for a new Sale or Authorisation transaction:

- Sale
- Authorisation (To capture the funds for an approved Authorisation transaction, be sure to perform a Delayed Capture transaction — **not** a Reference transaction.)
- Void
- Delayed Capture
- Credit

NOTE: PayPal Express Checkout does not support reference transactions for Authorisations or Sales. Reference transactions are only supported for Voids, Delayed Captures and Credits. For details on PayPal Express Checkout, see Chapter 6, "PayPal Express Checkout Transaction Processing."

Fields Copied from Reference Transactions

The following fields are copied from the reference transaction into the new Sale or Authorisation transaction (if they exist in the original transaction). If you provide a value for any of these parameters when submitting the new transaction, then the new value is used.

ACCTTYPE	STREET
ACCT	CITY
EXPDATE	STATE
FIRSTNAME	ZIP
LASTNAME	COUNTRY

Example Reference Transaction

In this example, you authorise an amount of £100 for a consignment and charge £66 for the first partial delivery using a normal Delayed Capture transaction. You charge the £34 for the final part of the delivery using a reference transaction to draw credit card and postal address information from the initial Authorisation transaction.

Step 1 Submit the Initial transaction (Authorisation in this example)

You use an Authorisation transaction for the full amount of the purchase of £100.

EXAMPLE 4.13 Authorisation for the full amount of the purchase

```
"TRXTYPE=A&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&ACCT=5555555555554444&EXPDATE=0308&AMT=100.00&INVNU
M=123456789&FIRSTNAME=John&LASTNAME=Jones&STREET=5199 MAPLE&ZIP=94588"
```

Note the value of the PNREF in the response.

EXAMPLE 4.14 Response to the Authorisation

```
RESULT=0&PNREF=EFHP0D426A51&RESPMSG=Approved&AVSADDR=N&AVSZIP=Y&CVV2MATCH=X
&PPREF=6FS950632E172331R&CORRELATIONID=3c1a7c1c411a
```

Step 2 Capture the authorised funds for a partial delivery of £66

When you deliver the first £66 worth of product, you use a normal Delayed Capture transaction to collect the £66. Set ORIGID to the value of PNREF in the original Authorisation.

EXAMPLE 4.15 Partial capture of the purchase amount

```
"TRXTYPE=D&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&ORIGID=EFHP0D426A51&AMT=66.00"

RESULT=0&PNREF=VXYZ01234568&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N&CORRELATIONI
D=2dc60e253495e
```

Step 3 Submit a new Sale transaction of £34 for the rest of the delivery

Once you have sent the remainder of the product, you can collect the remaining £34 in a Sale transaction that uses the initial Authorisation as a reference transaction.

EXAMPLE 4.16 New Sale transaction for the balance

```
"TRXTYPE=S&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&ORIGID=EFHP0D426A51&AMT=34.00"

RESULT=0&PNREF=EFHP0D426A53&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N&CORRELATIONI
D=2dc60e253495e
```

NOTE: In the case that your business model uses Authorisation/Delayed Capture for all transactions, you could have chosen to use partial captures to collect the £34. For an example, see "Delayed Capture Transaction: Capturing Transactions for Lower Amounts" on page 38.

Using Address Verification Service

Address Verification Service (AVS) consists of the information — postal address and postcode.

AVS compares the submitted billing postal address and postcode with the values on file at the cardholder's bank. The response includes values for AVSADDR and AVSZIP: Y, N or X for the match status of the customer's postal address and postcode. Y = match, N = no match, X = cardholder's bank does not support AVS. The AVS result is for advice only. Banks do not decline transactions based on the AVS result — the merchant makes the decision to approve or decline a transaction. AVS is supported by most US banks and some international banks.

NOTE: AVS checks only for a street number match, not a street name match, so 123 Main Street returns the same response as 123 Elm Street.

The International Address Verification Service response indicates whether the AVS response is international (**Y**), USA (**N**), or cannot be determined (**X**). SDK version 3.06 or later is required.

Example AVS Request Parameter String

This example request includes the AVS request parameters STREET and ZIP.

EXAMPLE 4.17 Request string with AVS request parameters

```
"TRXTYPE=A&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00&STRE
ET=5199 Maple&ZIP=98765"
```

Example AVS Response

In this example, the address value matches the value in the bank's records, but the postcode does not. The IAVS response is **X**.

EXAMPLE 4.18 AVS response parameters

```
RESULT=0&PNREF=EFHP0D426A56&RESPMSG=APPROVED&AVSADDR=Y&AVSZIP=N&IAVS=X&CORR
ELATIONID=2dc60e253496a
```

For details on Address Verification responses, see "Address Verification Responses from PayPal" on page 73.

Card Security Code Validation

The card security code is a three or four-digit number (not part of the credit card number) that is printed on the credit card. Because the card security code appears only on the card and not on receipts or statements, the card security code provides some assurance that the physical card is in the possession of the buyer.

NOTE: This fraud prevention tool has various names, depending on the payment network. Visa calls it CVV2 while MasterCard calls it CVC2. To ensure that your customers see a consistent name, PayPal recommends use of the term card security code on all end-user materials.

You must provide a CVV2 value as a transaction parameter for those credit cards that use card security code validation. The value is required for Visa, MasterCard, Switch, and Solo cards.

IMPORTANT: *To comply with credit card association regulations, you must not store the CVV2 value.*

American Express Card Security Code Enhancements

In a card-not-present environment, American Express recommends that you include the following information in your authorisation message:

- Card member billing name
- Postal information (SHIPTO* parameters) such as:
  - Address
  - Name
  - Postage method
- Customer information such as:
  - Email address
  - IP address
  - Host name
  - Browser type
- Order information such as product SKU)

On most cards, the card security code is printed on the back of the card (usually in the signature field). All or part of the card number appears before the card security code (**567** in the example).

For details on PayPal processor card security code responses, see "Card Security Code Results" on page 74.

Example CVV2 Request Parameter String

This example request parameter string includes the CVV2 parameter.

EXAMPLE 4.19 CVV2 request parameter string

```
"TRXTYPE=A&TENDER=C&PWD=SuperUserPassword&PARTNER=PayPalUK&VENDOR=SuperMerc
hant&USER=SuperMerchant&&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00&CVV
2=567"
```

Example CVV2 Response

In this example result, the card security code value matches the value in the bank's records.

EXAMPLE 4.20 CVV2 response

```
RESULT=0&PNREF=VXW412345678&RESPMSG=APPROVED&CVV2MATCH=Y&CORRELATIONID=2dc
60e2534971
```

5 Testing Credit Card Transactions

To test your application, direct all transactions to **pilot-payflowpro.paypal.com**. Transactions directed to this URL are processed through PayPal's simulated payment network, enabling you to test the configuration and operation of your application or shopfront — no money changes hands. (You must activate your account and configure your application for live transactions before accepting real orders.)

Testing Guidelines

- While testing, use only the credit card numbers listed in this chapter. Other numbers produce an error.
- **Expiry Date** must be a valid date in the future (use the **mmyy** format).
- To view the credit card processor that you have selected for testing, see **Account Info > Processor Info** in PayPal Manager.

Credit Card Numbers Used for Testing

Use the following credit card numbers for testing. Any other card number produces a general failure.

TABLE 5.1 Test credit card numbers

MasterCard	5555555555554444
MasterCard	5105105105105100
Visa	4111111111111111
Visa	4012888888881881
Visa	4222222222222 **NOTE:** Even though this number has a different character count than the other test numbers, it is the correct and functional number.
Maestro	5555555555554444
Maestro	5105105105105100
Switch/Solo (Paymentech)	6331101999990016

Testing Result Code Responses

You can use the amount of the transaction to generate a particular result code. Table 5.2 lists the general guidelines for specifying amounts.

TABLE 5.2 Result codes resulting from amount submitted

Amount	Result (RESPMSG)
£0 – £10000	0 (Approved)
£10001 or greater	Certain amounts in this range return specific PayPal result codes. If the amount is in this range but does not correspond to a PayPal result code supported by this testing mechanism, result 1000 is returned.

Table5.3 shows amounts that return specific PayPal result codes.

TABLE 5.3 Obtaining PayPal result code

Result	Definition	How to test using Website Payments Pro
0	Approved	Use an AMOUNT of 10000 or less
3	Invalid transaction type	Use the AMOUNT 10402
4	Invalid amount	Use any of these as AMOUNT: 10400 10401 10403 10414
5	Invalid merchant information	Use any of these as AMOUNT: 10548 10549

***TABLE 5.3 Obtaining PayPal result code** (Continued)*

Result	Definition	How to test using Website Payments Pro
7	Field format error	Use any of these as AMOUNT: 10405 10406 10407 10408 10409 10410 10412 10413 10416 10419 10420 10421 10509 10512 10513 10514 10515 10516 10517 10518 10540 10542
12	Declined	Use any of these as AMOUNT: 10417 15002 15005 10506 10528 10539 10544 10545 10546
13	Referral	Use the AMOUNT 10422

***TABLE 5.3 Obtaining PayPal result code** (Continued)*

Result	Definition	How to test using Website Payments Pro
23	Invalid account number	Use any of these as AMOUNT: 10519 10521 10522 10527 10535 10541 10543
24	Invalid expiry date	Use any of these as AMOUNT: 10502 10508
30	Duplicate Transaction	Use the AMOUNT 10536
105	Credit error	Attempt to credit an authorisation
112	Failed AVS check	Use the AMOUNT 10505
114	CVV2 Mismatch	Use the AMOUNT 10504
1000	Generic Host (Processor) Error	Use an AMOUNT other than those listed in this column

6 PayPal Express Checkout Transaction Processing

This chapter provides guidelines on how to implement PayPal Express Checkout. The chapter introduces you to this feature and provides the information you need to get started integrating it into your website application.

NOTE: If you also plan to use PayPal Direct Payments described in Chapter 4, "Performing Direct Payment Credit Card Transactions," to process credit cards, you must use PayPal Express Checkout together with Direct Payments. Direct Payments is not a standalone feature.

In this Chapter

What Is PayPal Express Checkout?

PayPal Express Checkout offers your customers an easy, convenient checkout experience. It lets them use postal and billing information stored securely at PayPal to check out, so they don't have to re-enter it on your site.

From the perspective of website development, PayPal Express Checkout works like other Website Payments Pro features. You submit transaction information to the server as name-value pair parameter strings.

NOTE: This chapter assumes that you are familiar with the following:

- The basic transaction parameters required in all Website Payments Pro transactions, as described in Chapter 3, "Creating a Simple Transaction Request"
- The parameters for each transaction type, as described in Chapter 4, "Performing Direct Payment Credit Card Transactions"

How PayPal Express Checkout Works

Figure 6.1 summarises the PayPal Express Checkout process.

FIGURE 6.1 Customer checkout sequence

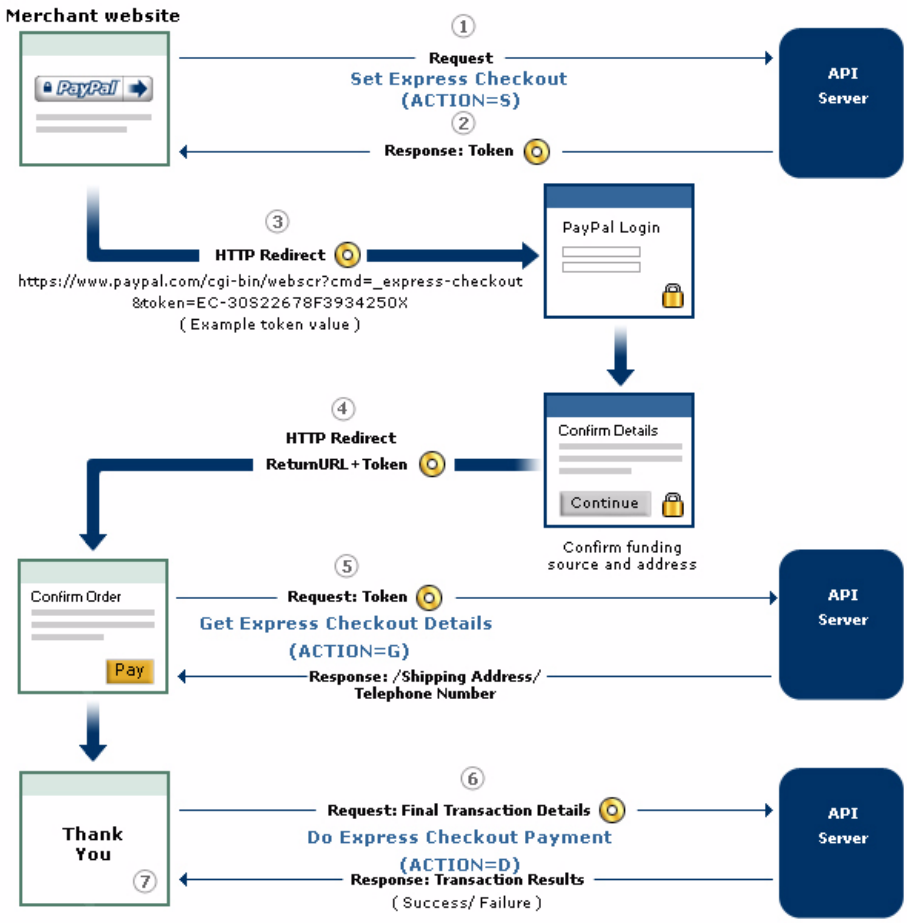


Figure 6.1 shows a typical set of web pages representing your merchant website. The PayPal logo is used by the customer to choose PayPal as their method of payment. PayPal Express Checkout gives you the flexibility to put this PayPal button graphic first in your checkout process - or on your billing page with other payment options. These guidelines are discussed in detail in Chapter 8, "PayPal Button Placement and Page Designs."

The web page layout may differ somewhat from your own web design, but the points at which the PayPal Express Checkout API calls are made and when the customer is redirected to PayPal and back to your website are important to understand. The events that take place at each numbered step in the figure are described below:

1. On your website when your customer chooses to pay with PayPal, you submit a Set Express Checkout request.
2. The server sends back a token, a string value to track your customer throughout the checkout process.
3. You direct your customer to the PayPal site, where they log in, select a funding source, and confirm contact and postal information. PayPal Express Checkout includes parameters that you can use to customise the PayPal pages so they match characteristics of your own website. For example, you can provide your own logo and colours. These parameters are described in "Set Express Checkout Request Parameters" on page 59.
4. When your customer clicks the "Continue" button, PayPal sends them back to your site at the return URL you specified in the Set Express Checkout request. The token is appended to the URL to identify the customer.
5. Optionally you can send the Get Express Checkout Details request to obtain details about your customer such as the customer's telephone number and postal address. You send the token to identify the customer. The server returns the requested information.
6. When your customer clicks the "Pay" button, you submit the Do Express Checkout Payment request to perform the actual payment transaction. The server returns the transaction result.

Sale and Authorisation Transactions

PayPal Express Checkout Sale and Authorisation transactions are handled a little differently than described in Chapter 4, "Performing Direct Payment Credit Card Transactions." Unlike a Direct Payment credit card Sale or Authorisation transaction request, which is submitted as a single request, a PayPal Express Checkout Sale or Authorisation requires that you submit at least two requests:

- Set Express Checkout
- Do Express Checkout

(A third request, Get Express Checkout Details, is optional.)

Do Express Checkout performs the actual money transfer. The Set Express Checkout and Get Express Checkout Details requests provide supporting data. To distinguish between a Sale or Authorisation request, you must pass an additional ACTION parameter with the respective value, S or G. Table 6.1 summarises the ACTION values and transaction types.

NOTE: PayPal Express Checkout does not support reference transactions for Sales and Authorisations.

TABLE 6.1 Mapping PayPal Express Checkout requests to ACTION values

Request	TRXTYPE	ACTION
Set Express Checkout	Identifies the transaction. S = Sale A = Authorisation	Is S (for Set Express Checkout)
Get Express Checkout Details	Identifies the transaction. S = Sale A = Authorisation	Is G (for Get Express Checkout Details)
Do Express Checkout Payment	Identifies the transaction. S = Sale A = Authorisation	Is D (for Do Express Checkout Payment)

Void, Delayed Capture and Credit Transactions

You perform Void, Delayed Capture and Credit transactions as described in Chapter 4, "Performing Direct Payment Credit Card Transactions," using the PayPal tender type P. Additional PayPal Express Checkout data parameters that you can use in these transaction types with PayPal Express Checkout are described in the following sections:

- "Void Transaction Parameters" on page 68
- "Delayed Capture Transaction Parameters" on page 68
- "Credit Transaction Parameters" on page 69

NOTE: PayPal Express Checkout supports reference transactions for Void, Delayed Capture and Credit transactions.

PayPal Express Checkout Sale Transaction Example

This section provides an example of a Sale transaction.

All required transaction parameters are described in Chapter 4, "Performing Direct Payment Credit Card Transactions."

Set Express Checkout (ACTION=S)

The Set Express Checkout request passes the transaction details from your website to PayPal when a customer chooses to pay with PayPal.

In addition to the parameter values required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," and the minimum required parameters for a Sale transaction described in Chapter 4, "Performing Direct Payment Credit Card Transactions," Set Express Checkout requires that you pass data for the following parameters.

ACTION
AMT
RETURNURL
CANCELURL

EXAMPLE 6.1 Set Express Checkout request parameter string for a Sale transaction

```
"TRXTYPE=S&ACTION=S&AMT=35.00&CANCELURL=http://www.order_page.com&PARTNER=P
ayPalUK&PWD=SuperUserPassword&RETURNURL=http://www.confirmation_page.com&TE
NDER=P&USER=SuperMerchant&VENDOR=SuperMerchant"
```

It is strongly recommended that RETURNURL be the URL of the final review page on your website, where the customer confirms the order and payment. Likewise, CANCELURL should be the URL of the original page on your website where the customer initially chose to use PayPal.

EXAMPLE 6.2 Set Express Checkout response

```
RESULT=0&RESPMSG=Approved&TOKEN=EC-17C76533PL706494P
```

You use the TOKEN value in the response to refer to this particular transaction in the following requests to PayPal (as shown in Figure 6.1 on page 54).

- In the HTTP request to redirect the customer's browser to the PayPal website (described in "Redirecting the Customer to PayPal Example" on page 57).
- In the Get Express Checkout Details request to obtain the customer's billing information (described in "Redirecting the Customer to PayPal Example" on page 57).
- In the Do Express Checkout Payment request to carry out the transaction (described in "Do Express Checkout Payment (ACTION=D)" on page 59).

Redirecting the Customer to PayPal Example

After your buyer clicks the PayPal button and you submit the Set Express Checkout request, you will want to automatically direct your customer to the PayPal website. The redirect URL for this is:

```
"https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=<TOKEN>"
```

where TOKEN is the value returned in the Set Express Checkout response.

PayPal recommends that you use the HTTPS response 302 "Object Moved" with your URL as the value of the Location header in the HTTPS response. Alternatively, you can generate a web page for your buyer that includes a META REFRESH tag in the header. An example is shown below. Remember to replace <TOKEN> with the token value that you received in the Set Express Checkout response.

EXAMPLE 6.3 Generating a web page with a META REFRESH tag

```
<html>
<head>
  <META HTTP-EQUIV="Refresh"CONTENT="0;URL=https://www.paypal.com/cgi-
bin/webscr?cmd=_express-checkout&token=<TOKEN>">
</head>

<body>
  <!-- Most buyers will see the text below for less than a second. -->
  <!- Some browser types (example, mobile phone) do not support META refresh tags. --
>

  <a href="https://www.paypal.com/cgi-bin/webscr?cmd=_express-
checkout&token=<TOKEN>"Click here if you are not redirected to PayPal within 5
seconds.</a>
</body>
</html>
```

Get Express Checkout Details (ACTION=G)

The Get Express Checkout Details request enables you to retrieve the customer's billing information, such as the postal address and email address. In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," Get Express Checkout Details requires that you pass data for these parameters.

ACTION
TOKEN

EXAMPLE 6.4 Get Express Checkout Details request parameter string

```
"TRXTYPE=S&VENDOR=SuperMerchant&USER=SuperMerchant&PWD=SuperUserPassword&TE
NDER=P&PARTNER=PayPalUK&ACTION=G&TOKEN=EC-17C76533PL706494P"
```

EXAMPLE 6.5 Get Express Checkout Details response

```
RESULT=0&RESPMSG=Approved&AVSADDR=Y&TOKEN=EC-
17C76533PL706494P&PAYERID=FHY4JXY7CV9PG&EMAIL=buyer_name@aol.com&PAYERSTATU
S=verified&CUSTOM=TRVV14459&FIRSTNAME=Chris&LASTNAME=Alexander&BUSINESS=Mon
roe Creek Regional Interiors&SHIPTOSTREET=5262 Green Street
#8&SHIPTOCITY=San Jose&SHIPTOSTATE=CA&SHIPTOZIP=95148&SHIPTOCOUNTRY=US
```

Redirecting the Customer to Your Website Example

PayPal redirects the customer back to your website at the location you specified in the RETURNURL parameter to Get Express Checkout request. PayPal appends the PAYERID name-value pair to the URL string, as shown below:

```
http://[RETURNURL]/?PayerID=<PAYERID>
```

You need to pass the PAYERID in the Do Express Checkout Payment request, described next.

Do Express Checkout Payment (ACTION=D)

The Do Express Checkout Payment request performs the actual money transfer of the Sale transaction.

In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," Do Express Checkout Payment request requires that you pass data for these parameters.

ACTION
TOKEN
PAYERID
AMT

EXAMPLE 6.6 Do Express Checkout Payment request parameter string

```
"TRXTYPE=S&VENDOR=SuperMerchant&USER=SuperMerchant&PWD=SuperUserPassword&TE
NDER=P&PARTNER=PayPalUK&ACTION=D&TOKEN=EC-
17C76533PL706494P&PAYERID=FHY4JXY7CV9PG&AMT=35.00"
```

EXAMPLE 6.7 Do Express Checkout Payment response

```
RESULT=0&PNREF=EFHP0CDBF5C7&RESPMSG=Approved&AVSADDR=Y&TOKEN=EC-
17C76533PL706494P&PAYERID=FHY4JXY7CV9PG&PPREF=2P599077L3553652G&PAYMENTTYPE
=instant
```

The response returns a 12-character PNREF (Payflow Manager Transaction ID) that is used by PayPal to identify this transaction in PayPal Manager reports. The PPREF value (maximum of 17 characters) is used by PayPal only to identify this transaction. For details on response parameters, see Chapter 7, "Responses to Transaction Requests."

PayPal Express Checkout Transaction Parameter Descriptions

Sale and Authorisation Transaction Parameters

Set Express Checkout Request Parameters

The Set Express Checkout request parameters include the following:

- The parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request"
- The following optional parameters listed below.

  CURRENCY
  EMAIL
  INVNUM
  ORDERDESC

  INVNUM
  SHIPTOSTREET

SHIPTOCITY
SHIPTOCOUNTRY
SHIPTOSTATE
SHIPTOZIP

- The parameters are described in Table 6.2.

TABLE 6.2 Set Express Checkout request parameters

Parameter Name	Description	Type	Max. Length
ACTION	Is S to indicate this is a Set Express Checkout request.	Alpha	1
CANCELURL	URL to which the customer is returned if the customer does not approve the use of PayPal to pay you. **NOTE:** PayPal recommends that the value of CANCELURL be the original page on which the customer chose to pay with PayPal.	String	No max length
RETURNURL	URL to which the customer's browser is returned after choosing to pay with PayPal. **NOTE:** PayPal recommends that the value of RETURNURL be the final review page on which the customer confirms the order and payment	String	No max length
TOKEN	Include this parameter to modify an existing Sale or Authorisation request. The value is returned in a previous Set Express Checkout response.	String	20
MAXAMT	The expected maximum total amount of the complete order, including postage and tax charges.	Decimal	9
CUSTOM	Free-form field for your own use such as a tracking number or other value you want PayPal to return in the Get Express Checkout Details response.	Alpha-numeric	256
REQCONFIRMSHIPPING	Is 1 or 0. The value 1 indicates that you require that the customer's postal address on file with PayPal be a confirmed address. Setting this element overrides the setting you have specified in your Merchant Account Profile.	String	1
NOSHIPPING	Is 1 or 0. The value 1 indicates that on the PayPal pages, no postal address fields should be displayed whatsoever.	String	4

TABLE 6.2 Set Express Checkout request parameters

Parameter Name	Description	Type	Max. Length
ADDROVERRIDE	Is 1 or 0. The value 1 indicates that the PayPal pages should display the postal address set by you in the postal address (SHIPTO* parameters) passed to this Set Express Checkout request, not the postal address on file with PayPal for this customer. Displaying the PayPal postal address on file does not allow the customer to edit that address.	String	4
LOCALECODE	Locale of pages displayed by PayPal during PayPal Express Checkout.	Alpha upper-case or lower-case AU or en_AU DE or de_DE FR or fr_FR GB or en_GB IT or it_IT JP or ja_JP US or en_US	5
PAGESTYLE	Sets the Custom Payment Page Style for payment pages associated with this button/link. PageStyle corresponds to the HTML variable page_style for customising payment pages. The value is the same as the Page Style Name you chose when adding or editing the page style from the Profile subtab of the My Account tab of your PayPal account.	Alpha	30
HDRIMG	A URL for the image you want to appear at the top left of the payment page. The image has a maximum size of 750 pixels wide by 90 pixels high. PayPal recommends that you provide an image that is stored on a secure (https) server.	String	127
HDRBORDERCOLOR	Sets the border colour around the header of the payment page. The border is a two-pixel perimeter around the header space, which is 750 pixels wide by 90 pixels high.	String HTML hexadecimal colour code in ASCII	6

TABLE 6.2 Set Express Checkout request parameters

Parameter Name	Description	Type	Max. Length
HDRBACKCOLOR	Sets the background colour for the header of the payment page.	String HTML hexadecimal colour code in ASCII	6
PAYFLOWCOLOR	Sets the background colour for the payment page.	String HTML hexadecimal colour code in ASCII	6

Set Express Checkout Response Parameters

Set Express Checkout response parameters include the RESULT and RESPMSG described in Chapter 7, "Responses to Transaction Requests," as well as the TOKEN parameter described in Table 6.3.

TABLE 6.3 Set Express Checkout response parameters

Parameter Name	Description	Type	Max. Length
TOKEN	A time-stamped token by which you identify to PayPal that you are processing this payment with PayPal Express Checkout. The token expires after three hours. If you set TOKEN in the Set Express Checkout request, the value of TOKEN in the response is identical to the value in the request.	String	20

Get Express Checkout Details Request Parameters

Get Express Checkout Details request parameters are described in Table 6.4.

TABLE 6.4 Get Express Checkout Details request parameters

Parameter Name	Description	Required	Type	Max. Length
ACTION	Is G to indicate this is a Get Express Checkout Details request	Yes	Alpha	1
TOKEN	String value returned by the Set Express Checkout response.	Yes	String	20

Get Express Checkout Details Response Parameters

Get Express Checkout Details response parameters include RESULT and RESPMSG described in Chapter 7, "Responses to Transaction Requests," the parameters listed below, and the parameters described in Table 6.5.

EMAIL
INVNUM
SHIIPTOCITY
SHIPTOCOUNTRY
SHIPTOSTATE
SHIPTOZIP

TABLE 6.5 Get Express Checkout Details response parameters

Parameter Name	Description	Type	Max. Length
TOKEN	String value returned by Set Express Checkout response.	String	20
SHIPTOCOUNTRYCODE	Customer's country of residence in the form of ISO standard 3166 two-character country codes. **Note:** Currently US is the only country code supported.	String	2
SHIPTOSTREET	Postal Address. **Note:** If you include a postal address and provide a value for the AddressOverride (ADDROVERRIDE) parameter, PayPal returns this same address in the Get Express Checkout Details response.	String	30
SHIPTOSTREET2	Extended postal address. Example: Bldg. 6, Flat 3.	String	30
SHIPTOBUSINESS	Customer's business name.	String	127
COUNTRY	Customer's country of residence in the form of ISO standard 3166 two-character country codes.	String	2
PAYERID	Unique PayPal customer account identification number.	String	13
PAYERSTATUS	Status of customer. Values are: verified unverified	Alpha	10
CUSTOM	Free-form field for your own use as set by you in the Set Express Checkout request.	Alpha-numeric	256

TABLE 6.5 Get Express Checkout Details response parameters

Parameter Name	Description	Type	Max. Length
PHONENUM	Account holder's telephone number. See "Obtaining the Customer's Telephone Number During PayPal Checkout" on page 64. The field mask is xxx-xxx-xxxx (US numbers) +xxxxxxxxxxx (international numbers)	String	20

Obtaining the Customer's Telephone Number During PayPal Checkout

You can request the buyer's phone number from within the PayPal checkout. You have three options:

- Not request the telephone number (default)
- Request the telephone number as an optional field
- Require that the buyer enter his or her telephone number to proceed

To set these options, log in to your PayPal account, click **Profile**, and then click **Website Payment Preferences**. The section to change the default is located at the bottom of the screen.

Do Express Checkout Payment Request Parameters

In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," the Do Express Checkout Payment request parameters include:

- The parameters listed below and described in Table 4.1, "Transaction parameters."

  BUTTONSOURCE
  CUSTOM
  FREIGHTAMT
  HANDLINGAMT
  INVNUM
  ITEMAMT
  L_AMTn
  L_DESCn
  L_QTYn
  L_TAXAMTn
  NOTIFYURL
  ORDERDESC
  SHIPTOCITY
  SHIPTOCOUNTRY
  SHIPTOSTATE
  SHIPTOSTREET
  SHIPTOZIP

- The required parameters described in Table 6.6.

TABLE 6.6 Do Express Checkout Payment request parameters

Parameter Name	Description	Required	Type	Max. Length
TOKEN	String value returned by Set Express Checkout response.	Yes	String	20
ACTION	Is D to indicate this is a Do Express Checkout Payment request.	Yes	Alpha	1
PAYERID	Unique PayPal customer account identification number. This value is returned in the URL when the customer is redirected to your website.	Yes	String	13
TAXAMT	Sum of tax for all items in this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. CURRENCY is described in Table 4.1. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	No	Decimal	6

Do Express Checkout Payment Response Parameters

The Do Express Checkout Payment response parameters include:

- RESULT, RESPMSG, PNREF, and PPREF described in Chapter 7, "Responses to Transaction Requests"
- The parameters described in Table 6.7

TABLE 6.7 Do Express Checkout Payment response parameters

Parameter Name	Description	Type	Max. Length
TOKEN	The time-stamped token value that was returned in the Set Express Checkout response.	String	20

TABLE 6.7 Do Express Checkout Payment response parameters

Parameter Name	Description	Type	Max. Length
FEEAMT	PayPal fee amount charged for the transaction. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. CURRENCY is described in Table 4.1. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	Decimal	9
PAYMENTTYPE	Returns instant if the payment is instant or eCheque if the payment is delayed.	Alpha	7
TAXAMT	Sum of tax for all items in this order. **NOTE:** You must set CURRENCY to one of the three-character currency codes for any of the supported PayPal currencies. CURRENCY is described in Table 4.1. Limitations: Must not exceed £5,500 GBP in any currency. No currency symbol. Decimal separator must be a period (.). Do not use comma separators. Use 1199.95, not 1,199.95.	Decimal	6

TABLE 6.7 Do Express Checkout Payment response parameters

Parameter Name	Description	Type	Max. Length
PENDINGREASON	The reason the payment is pending. Values are: none = No pending reason address = The payment is pending because your customer did not include a confirmed postal address and your Payment Receiving Preferences is set such that you want to manually accept or refuse each of these payments. To change your preference, go to the Preferences section of your Profile. echeque = The payment is pending because it was made by an eCheque that has not yet cleared. intl = The payment is pending because you hold a non-US account and do not have a withdrawal mechanism. You must manually accept or refuse this payment from your Account Overview. multi-currency = You do not have a balance in the currency sent, and you do not have your Payment Receiving Preferences set to automatically convert and accept this payment. You must manually accept or refuse this payment. verify = The payment is pending because you are not yet verified. You must verify your account before you can accept this payment. other = The payment is pending for a reason other than those listed above. For more information, contact PayPal customer service. completed = The payment has been completed, and the funds have been added successfully to your account balance.	String	

Pending Payments. If the Do Express Checkout Payment PENDINGREASON response is a value other than none or Completed, the payment is pending. Typically, the customer has paid with an eCheque. In such a case, funds are not guaranteed, and you should not send or deliver items or services until the payment has successfully completed. To find out the status of a pending payment, sign up for PayPal's instant payment notification service (IPN). You can also check the status using PayPal Manager. See PayPal Manager Online Help for details.

Void Transaction Parameters

In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," and the Void transaction parameters described in Chapter 4, "Performing Direct Payment Credit Card Transactions," the following NOTE parameter can be used in PayPal Express Checkout Void transactions.

TABLE 6.8 Void transaction optional request parameters

Parameter Name	Description	Required	Type	Max. Length
NOTE	An informal note about this settlement that is displayed to the customer in an email and in the customer's transaction history.	No	String	255

Delayed Capture Transaction Parameters

In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," and the Delayed Capture transaction parameters described in Chapter 4, "Performing Direct Payment Credit Card Transactions," the following NOTE parameter can be used in PayPal Express Checkout Delayed Capture transactions.

TABLE 6.9 Delayed Capture transaction optional request parameters

Parameter Name	Description	Required	Type	Max. Length
NOTE	An informal note about this settlement that is displayed to the customer in an email and in the customer's transaction history.	No	String	255

In addition to the response parameters described in Chapter 4, "Performing Direct Payment Credit Card Transactions," the following PAYMENTTYPE parameter can be returned in PayPal Express Checkout Delayed Capture responses.

TABLE 6.10 Delayed Capture transaction response parameters

Parameter Name	Description	Type	Max. Length
PAYMENTTYPE	Returns instant if the payment is instant or eCheque if the payment is delayed.	String	7

Credit Transaction Parameters

In addition to the parameters required by all transaction types described in Chapter 3, "Creating a Simple Transaction Request," and the parameters described in Table 4.1, "Transaction parameters," the following MEMO parameter can be used in PayPal Express Checkout Credit transactions.

NOTE: PayPal Express Checkout only supports reference transactions for Credits.

TABLE 6.11 Credit transaction request parameters

Parameter Name	Description	Required	Type	Max. Length
MEMO	Custom memo about the credit.	No	Alphanumeric	255

7 Responses to Transaction Requests

This chapter describes the contents of a response to a transaction request. When a transaction finishes, the Payflow server returns a response string made up of name-value pairs. For example, this is a response to a credit card Sale transaction request:

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456
&AVSADDR=Y&AVSZIP=N&IAVS=Y&CVV2MATCH=Y
```

Contents of a Transaction Response

All transaction responses include values for RESULT, PNREF and RESPMSG. Values for AVSADDR and AVSZIP are included if you use AVS. Table 7.1 describes the values returned in a response string.

TABLE 7.1 Transaction response values

Field	Description	Type	Length
PNREF	Reference ID, a unique number that identifies the transaction. PNREF is described in "PNREF Format" on page 75.	Alphanumeric	12
RESULT	The outcome of the attempted transaction. A result of 0 (zero) indicates the transaction was approved. Any other number indicates a decline or error. RESULT codes are described in "RESULT Codes and RESPMSG Values" on page 76.	Numeric	Variable
CVV2MATCH	Result of the card security code (CVV2) check. The issuing bank may decline the transaction if there is a mismatch. In other cases, the transaction may be approved despite a mismatch.	Alpha Y, N, X, or no response For details on PayPal-specific responses, also see "Card Security Code Results," in this chapter.	1

***TABLE 7.1 Transaction response values** (Continued)*

Field	Description	Type	Length
PPREF	Unique transaction ID of the payment. If the TRXTYPE of the request is A, then you will need the value of PPREF for use with Authorisation and Delayed Capture transactions.	string	17
RESPMSG	The response message returned with the transaction result. Exact wording varies. Sometimes a colon appears after the initial RESPMSG followed by more detailed information. Response messages are described in "RESULT Codes and RESPMSG Values" on page 76.	Alphanumeric	Variable
AVSADDR	AVS address responses are for advice only. This process does not affect the outcome of the authorisation. See "Using Address Verification Service" on page 45. For details on PayPal-specific responses, also see "Address Verification Responses from PayPal," in this chapter.	Alpha Y, N, X, or no response.	1
AVSZIP	AVS postcode responses are for advice only. This process does not affect the outcome of the authorisation. See "Using Address Verification Service" on page 45. For details on PayPal-specific responses, also see "Address Verification Responses from PayPal," in this chapter.	Alpha Y, N, X, or no response	1
PROCAVS	AVS response from the processor when the merchant sends a VERBOSITY request parameter value of MEDIUM. See Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results," for details.	Char	1
PROCCVV2	CVV2 response from the processor when the merchant sends a VERBOSITY request parameter value of MEDIUM. See Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results," for details.	Char	1

***TABLE 7.1 Transaction response values** (Continued)*

Field	Description	Type	Length
IAVS	International AVS address responses are for advice only. This value does not affect the outcome of the transaction. Indicates whether AVS response is international (**Y**), US (**N**), or cannot be determined (**X**). Client version 3.06 or later is required.	Alpha Y, N, X, or no response	1
PAYMENTTYPE	Returns instant if the payment is instant or eCheque if the payment is delayed.	String	7
CORRELATIONID	Value used for tracking this Direct Payment transaction.	Alphanumeric	13

Address Verification Responses from PayPal

Table 7.2, "Address verification response value mapping," compares the detailed response returned by the PayPal processor for address verification to the normalised response value (Y, N or X) returned in the AVSADDR and AVSZIP response parameters. If you want to obtain the PayPal processor value, set the VERBOSITY parameter to MEDIUM. With this setting, the processor value is returned in the PROCAVS response parameter. For details on VERBOSITY, see Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results."

TABLE 7.2 Address verification response value mapping

PayPal Processor AVSCode	PayPal Processor AVSCode Meaning	AVSADDR	AVSZIP
A	Address	Y	N
B	International "A"	Y	N
C	International "N"	N	N
D	International "X"	Y	Y
E	Not allowed for MOTO (Internet/Phone) transactions	X	X
F	UK-specific "X"	Y	Y
G	Global Unavailable	X	X
I	International Unavailable	X	X
N	No	N	N

***TABLE 7.2 Address verification response value mapping** (Continued)*

PayPal Processor AVSCode	PayPal Processor AVSCode Meaning	AVSADDR	AVSZIP
P	Postal (International “Z”)	N	Y
R	Retry	X	X
S	Service Not Supported	X	X
U	Unavailable	X	X
W	Whole Postcode	N	Y
X	Exact Match	Y	Y
Y	Yes	Y	Y
Z	Zip (postcode)	N	Y
All other		X	X

Card Security Code Results

The CVV2MATCH parameter returns Y, N, or X or a PayPal processor-specific response.

Normalised Results

If you submit the transaction request parameter for card security code (that is, the CVV2 parameter), the cardholder’s bank returns a normalised Yes/No response in the CVV2MATCH response parameter, as described in Table 7.3.

TABLE 7.3 CVV2MATCH response values

CVV2MATCH Value	Description
Y	The submitted value matches the data on file for the card.
N	The submitted value does not match the data on file for the card.
X	The cardholder’s bank does not support this service.

PayPal Card Security Code Results

Table 7.4, "Card security code response code mapping," shows the detailed results returned by the PayPal processor for card security codes. If you want to obtain the PayPal processor value, set the VERBOSITY parameter to MEDIUM. The processor value is returned in the PROCCVV2 response parameter. For details on VERBOSITY, see Appendix A, "Verbosity: Viewing Processor-Specific Transaction Results."

TABLE 7.4 Card security code response code mapping

PayPal Processor CVV2 Code	PayPal Processor Code Description	PROCVV2MATCH
M	Match	Y
N	No Match	N
P	Not Processed	X
S	Service Not Supported	X
U	Unavailable	X
X	No Response	X
All other		X

PNREF Value

The PNREF is a unique transaction identification number issued by the Payflow server that identifies the transaction for billing, reporting and transaction data purposes. The PNREF value appears in the Transaction ID column in PayPal Manager reports.

- The PNREF value is used as the ORIGID value (original transaction ID) in delayed capture transactions (TRXTYPE=D), credits (TRXTYPE=C), inquiries (TRXTYPE=I) and voids (TRXTYPE=V).
- The PNREF value is used as the ORIGID value (original transaction ID) value in reference transactions for authorisation (TRXTYPE=A) and Sale (TRXTYPE=S).

NOTE: The PNREF is also referred to as the Transaction ID in Payflow Link documentation.

PNREF Format

The PNREF is a 12-character string of printable characters, for example:

- EFHP0D42687C
- ACRAF23DB3C4

NOTE: Printable characters also include symbols other than letters and numbers such as the question mark (?). A PNREF typically contains letters and numbers only.

The PNREF in a transaction response tells you that your transaction is connecting to PayPal.

Historically, the contents of a PNREF indicated a test or a live transaction:

- For test servers, the first and fourth characters were alpha characters (letters), and the second and third characters were numeric, for example: V53A17230645.
- For live servers, the first four characters were alpha characters (letters), for example: VPNE12564395.

However, this is not always the case, and as a rule, you should not place any meaning on the contents of a PNREF.

RESULT Codes and RESPMSG Values

RESULT is the first value returned in the server response string. The value of the RESULT parameter indicates the overall status of the transaction attempt.

- A value of 0 (zero) indicates that no errors occurred and the transaction was approved.
- A value less than zero indicates that a communication error occurred. In this case, no transaction is attempted.
- A value greater than zero indicates a decline or error.

The response message (RESPMSG) provides a brief description for decline or error results.

RESULT Values for Transaction Declines or Errors

For non-zero Results, the response string includes a RESPMSG name-value pair. The exact wording of the RESPMSG (shown in bold) may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

TABLE C.1 Payflow transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
0	**Approved**
1	**User authentication failed.** Error is caused by one or more of the following: • Invalid Processor information entered. Contact merchant bank to verify. • 'Allowed IP Address' security feature implemented. The transaction is coming from an unknown IP address. See PayPal Manager Online Help for details on how to use Manager to update the allowed IP addresses. • You are using a test (not active) account to submit a transaction to the live PayPal servers. Change the URL from pilot-payflowpro.paypal.com to payflowpro.paypal.com.
2	**Invalid tender type.** Your merchant bank account does not support the following credit card type that was submitted.
3	**Invalid transaction type.** Transaction type is not appropriate for this transaction. For example, you cannot credit an authorisation-only transaction.
4	**Invalid amount format. Use the format: "#####.##" Do not include currency symbols or commas.**
5	**Invalid merchant information.** Processor does not recognise your merchant account information. Contact your bank account acquirer to resolve this problem.
6	Invalid or unsupported currency code
7	**Field format error.** Invalid information entered. See RESPMSG.
8	**Not a transaction server**
9	**Too many parameters or invalid stream**
10	**Too many line items**
11	**Client time-out waiting for response**
12	**Declined.** Check the credit card number, expiry date and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call their card issuing bank to resolve.
13	**Referral.** Transaction cannot be approved electronically but can be approved with a verbal authorisation. Contact your merchant bank to obtain an authorisation and submit a manual Voice Authorisation transaction.
14	**Invalid Client Certification ID.** Check the HTTP header. If the tag, X-VPS-VIT-CLIENT-CERTIFICATION-ID, is missing, RESULT code 14 is returned.
19	**Original transaction ID not found.** The transaction ID you entered for this transaction is not valid. See RESPMSG.
20	**Cannot find the customer reference number**

***TABLE C.1 Payflow transaction RESULT values and RESPMSG text** (Continued)*

RESULT	RESPMSG and Explanation
22	**Invalid ABA number**
23	**Invalid account number.** Check credit card number and re-submit.
24	**Invalid expiry date.** Check and re-submit.
25	**Invalid Host Mapping.** You are trying to process a tender type such as Discover Card, but you are not set up with your merchant bank to accept this card type.
26	**Invalid vendor account.** Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. VENDOR is your merchant ID and USER is the same as VENDOR unless you created a Payflow Pro user.
27	**Insufficient partner permissions**
28	**Insufficient user permissions**
29	**Invalid XML document.** This could be caused by an unrecognised XML tag or a bad XML format that cannot be parsed by the system.
30	**Duplicate transaction**
31	**Error in adding the recurring profile**
32	**Error in modifying the recurring profile**
33	**Error in cancelling the recurring profile**
34	**Error in forcing the recurring profile**
35	**Error in reactivating the recurring profile**
36	**OLTP Transaction failed**
37	**Invalid recurring profile ID**
50	**Insufficient funds available in account**
51	**Exceeds per transaction limit**
99	**General error.** See RESPMSG.
100	**Transaction type not supported by host**
101	**Time-out value too small**
102	**Processor not available**
103	**Error reading response from host**
104	**Timeout waiting for processor response.** Try your transaction again.
105	**Credit error.** Make sure you have not already credited this transaction, or that this transaction ID is for a creditable transaction. (For example, you cannot credit an authorisation.)
106	**Host not available**
107	**Duplicate suppression time-out**

TABLE C.1 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
108	**Void error.** See RESPMSG. Make sure the transaction ID entered has not already been voided. If not, then look at the Transaction Detail screen for this transaction to see if it has settled. (The Batch field is set to a number greater than zero if the transaction has been settled.) If the transaction has already settled, your only recourse is a reversal (credit a payment or submit a payment for a credit).
109	**Time-out waiting for host response**
110	**Referenced auth (against order) Error**
111	**Capture error.** Either an attempt to capture a transaction that is not an authorisation transaction type, or an attempt to capture an authorisation transaction that has already been captured.
112	**Failed AVS check.** Address and ZIP code (postcode) do not match. An authorisation may still exist on the cardholder's account.
113	**Merchant sale total will exceed the sales cap with current transaction.** ACH transactions only.
114	**Card Security Code (CSC) Mismatch.** An authorisation may still exist on the cardholder's account.
115	**System busy, try again later**
116	**VPS Internal error. Failed to lock terminal number**
117	**Failed merchant rule check.** One or more of the following three failures occurred: An attempt was made to submit a transaction that failed to meet the security settings specified on the PayPal Manager *Security Settings* page. If the transaction exceeded the Maximum Amount security setting, then no values are returned for AVS or CSC. AVS validation failed. The AVS return value should appear in the RESPMSG. CSC validation failed. The CSC return value should appear in the RESPMSG.
118	**Invalid keywords found in string fields**
119	**General failure within PIM Adapter**
120	**Attempt to reference a failed transaction**
121	**Not enabled for feature**
122	**Merchant sale total will exceed the credit cap with current transaction.** ACH transactions only.
125	**Fraud Protection Services Filter — Declined by filters**

TABLE C.1 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
126	**Fraud Protection Services Filter — Flagged for review by filters** **Important Note:** Result code 126 indicates that a transaction triggered a fraud filter. This is not an error, but a notice that the transaction is in a review status. The transaction has been authorised but requires you to review and manually accept the transaction before it will be allowed to settle. Result code 126 is intended to give you an idea of the kind of transaction that is considered suspicious to enable you to evaluate whether you can benefit from using the Fraud Protection Services. To eliminate result 126, turn the filters off. For more information, see the Fraud Protection Services documentation for your payments solution. It is available on the PayPal Manager Documentation page.
127	**Fraud Protection Services Filter — Not processed by filters**
128	**Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters**
131	**Version 1 Website Payments Pro SDK client no longer supported.** Upgrade to the most recent version of the Website Payments Pro client.
132	**Card has not been submitted for update**
133	**Data mismatch in HTTP retry request**
150	**Issuing bank timed out**
151	**Issuing bank unavailable**
200	**Reauth error**
201	**Order error**
402	**PIM Adapter Unavailable**
403	**PIM Adapter stream error**
404	**PIM Adapter Timeout**
600	**Cybercash Batch Error**
601	**Cybercash Query Error**
1000	**Generic host error.** This is a generic message returned by your credit card processor. The RESPMSG will contain more information describing the error.
1001	**Buyer Authentication Service unavailable**
1002	**Buyer Authentication Service — Transaction timeout**
1003	**Buyer Authentication Service — Invalid client version**
1004	**Buyer Authentication Service — Invalid timeout value**
1011	**Buyer Authentication Service unavailable**
1012	**Buyer Authentication Service unavailable**
1013	**Buyer Authentication Service unavailable**

TABLE C.1 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
1014	**Buyer Authentication Service — Merchant is not enrolled for Buyer Authentication Service (3-D Secure).**
1016	**Buyer Authentication Service — 3-D Secure error response received.** Instead of receiving a PARes response to a Validate Authentication transaction, an error response was received.
1017	**Buyer Authentication Service — 3-D Secure error response is invalid.** An error response is received and the response is not well formed for a Validate Authentication transaction.
1021	**Buyer Authentication Service — Invalid card type**
1022	**Buyer Authentication Service — Invalid or missing currency code**
1023	**Buyer Authentication Service — merchant status for 3D secure is invalid**
1041	**Buyer Authentication Service — Validate Authentication failed: missing or invalid PARES**
1042	**Buyer Authentication Service — Validate Authentication failed: PARES format is invalid**
1043	**Buyer Authentication Service — Validate Authentication failed: Cannot find successful Verify Enrolment**
1044	**Buyer Authentication Service — Validate Authentication failed: Signature validation failed for PARES**
1045	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid amount in PARES**
1046	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid acquirer in PARES**
1047	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid Merchant ID in PARES**
1048	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid card number in PARES**
1049	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid currency code in PARES**
1050	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid XID in PARES**
1051	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid order date in PARES**
1052	**Buyer Authentication Service — Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction**

RESULT Values for Communications Errors

A value for RESULT less than zero indicates that a communication error occurred. In this case, no transaction is attempted.

A value of -1 or -2 usually indicates a configuration error caused by an incorrect URL or by configuration issues with your firewall. A value of -1 or -2 can also be possible if the PayPal servers are unavailable, or an incorrect server/socket pair has been specified. A value of -1 can also result when there are Internet connectivity errors. Contact Customer Support regarding any other errors.

NOTE: Details of the response message may vary slightly depending on your SDK integration.

TABLE 3.2 RESULT values for communications errors

RESULT	Description
-1	**Failed to connect to host**
-2	**Failed to resolve hostname**
-5	**Failed to initialise SSL context**
-6	**Parameter list format error: & in name**
-7	**Parameter list format error: invalid [ ] name length clause**
-8	**SSL failed to connect to host**
-9	**SSL read failed**
-10	**SSL write failed**
-11	**Proxy authorisation failed**
-12	**Timeout waiting for response**
-13	**Select failure**
-14	**Too many connections**
-15	**Failed to set socket options**
-20	**Proxy read failed**
-21	**Proxy write failed**
-22	**Failed to initialise SSL certificate**
-23	**Host address not specified**
-24	**Invalid transaction type**
-25	**Failed to create a socket**
-26	**Failed to initialise socket layer**
-27	**Parameter list format error: invalid [ ] name length clause**

TABLE 3.2 RESULT values for communications errors *(Continued)*

RESULT	Description
-28	**Parameter list format error: name**
-29	**Failed to initialise SSL connection**
-30	**Invalid timeout value**
-31	**The certificate chain did not validate, no local certificate found**
-32	**The certificate chain did not validate, common name did not match URL**
- 40	**Unexpected Request ID found in request**
- 41	**Required Request ID not found in request**
-99	**Out of memory**
-100	**Parameter list cannot be empty**
-103	**Context initialisation failed**
-104	**Unexpected transaction state**
-105	**Invalid name value pair request**
-106	**Invalid response format**
-107	**This XMLPay version is not supported**
-108	**The server certificate chain did not validate**
-109	**Unable to do logging**
-111	**The following error occurred while initialising from message file: <Details of the error message>**
-113	**Unable to round and truncate the currency value simultaneously**

8 PayPal Button Placement and Page Designs

When you offer PayPal Express Checkout to your customers, PayPal recommends that you display it in two forms for your customers' best buying experience:

- PayPal as a checkout choice on your shopping cart page
- PayPal as a payment method

Table 8.1 summarizes these guidelines.

TABLE 8.1 PayPal Button Placement Guidelines

PayPal Button Graphic	Placement	Requirements
	At the beginning of checkout as a checkout choice	Align the PayPal Checkout button on your shopping cart page with any other checkout buttons
	At the end of checkout as a payment method option	Place the PayPal Acceptance mark: • On your Payment Billing page • On your home page, along with credit card logos, if applicable

PayPal button graphics and placement topics below include:

- HTML for PayPal Button Graphics
- Design Variation: Eliminating Your Order Review Page
- Payment Method Page Layout Recommendations

HTML for PayPal Button Graphics

You can get HTML for the Express Checkout button and PayPal Acceptance Mark from the following location: https://www.paypal.com/express-checkout-buttons

Rather than storing the button graphics on your own server, reference the PayPal image paths on the PayPal website. This ensures that you are always displaying the most up-to-date logos.

Examples of Button Placement

Below are two examples of proper PayPal button graphic placement within the context of web pages.

Figure 8.1 places the PayPal button graphic as a checkout choice.

FIGURE 8.1 PayPal as a Checkout Choice

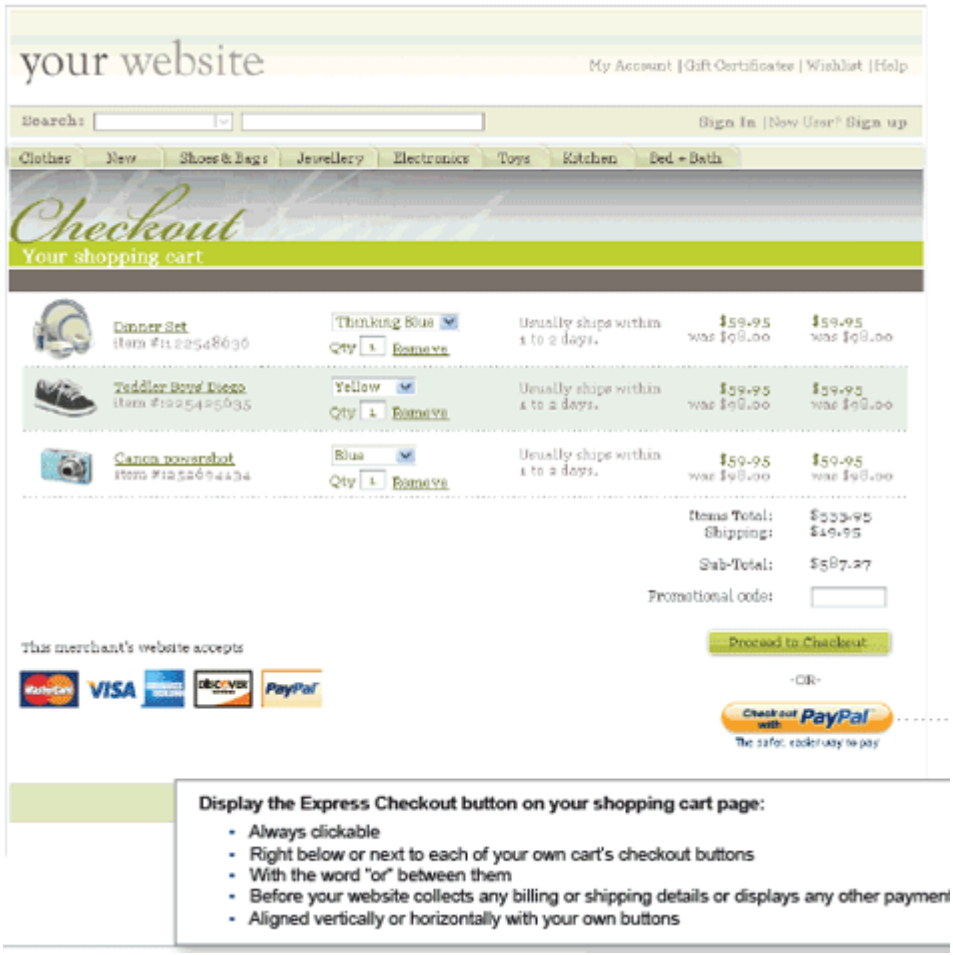
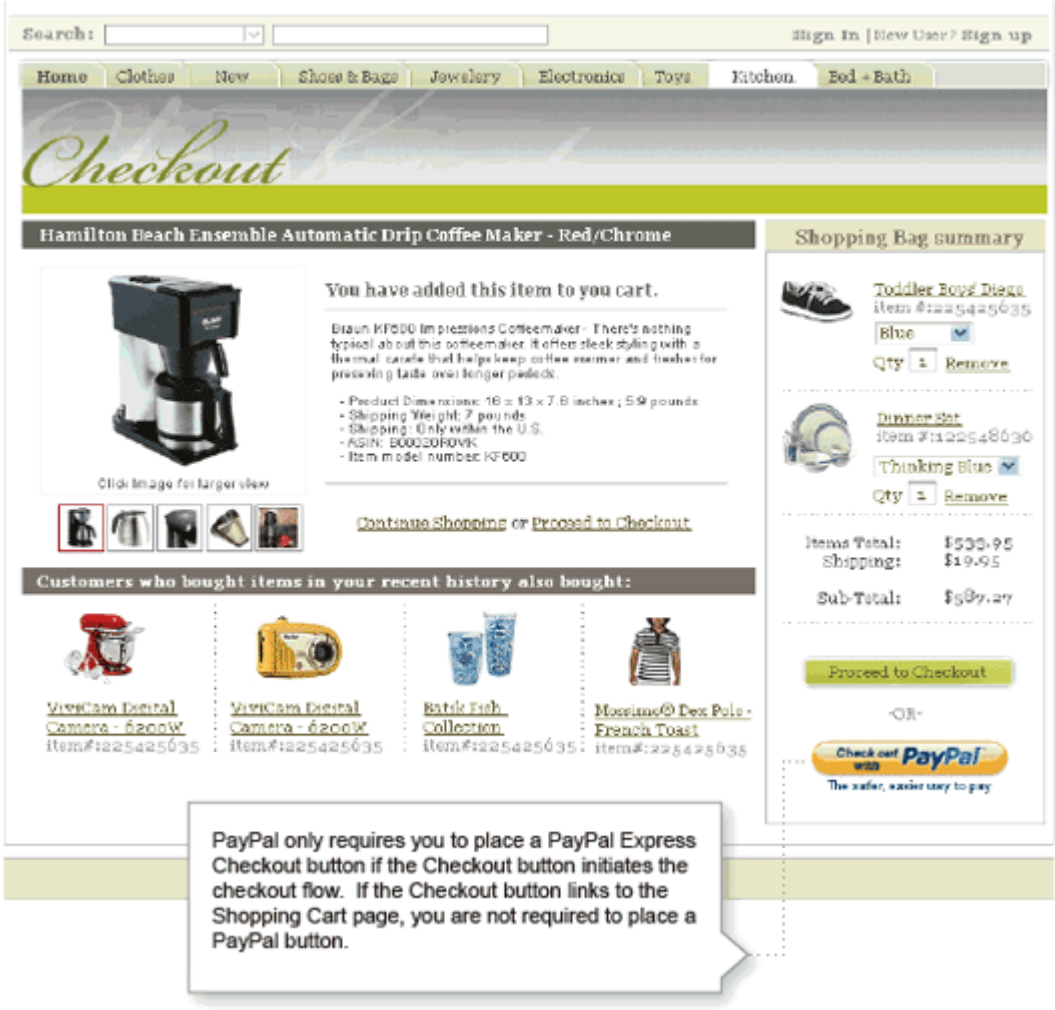


Figure 8.2 places the PayPal mark as a payment method with other payment methods.

FIGURE 8.2 PayPal Mark as a Payment Method



Design Variation: Eliminating Your Order Review Page

You can make checkout appear to complete on the PayPal website rather than on your own and, therefore, eliminate the need for an order review page on your site. (Of course, when the customer returns from PayPal, you still call the Do Express Checkout Payment request to complete the transaction.) In this situation, you would want the button text on PayPal to appear as “Pay” rather than “Continue.”

You control the button text through the value of the `useraction` variable. You set this variable on the PayPal URL to which you redirect the buyer after calling Set Express Checkout.

Values and resulting button text are described below:

- If you do not set `useraction` or you set `useraction continue`, PayPal displays the button text "Continue Checkout."
- If you set `useraction` to `commit`, PayPal displays the button text "Pay."

To display the "Pay" button text, for example, append `&useraction=commit` to the redirect URL string as shown below where *tokenvalue* is the token value returned in the Set Express Checkout response.

```
"https://www.paypal.com/cgi-bin/webscr?cmd=_express-
checkout&token=tokenvalue&useraction=commit"
```

Payment Method Page Layout Recommendations

When you display the PayPal Acceptance mark with other payment methods, you have several designs to choose from:

- As a radio button
- As horizontal field options
- In a dropdown list

IMPORTANT: *Do not preselect any payment method. Allow the customer to make a choice without any default.*

The figures below illustrate each of these layouts.

FIGURE 8.3 As a Radio Button

FIGURE 8.4 As Horizontal Field Options

FIGURE 8.5 In a Dropdown List

9 Implementing 3-D Secure Transactions

Website Payments Pro allows merchants to pass 3-D Secure™ authentication data to PayPal for debit and credit cards processed with the Direct Payment transaction requests. Updating your site with 3-D Secure enables your participation in the Verified by Visa and MasterCard SecureCode programs.

IMPORTANT: *Note the following key dates:*

- Effective 1 January, 2010, *existing* merchants who accept the Maestro card must be fully compliant with 3-D Secure for Internet-based transactions using this card. Virtual terminal transactions are not affected.
- Effective immediately, *new* merchants who want to accept Maestro must implement 3-D Secure before PayPal will enable Maestro for your account.

Introduction to 3-D Secure

3-D Secure is a protocol developed by the card schemes that improves the security of Internet payments that are not within a closed-loop checkout option (such as PayPal). It allows merchants to authenticate cardholders through the cards' issuers. Its goals are to reduce the likelihood of fraud when using supported cards and to improve transaction performance. Merchants who do not use 3-D Secure may be liable for fraudulent transactions even if the transaction was authorised by other means. Visa offers 3-D Secure under the name Verified by Visa and MasterCard offers it as MasterCard SecureCode.

PayPal enables you to pass 3-D Secure data to PayPal for Payments Pro transactions, but you must obtain the 3-D Secure authentication data from the card's issuer. PayPal has an agreement with Cardinal Commerce that allows Payments Pro merchants free access to Cardinal's 3-D Secure technology, Cardinal Centinel™. The Cardinal Centinel® Thin Client

interface provides access to payer authentication for transactions using Visa, MasterCard, and Maestro branded cards. Use of 3-D Secure authentication is optional for Visa and MasterCard transactions.

3-D Secure is *not supported* for direct Recurring Billing and Reference Transactions. Cards that require 3-D Secure authentication cannot use these APIs; however, cards where 3-D Secure is optional can continue to process transactions without authentication. If you use either of these features in your current integration, you must exclude the Maestro card type from the available options.

NOTE: Merchants must register with Cardinal Commerce before using this feature.

For more information, see

- Verified by Visa: http://www.visaeurope.com/personal/onlineshopping/verifiedbyvisa/main.jsp
- MasterCard SecureCode: http://www.mastercard.com/us/merchant/solutions/mastercard_securecode.html
- Cardinal Centinel: http://www.paypal-business.co.uk/3Dsecure.asp

Integration Overview

To use 3-D Secure with PayPal, you must do the following. Each item is explained in detail later in this document.

- Register your company with Cardinal Commerce and download and install the Cardinal Thin Client package.
- Insert processing for 3-D Secure into your application's debit or credit card payment flow immediately before the direct payment API request.
- Add additional fields to the direct payment API request.
- Update your website with required 3-D Secure logos, status windows, and other information for your customers.
- Test your 3-D Secure integration using Cardinal's testing facilities. PayPal's Sandbox cannot be used for testing 3-D Secure functionality.

Cardinal Commerce Registration and Installation

Before you can use Cardinal Centinel to obtain cardholder authentication:

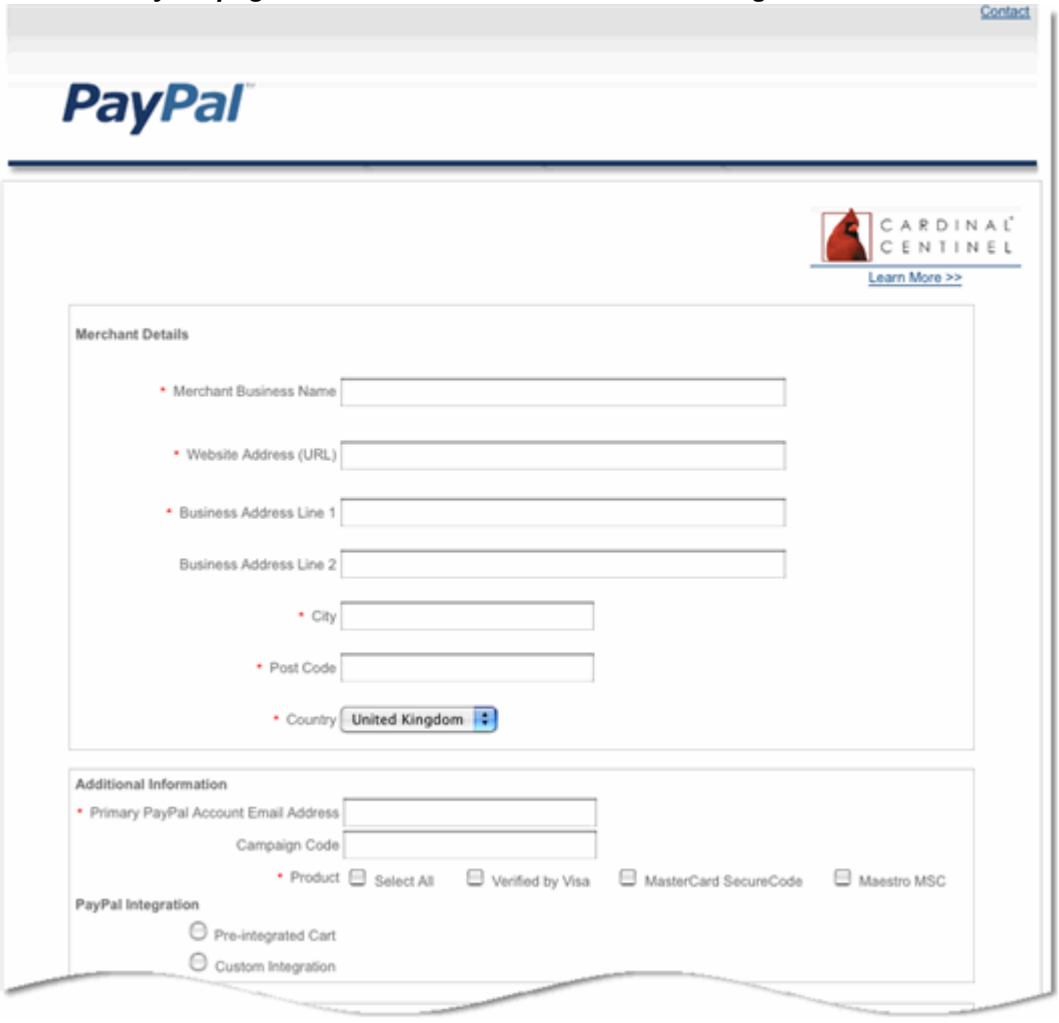
1. Register with Cardinal by filling in a simple form: http://www.paypal-business.co.uk/3Dsecure.asp.

   After you have registered, Cardinal Commerce acknowledges your 3-D Secure registration by sending you an email and welcome pack, which includes information about next steps and links for downloading their documentation and software.

2. Download and install the Cardinal Centinel Thin Client software. Refer to the Cardinal documentation for installation instructions.

NOTE: Cardinal Commerce will be available to schedule an integration meeting with you and will support you with your Cardinal Centinel Integration requirements.

FIGURE 9.1 PayPal page for Cardinal Commerce merchant registration



Transaction Processing

Integrating Cardinal Centinel and 3-D Secure with your PayPal transaction processing is fairly straightforward. You need to set up a web page that can handle a return call from the card's issuer, insert three additional requests into your application before the direct payment request, and add 3-D Secure payer authentication fields to whichever of the following requests are used in your integration:

- Authorization (`TRXTYPE=A&TENDER=C`)

- Sale (`TRXTYPE=S&TENDER=C`)

NOTE: Refer to the Cardinal documentation for the most recent Cardinal Centinel information. Cardinal requests, responses, and processes are provided for you in this document as a convenience but might not reflect the most current Cardinal information.

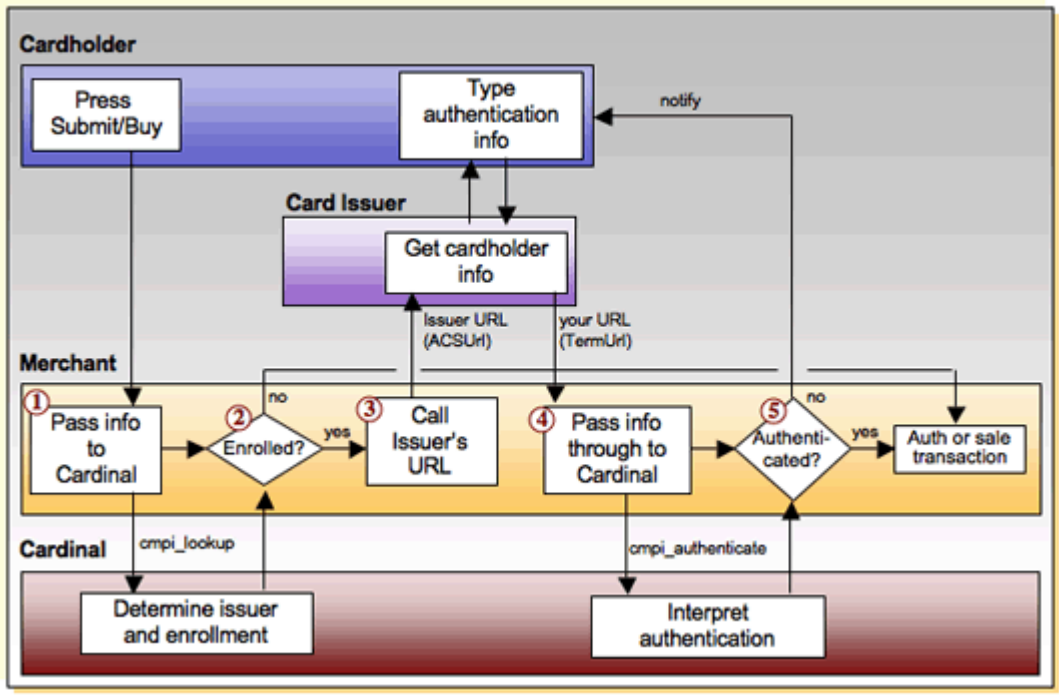
URL to Handle Issuer's Response

You must establish a page on your site whose URL can receive a form POST from the card's issuer that contains two fields, `PaRes` and `MD`. The page must then request `cmpi_authenticate` as described in the next section. Your page's URL is referred to as `TermURL`.

Transaction Flow

NOTE: The steps in this section are explained in the Cardinal *Thin Client Integration Guide Payer Authentication* document; refer there for the most current information. This summary is provided for you as a convenience.

FIGURE 9.2 Transaction flow with numbered steps



To create a 3-D Secure transaction using Website Payments Pro and Cardinal Centinel, do the following before executing the direct payment request:

1. Call Cardinal Centinel with the `cmpi_lookup` request, passing your merchant and transaction information.

   See "cmpi_lookup API" for the complete list of required fields.

2. The `cmpi_lookup` request responds with several fields; see "cmpi_lookup API" for details about these fields:

   – Error information: Evaluate and take appropriate action if nonzero. Refer to the *Thin Client Integration Guide* for error codes, descriptions, explanations, and recommended actions.
   – Cardinal transaction information that you will pass to other requests: `TransactionId`, `Enrolled`, `Payload`, and `EciFlag`.
   – `ACSUrl`: If `Enrolled`=Y, this contains the URL for the card issuer's (bank's) authentication site.

   Evaluate `Enrolled` and `ACSUrl`:
   – If cardholder is not enrolled (`Enrolled` is N) or if the Authentication service is unavailable (`ACSUrl` is U or N), continue with Step 5 below.
   – If cardholder is enrolled, continue with the next step.

3. Using an HTTP form POST, pass the cardholder to the URL (`ACSUrl`) returned by `cmpi_lookup`, which is the card issuer's authentication URL. Pass several fields to this request:

   – Transaction information from `cmpi_lookup`.
   – `MD` field optionally containing arbitrary merchant data; set to blank if not used.
   – `TermUrl`: The URL of the page you set up to handle the issuer's return call.

   See "Issuer Authentication Fields" for the complete list of required fields.

   Cardholders attempt to authenticate themselves at the issuer's URL. The completion of the attempt returns a response to your application by using HTTP Form POST to call the URL you specified in `TermUrl`. The response contains the `PaRes`.

4. Call `cmpi_authenticate`, passing `PaRes` as `PAResPayLoad`. This interprets the payload to determine whether the cardholder passed the authentication process with the card's issuer.

   See "cmpi_authenticate API" for the complete list of required fields.

5. The `cmpi_authenticate` request returns several fields:

   – Error information: Evaluate and take appropriate action if nonzero. Refer to the *Thin Client Integration Guide* for error codes, descriptions, explanations, and recommended actions.
   – Authentication information in `PAResStatus`, `SignatureVerification`, `Cavv`, `EciFlag`, and `Xid`.

     See "cmpi_authenticate API" for details about the returned fields.

   Evaluate `SignatureVerification`:

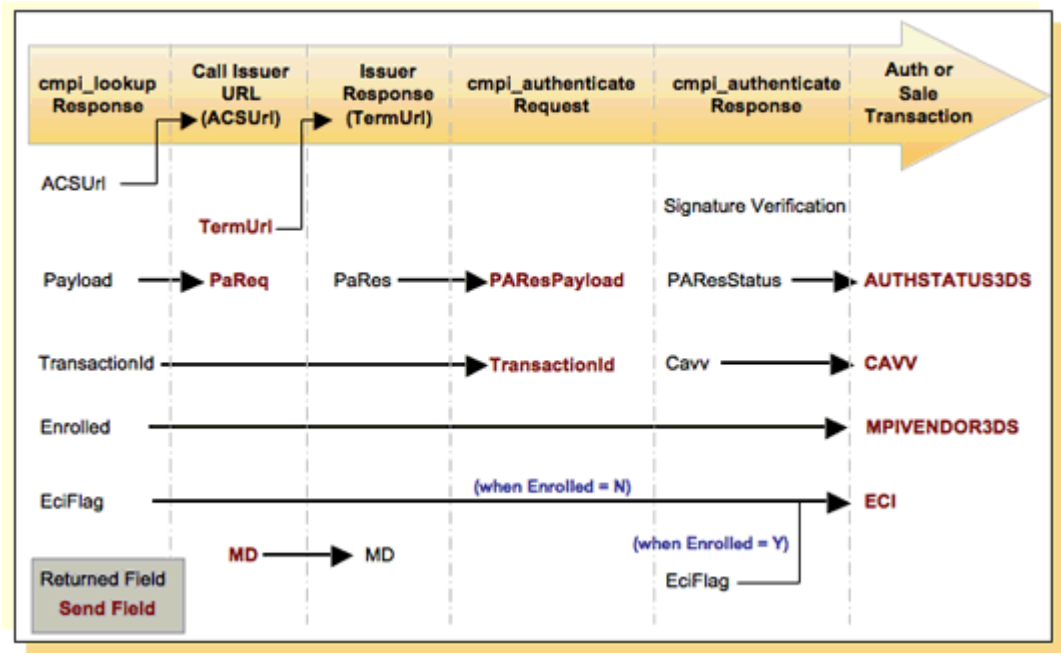
– If the signature is not verified, return an authentication-failed message to the cardholder and stop processing the transaction.
– If the signature is verified, continue with the next section.

3-D Secure Fields for Direct Payment Transaction Requests

If the cardholder is authenticated, or if not authenticated for valid reasons such as the authentication service being unavailable or the cardholder not being enrolled, execute the direct payment transaction request with the following additional fields:

Field	Description
AUTHSTATUS3DS	Set this to the returned PAResStatus value.
MPIVENDOR3DS	Set to the Enrolled value from Step 2.
CAVV	Set to the returned Cavv value.
ECI	Set to the returned EciFlag value.
XID	Set to the returned Xid value.

FIGURE 9.3 Flow of field values among requests and responses. Not all fields are shown.



EXAMPLE 9.1 Example direct payment transaction request

```
TRXTYPE=S&TENDER=C&USER=SuperMerchant&PWD=SuperUserPassword&PARTNER=
PayPalUK&ACCT=5105105105105100&EXPDATE=1209&AMT=99.06&COMMENT1=Reser
```

```
vation&FIRSTNAME=John&LASTNAME=Jones&STREET=123 Main
St.&CITY=London&ZIP=123451234&COUNTRY=GB&CVV2=123&CUSTIP=0.0.0.0&ECI
=5&CAVV[28]=OTJlMzViODhiOTllMjBhYmVkMGU=&AuthStatus3ds=Y&MPIVendor3d
s=Cardinal
```

Website Set-Up

Cardinal and/or 3-D Secure require that you add specific elements to your web pages. These include:

- Integrate the authentication window to allow for consistent site branding during the authentication process.
- Display the Visa and MasterCard "Learn More" logos on your home and check-out pages.
- Provide text and logo on the check-out page in which you collect payment information. Notify the cardholder that they may be required to provide their authentication password.
- Notify the cardholder of authentication results.

Refer to the Cardinal *Thin Client Integration Guide* for details.

Examples

The following examples outline the transaction process for three basic situations.

Example 1: Successful 3-D Secure Authentication

In this example, the cardholder's issuer uses 3-D Secure and the authentication is successful:

1. Construct your message for `cmpi_lookup`.
2. Review the response from `cmpi_lookup`. Ensure that all of the following are true:
   - `ErrorNo`=0
   - `Enrolled`=Y
   - `ACSUrl` has content; for example: <ACSUrl>https://www.somewebsite.com/acs</ACSUrl>
3. Using HTTP Form POST, redirect the cardholder to the issuer's URL that was provided in `ACSUrl`. Ensure that the `PaReq` has the data from the field `PayLoad`, from the `cmpi_lookup` response.
4. Send the response (redirect) from the issuer's HTTP Form POST to Cardinal using the `cmpi_authenticate` message to determine how to proceed with the transaction.
5. The `cmpi_authenticate` response will specify how to proceed. To continue with authorisation, the following must be true:

- `SignatureVerification`=Y
- `PAResStatus`=Y, U, or A

6. Authorise as normal, with the additional fields described in 3-D Secure Fields for Direct Payment Transaction Requests.

Example 2: 3-D Secure with Unsuccessful Authentication

In this example, the cardholder's issuer uses 3-D Secure and the authentication is **not** successful:

1. Construct your message for `cmpi_lookup`.
2. Review the response from `cmpi_lookup`. Ensure that all of the following are true:
   - `ErrorNo` is 0
   - `Enrolled` is Y
   - `ACSUrl` has content; for example: <ACSUrl>https://www.somewebsite.com/acs</ACSUrl>
3. Using HTTP Form POST, redirect the cardholder to the issuer's URL that was provided in `ACSUrl`. Ensure that the `PaReq` has the data from the field `PayLoad`, from the `cmpi_lookup` response.
4. Send the response (redirect) from the issuer's HTTP Form POST to Cardinal using the `cmpi_authenticate` message to determine how to proceed with the transaction.
5. The `cmpi_authenticate` response determines how to proceed. In this example, when authentication fails, the following are true:
   - `SignatureVerification`=Y
   - `PAResStatus`=N
6. Notify the cardholder that the transaction is declined.

Example 3: Card Issuer Not Using 3-D Secure

In this example, the card's issuer does not use 3-D Secure:

1. Construct message for `cmpi_lookup`.
2. Review the response from `cmpi_lookup`. Ensure that:
   - `ErrorNo`=0
   - `Enrolled`=N or U
3. Authorise as normal, with the additional fields described in 3-D Secure Fields for Direct Payment Transaction Requests.

Example 4: Merchant Not Using 3-D Secure

In this example, the merchant does not authenticate a Maestro transaction using 3-D Secure before executing a direct-payment transaction request:

- Through 31 December, 2009, a direct payment request continues to return `RESULT=0`.
- Beginning on 1 January, 2010, a direct payment request will be declined with `RESULT=7`.

Testing

For 3-D Secure, you cannot use PayPal's Test Mode for testing. You must use Cardinal's test procedures.

Refer to the Cardinal documentation.

cmpi_lookup API

The `cmpi_lookup` request is a Cardinal Centinel request. This section lists required fields and responses as a convenience for you. Refer to the Cardinal *Thin Client Integration Guide Payer Authentication* document for details and the most current information.

cmpi_lookup Request

TABLE 9.1 cmpi_lookup Request Fields

Field	Description
`MsgType`	*(Required)* Must be `cmpi_lookup`.
`Version`	*(Required)* Must be 1.7.
`ProcessorId`	*(Required)* Your processor identification code, assigned by Cardinal when you register.
`MerchantId`	*(Required)* Your merchant identification code as assigned by Cardinal.
`TransactionPwd`	*(Required)* Your Cardinal password as you configured it at the Cardinal site.
`TransactionType`	*(Required)* Must be C.
`Amount`	*(Required)* The value of the transaction in cents or pence with no decimal point. For example, £100 is specified as 10000.
`CurrencyCode`	*(Required)* The 3-digit numeric ISO 4217 currency code for the sale amount. For example, GBP = 826, EUR = 978.

Field	Description
`CardNumber`	*(Required)* The debit or credit card number, up to 19 digits with no nonnumeric characters.
`CardExpMonth`	*(Required)* The card's expiration month, formatted as MM.
`CardExpYear`	*(Required)* The card's expiration year, formatted as YYYY.
`OrderNumber`	*(Required)* Your order number or transaction identifier. Limited to 50 characters.
various additional fields	*(Optional)* Cardinal allows several additional optional fields, which you can choose to use. Refer to the Cardinal documentation for details.

cmpi_lookup Response

TABLE 9.2 cmpi_lookup Response Fields

Field	Description
`ErrorNo`	Error number. 0 indicates no error.
`ErrDesc`	Empty if there is no error, otherwise, describes the error.
`TransactionId`	Centinel transaction identifier. Identifies the transaction within Centinel.
`Enrolled`	Status of authentication eligibility. If not Y, then the cardholder is *not* eligible for authentication. Possible values are: • Y: Enrolled • N: Not enrolled • U: Cardholder authentication unavailable.
`ACSUrl`	If Enrolled=Y, this contains the URL to which your application must next send the cardholder to complete authentication.
`Payload`	If Enrolled=Y, this contains the encoded transaction details; otherwise, this field is empty.
`EciFlag`	The Electronic Commerce Indicator (ECI). **MasterCard:** • 01: Merchant Liability • 02: Issuer Liability **Visa:** • 05: Issuer Liability • 06: Issuer Liability • 07: Merchant Liability

Issuer Authentication Fields

The call to the card issuer's site is explained in the Cardinal *Thin Client Integration Guide Payer Authentication.* document. This section lists required fields and responses as a convenience.

Issuer Authentication Request

Specify the following fields when you call the card issuer's URL that you received from `cmpi_lookup` in `ACSUrl`.

TABLE 9.3 Issuer Authentication Request Fields

Field	Description
`PaReq`	*(Required)* Content of the `Payload` field from `cmpi_lookup`.
`TermUrl`	*(Required)* Your URL for handling and processing the response from the ACSUrl.
`MD`	*(Required)* Merchant's session tracker. Set to blank if not used.

Issuer Authentication Response

When the issuer has completed its authentication processing, it calls the URL that you provided to it in `TermURL`. The issuer returns the following fields.

TABLE 9.4 Issuer Authentication Response Fields

Field	Description
`PaRes`	Authentication information to pass to `cmpi_authenticate`.
`MD`	Copy of `MD` sent by merchant.

cmpi_authenticate API

The `cmpi_authenticate` request is a Cardinal Centinel request. This section lists required fields as a convenience for you. Refer to the Cardinal *Thin Client Integration Guide Payer Authentication* document for details and the most current information.

cmpi_authenticate Request

TABLE 9.5 cmpi_authenticate Request Fields

Field	Description
MsgType	*(Required)* Must be cmpi_authenticate.
Version	*(Required)* Must be 1.7.
ProcessorId	*(Required)* Your Processor identification code as assigned by Cardinal.
MerchantId	*(Required)* Your merchant identification code as assigned by Cardinal.
TransactionPwd	*(Required)* Your Cardinal password as you configured it at the Cardinal site.
TransactionType	*(Required)* Must be C.
TransactionId	*(Required)* The transaction identifier returned from cmpi_lookup.
PAResPayload	*(Required)* PaRes provided in the package returned after the call to the card's issuer.

cmpi_authenticate Response

TABLE 9.6 cmpi_authenticate Response Fields

Field	Description
ErrorNo	Error number. 0 indicates no error; 1140 indicates that the cardholder pressed "Back."
ErrDesc	Empty if there is no error, otherwise, describes the error.
PAResStatus	The outcome of the issuer's authentication. Possible values are: • Y: Successful; merchant is protected. • N: Failed; no protection. • U: Unable to complete; no protection. • A: Successful; merchant is protected.
Cavv	A random sequence of characters; this is the encoded authentication.
SignatureVerification	Status of authentication eligibility. If not Y, then the cardholder is *not* eligible for authentication. Possible values are: • Y: Good • N: Bad

Field	Description
`EciFlag`	The Electronic Commerce Indicator (ECI). **MasterCard:** • 01: Merchant Liability • 02: Issuer Liability **Visa:** • 05: Issuer Liability • 06: Issuer Liability • 07: Merchant Liability
`Xid`	Transaction identifier from authentication.

A Verbosity: Viewing Processor-Specific Transaction Results

Transaction results (especially values for declines and error conditions) returned by the PayPal processor vary in detail level and in format. The VERBOSITY parameter enables you to control the kind and level of information you want returned.

By default, VERBOSITY is set to LOW. A LOW setting causes the server to normalise the transaction result values. Normalising the values limits them to a standardised set of values and simplifies the process of integrating Website Payments Pro.

By setting VERBOSITY to MEDIUM, you can view PayPal's raw response values. This setting is more "verbose" than the LOW setting in that it returns more detailed, processor-specific information.

Supported Verbosity Settings

PayPal supports the following VERBOSITY settings.

- LOW: This is the default setting for Website Payments Pro accounts. The following values are returned: {RESULT, PNREF, RESPMSG, AUTHCODE, AVSADDR, AVSZIP, CVV2MATCH, IAVS, CARDSECURE}
- MEDIUM: All of the values returned for a LOW setting, plus the following values:

NOTE: For information on interpreting the responses returned by the processor for the MEDIUM VERBOSITY setting, contact your processor directly.

TABLE A.1 Verbosity settings

Field Name	Type	Length	Description
HOSTCODE	char	7	Response code returned by the PayPal processor. This value is not normalised.
RESPTEXT	char	17	Text corresponding to the response code returned by the PayPal processor. This text is not normalised.
PROCAVS	char	1	AVS response from the PayPal processor
PROCCVV2	char	1	CVV2 response from the PayPal processor
PROCCARDSECURE	char	1	VPAS/SPA response from the PayPal processor.
ADDLMSGS	char	Up to 1048 characters. Typically 50 characters.	Additional error message that indicates that the merchant used a feature that is disabled.

***TABLE A.1 Verbosity settings** (Continued)*

Field Name	Type	Length	Description
TRANSSTATE	Integer	10	State of the transaction. The values are: 0 = General succeed state 1 = General error state 3 = Authorisation approved 6 = Settlement pending (transaction is scheduled to be settled) 7 =Settlement in progress (transaction involved in a currently ongoing settlement) 8 = Settled successfully 9 = Authorisation captured (once an authorisation type transaction is captured, its TRANSSTATE becomes 9) 10 = Capture failed (an error occurred while trying to capture an authorisation because the transaction was already captured) 11 = Failed to settle (transactions fail settlement usually because of problems with the processor or because the card type is not set up with the processor) 1 2= Unsettled transaction because of incorrect account information 14 = For various reasons, the batch containing this transaction failed settlement 15 = Settlement incomplete due to a chargeback. 106 = Unknown Status Transaction - Transactions not settled. 206 = Transactions on hold pending customer intervention.
DATE_TO_SETTLE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only before settlement has started.
BATCHID	Integer	10	Value available only after settlement has assigned a Batch ID.
SETTLE_DATE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only after settlement has completed.

Table A.2 shows the increments that are possible on basic TRANSSTATE values.

TABLE A.2 TRANSSTATE increments

Increment	Meaning
+100	No client acknowledgment (ACK) is received (=status 0 in V2), for example, 106 is TRANSSTATE 6. Transactions in this range do not settle. For transactions in TRANSSTATE 106, use Auto Resettle in PayPal Manager's Transaction Terminal to submit them for settlement or void them using a manual Void. See PayPal Manager Online Help for details on using PayPal Manager.
+200	The host process never receives ACK from the transaction broker (or backend payment server). A transaction with a TRANSSTATE of +200 is basically in limbo and will not be settled.
+1000	Voided transactions. Any TRANSSTATE of +1000 (for example, 1006) means the transaction was settle pending. However, it was voided either through the API, PayPal Manager or PayPal Customer Service.

Changing the Verbosity Setting

Setting the Default Verbosity Level for All Transactions

Contact PayPal Customer Service to set your account's VERBOSITY setting to LOW or MEDIUM for all transaction requests.

Setting the Verbosity Level on a Per-Transaction Basis

To specify a setting for Verbosity that differs from your account's current setting, include the VERBOSITY=<value> name-value pair in the transaction request, where <value> is LOW or MEDIUM.

B ISO Country Codes

The following International Standards Organisation (ISO) country codes are used when filling the order fields BILLTOCOUNTRY and POSTTOCOUNTRY.

TABLE B.1 Country codes

Country	Code
ALBANIA	AL
ALGERIA	DZ
AMERICAN SAMOA	AS
ANDORRA	AD
ANGUILLA	AI
ANTIGUA AND BARBUDA	AG
ARGENTINA	AR
ARMENIA	AM
ARUBA	AW
AUSTRALIA	AU
AUSTRIA	AT
AZERBAIJAN	AZ
BAHAMAS	BS
BAHRAIN	BH
BANGLADESH	BD
BARBADOS	BB
BELARUS	BY
BELGIUM	BE
BELIZE	BZ
BENIN	BJ
BERMUDA	BM

***TABLE B.1 Country codes** (Continued)*

Country	Code
BOLIVIA	BO
BOSNIA AND HERZEGOVINA	BA
BOTSWANA	BW
BRAZIL	BR
BRITISH VIRGIN ISLANDS	VG
BRUNEI	BN
BULGARIA	BG
BURKINA FASO	BF
CAMBODIA	KH
CAMEROON	CM
CANADA	CA
CAPE VERDE	CV
CAYMAN ISLANDS	KY
CHILE	CL
CHINA	CN
COLOMBIA	CO
COOK ISLANDS	CK
COSTA RICA	CR
CÔTE D'IVOIRE	CI
CROATIA	HR
CYPRUS	CY
CZECH REPUBLIC	CZ
DENMARK	DK
DJIBOUTI	DJ
DOMINICA	DM
DOMINICAN REPUBLIC	DO
EAST TIMOR	TP
ECUADOR	EC

***TABLE B.1 Country codes** (Continued)*

Country	Code
EGYPT	EG
EL SALVADOR	SV
ESTONIA	EE
FIJI	FJ
FINLAND	FI
FRANCE	FR
FRENCH GUIANA	GF
FRENCH POLYNESIA	PF
GABON	GA
GEORGIA	GE
GERMANY	DE
GHANA	GH
GIBRALTAR	GI
GREECE	GR
GRENADA	GD
GUADELOUPE	GP
GUAM	GU
GUATEMALA	GT
GUINEA	GN
GUYANA	GY
HAITI	HT
HONDURAS	HN
HONG KONG	HK
HUNGARY	HU
ICELAND	IS
INDIA	IN
INDONESIA	ID
IRELAND	IE

***TABLE B.1 Country codes** (Continued)*

Country	Code
ISRAEL	IL
ITALY	IT
JAMAICA	JM
JAPAN	JP
JORDAN	JO
KAZAKHSTAN	KZ
KENYA	KE
KUWAIT	KW
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA
LATVIA	LV
LEBANON	LB
LESOTHO	LS
LITHUANIA	LT
LUXEMBOURG	LU
MACAO	MO
MACEDONIA	MK
MADAGASCAR	MG
MALAYSIA	MY
MALDIVES	MV
MALI	ML
MALTA	MT
MARSHALL ISLANDS	MH
MARTINIQUE	MQ
MAURITIUS	MU
MEXICO	MX
MICRONESIA, FEDERATED STATES OF	FM
MOLDOVA	MD
MONGOLIA	MN

TABLE B.1 Country codes *(Continued)*

Country	Code
MONTSERRAT	MS
MOROCCO	MA
MOZAMBIQUE	MZ
NAMIBIA	NA
NEPAL	NP
NETHERLANDS	NL
NETHERLANDS ANTILLES	AN
NEW ZEALAND	NZ
NICARAGUA	NI
NORTHERN MARIANA ISLANDS	MP
NORWAY	NO
OMAN	OM
PAKISTAN	PK
PALAU	PW
PALESTINE	PS
PANAMA	PA
PAPUA NEW GUINEA	PG
PARAGUAY	PY
PERU	PE
PHILIPPINES, REPUBLIC OF	PH
POLAND	PL
PORTUGAL	PT
PUERTO RICO	PR
QATAR	QA
ROMANIA	RO
RUSSIAN FEDERATION	RU
RWANDA	RW
SAINT KITTS AND NEVIS	KN

***TABLE B.1 Country codes** (Continued)*

Country	Code
SAINT LUCIA	LC
SAINT VINCENT AND THE GRENDINES	VC
SAMOA	WS
SAUDI ARABIA	SA
SENEGAL	SN
SERBIA AND MONTENEGRO	CS
SEYCHELLES	SC
SINGAPORE	SG
SLOVAKIA	SK
SLOVENIA	SI
SOLOMON ISLANDS	SB
SOUTH AFRICA	ZA
SOUTH KOREA	KR
SPAIN	ES
SRI LANKA	LK
SWAZILAND	SZ
SWEDEN	SE
SWITZERLAND	CH
TAIWAN	TW
TANZANIA, UNITED REPUBLIC OF	TZ
THAILAND	TH
TOGO	TG
TONGA	TO
TRINIDAD AND TOBAGO	TT
TUNISIA	TN
TURKEY	TR
TURKMENISTAN	TM
TURKS AND CAICOS ISLANDS	TC

***TABLE B.1 Country codes** (Continued)*

Country	Code
UGANDA	UG
UKRAINE	UA
UNITED ARAB EMIRATES	AE
UNITED KINGDOM	GB
UNITED STATES OF AMERICA	US
URUGUAY	UY
UZBEKISTAN	UZ
VANUATU	VU
VENEZUELA	VE
VIETNAM	VN
VIRGIN ISLANDS, U.S.	VI
YEMEN ARAB REPUBLIC	YE
ZAMBIA	ZM