PayPal™

Payflow 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: September 2007

Payflow Pro Developer's Guide

Document Number: 200010.en_US-200709

Contents

Preface

Payflow Pro is a high performance TCP/IP-based Internet payment solution. Payflow Pro is pre-integrated with leading e-commerce solutions and is also available as a downloadable software development kit (SDK).

Intended Audience

This guide assumes that its readers:

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

Organization of This Document

This document is organized as follows:

- Chapter 1, "Introduction," describes the Payflow Pro internet payment solution.
- Chapter 2, "Installing and Configuring the Payflow APIs," shows a typical Payflow installation procedure for Windows NT and UNIX.
- Chapter 3, "Performing Credit Card Transactions," discusses credit card transaction syntax and parameters and describes how to perform transactions.
- Chapter 4, "Responses to Credit Card Transaction Requests," describes the responses to credit card transaction requests.
- Chapter 5, "Testing Payflow Pro Credit Card Transactions," describes how to test your Payflow Pro integration for credit card transactions.
- Chapter 6, "Activating Your Payflow Pro Account," specifies the steps you follow when you are ready to accept live transactions with Payflow.
- Appendix A, "Processors Requiring Additional Transaction Parameters," lists processors and their processor-specific parameters.
- Appendix B, "Verbosity: Viewing Processor-Specific Transaction Results," describes how you can use the Payflow Verbosity parameter to control the kind and level of information you want returned in a transaction response.
- Appendix C, "Additional Reporting Parameters," details the parameters that can be passed to the server for reporting purposes.
- Appendix D, "XMLPay," briefly describes XMLPay and tells where you may obtain a copy of *Payflow Pro XMLPay Developer's Guide*.

Where to Go for More Information

PayPal Manager online help describes the use of PayPal Manager—the web-based administration tool that you use to process transactions manually, issue credits, and generate reports.

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 gateway-ausupport@paypal.com.

Revision History

Revision history for *Payflow Pro Developer's Guide.*

TABLE P.1 Revision History

Date	Description
September 2007	Adapted for Australia.

1 Introduction

Payflow Pro is a high performance TCP/IP-based internet payment solution. It is pre-integrated with leading e-commerce solutions and is also available as a downloadable software development kit (Payflow SDK).

About Payflow Pro

Payflow Pro resides on your computer system. It available from the PayPal Manager Downloads page as a .NET or Java library, or you can build your own API by posting directly to the Payflow servers via HTTPS.

Payflow Pro is multi-threaded and allows multiple concurrent transactions from a single client. It can be integrated as a web-based or a non-web-based application.

Host Addresses

Unless you are using a V3 software development kit (SDK), use the new HOSTADDRESS values:

- For live transactions, use **payflowpro.verisign.com**
- For testing purposes, use **pilot-payflowpro.verisign.com**

Otherwise (you are using a V3 SDK in the process of being phased out), continue to use the host addresses below:

- For live transactions, use **payflow.verisign.com**
- For testing purposes, use **test-payflow.verisign.com**

How Payflow Pro Works

Payflow Pro uses a client/server architecture to transfer transaction data from you to the processing networks, and then returns the authorisation results to you. Payflow Pro can process real-time credit card transactions and other transaction types to most of the financial processing centres in the United States and Australia.

1. The Payflow client encrypts each transaction request using the latest Secure Sockets Layer (SSL) encryption and establishes a secure link with the Payflow server over the internet.
2. The Payflow server, a multi-threaded processing environment, receives the request and transmits it (over a secure private network) to the appropriate financial processing network for real-time payment authorisation.

3. The response (approved/declined, and so on) is received from the financial network and is returned in the same session to the Payflow client.
4. The Payflow client completes each transaction session by transparently sending a transaction receipt to the server before disconnecting the session.

The entire process is a real-time synchronous transaction. Once connected, the transaction is immediately processed and the answer returned in about three seconds. Processing transactions through the Payflow service does not affect or define the time periods of authorisations, nor does it influence the approval or denial of a transaction by the issuer.

When integrating with Payflow Pro, you need only be concerned with passing all the required data for transaction authorisation.

Payflow Pro Advantages

- **Configurable to any e-commerce application**. Payflow Pro is ideal for enterprise merchants who require complete customizability for a controlled buyer experience.
- Downloadable from PayPal Manager Downloads page, the Payflow SDK can be easily integrated into a customized e-commerce solution in a matter of hours.
- **Integration versatility.** Payflow Pro can be integrated as an application library or can be run using CGI scripts.

Supported Processing Platforms

Payflow Pro supports the following processing platforms:

American Express Asia Pacific (APA)

Citibank Singapore (CSIN)

First Data Resources International (FDI)

See Appendix A, "Processor Details," for more information.

Payflow Pro Recurring Billing Service

The Recurring Billing Service is a scheduled payment solution that enables you to automatically bill your customers at regular intervals—for example, a monthly fee of $42 for 36 months with an initial fee of $129.

You enroll separately for the Payflow Pro Recurring Billing Service. Using Payflow Pro to define and manage recurring transactions is described in *Payflow Pro – Recurring Billing Service User's Guide* and in PayPal Manager online help.

About Security

It is your responsibility to protect your passwords and other confidential data and to implement security safeguards on your website and in your organization, or to ensure that your hosting company or internal web operations team is implementing them on your behalf.

IMPORTANT: *To enable testing of Payflow Pro, PayPal provides sample transaction scripts that you customize with your Payflow Pro account information and password. Because the password is initially stored in the text of the program, it is vulnerable.*

Do not use the test scripts in your production environment. To minimize fraud, machine passwords should always be encrypted. You must write a program that encrypts and decrypts your Payflow Pro account password.

2 Installing and Configuring the Payflow APIs

The Payflow software development kit (SDK) is available either as a standalone client that you can integrate with your web store using CGI scripts or as a set of APIs for direct integration with your application.

This chapter provides instructions for downloading the SDK appropriate to your platform.

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 the Payflow application.

Step 1 Download the Payflow SDK

From the **Download** section of PayPal Manager, download the Payflow SDK appropriate for your platform.

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 Read the Readme.txt file

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

3 Performing Credit Card Transactions

This chapter describes performing credit card transactions.

Responses to transaction requests are described in Chapter 4, "Responses to Credit Card Transaction Requests."

In This Chapter

About Credit Card Processing

Credit card processing occurs in two steps — a real-time Authorisation and a capture (settlement) of the funds that were authorised. As discussed below, you perform these two steps either as a single transaction or as two transactions, depending on your business model.

For an Authorisation, the server sends the transaction information to a credit card processor who routes the transaction through the financial networks to the cardholder's issuing bank. The issuing bank checks whether the card is valid, evaluates whether sufficient credit exists, checks values such as card security codes (discussed below), and returns a response: Approval, Decline, Referral, or others.

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

NOTE: You cannot remove a hold on funds through the processing networks—you must contact the card issuing bank to lift a hold early.

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

Obtaining an Internet Merchant Account

To accept credit cards over the internet, you need a special account called an Internet Merchant Account. Your account provider or merchant (acquiring) bank works with a PayPal-supported credit card processor, such as First Data Resources International or American Express Asia Pacific. To use Payflow Pro to accept live credit cards, you must provide certain details about your account to PayPal during the "Go Live" part of the enrolment process.

NOTE: An Internet Merchant Account is a different type of merchant account than a merchant account used for face-to-face (in-person) retail transactions. It has additional risks associated with card-not-present (e-commerce) transactions. You need to obtain an Internet Merchant Account even if you already accept credit cards at your location.

To apply for an Internet Merchant Account, contact your merchant (acquiring) bank.

Planning Your Payflow Pro Integration

In designing your Payflow Pro integration, you should evaluate the following:

- Whether to use a one-step or two-step transaction process. One-step: Submit a Sale transaction, which performs the Authorisation and (if successful) then flags the transaction for settlement. Two-step: Perform an Authorisation-only transaction and then later perform a Delayed Capture transaction. The Delayed Capture transaction can be for the same amount as the original transaction or for a lower amount. (In the case of a split shipment, you can perform a Delayed Capture transaction for the initial shipment and a reference transaction for the final payment. These transaction types, plus the details of performing a Delayed Capture for an amount higher than the original, are described in "Submitting Authorisation/Delayed Capture Transactions" on page 25.)

  According to card association rules, most physical goods merchants should use a two-step process, since settlement should occur when the goods are fulfilled or shipped. A two-step process is also useful if you want to evaluate information in the response, such as whether the issuer verifies the billing address, and so on. Electronic goods merchants, who fulfill the order immediately, can use the one-step process. Check with your Internet Merchant Account provider for suggestions on the best method for you.

- Whether or how to use risk management tools such as card security code.

  Card security code refers to a 3- or 4-digit number that appears on the back of most credit cards. On American Express, the number appears above and to the right of the embossed card number. Card security code is known by other names, such as CVV2, depending on

the type of card. If card security code data is submitted, the issuer can notify you whether the number matches the number assigned to the card. Card security code is described on page 37.

It may also be possible to implement additional safeguards yourself or to use a fraud service. You might want to discuss risk management with your Internet Merchant Account provider.

- Store information in your local database or use PayPal Manager reports to manage the data. You may want to store shipping 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 reports to your orders/customers or to report on other information about the transaction.

- If or how you want to integrate with other systems, such as order fulfillment, customer service, and so on. You may wish to connect these systems directly to Payflow 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.
- You may want to discuss, with your Internet Merchant Acquirer, practices that help you to obtain the most advantageous rates.

Complying With the E-commerce Indicator (ECI)

Some processors support a software flag called E-commerce Indicator (ECI) that indicates that the associated transaction is an internet transaction. Payflow Pro complies with ECI basic requirements for all supported processors.

If you use the Buyer Authentication Service, then the ECI values reflects the Authentication status. See *Payflow Pro Fraud Protection Service User's Guide*.

Handling Credit Card Type Information

The Payflow SDK does not check the credit card types that you are accepting. If a customer uses a card type that you are not signed up to accept, the Payflow SDK responds with RESULT code 23, "Invalid account number," or the processor returns a message that the customer is not signed up for the card type. For details on RESULT codes and response messages, see Chapter 4, "Responses to Credit Card Transaction Requests." Optionally, you can provide your customer with a list of the card types that you accept (in a drop-down list or menu, for example).

To accept additional credit card types, you must contact your acquiring bank (the merchant that holds your Internet Merchant Account) and ask them to add the card type to your account. Upon notification from your Acquirer that you can start accepting the card type, you must add

the card to your Payflow Pro account through PayPal Manager. See PayPal Manager online help for details.

Contents of a Transaction Request

Table 3-1 describes the connection parameters that you need to pass when submitting a transaction request to the Payments gateway. Pass them in the format and syntax required by the SDK and programming language that you are using. See your integration documentation for details.

TABLE 3.1 Connection parameters

Argument	Required	Description
HOSTADDRESS	Yes	PayPal's host name. For live transactions, use **payflowpro.verisign.com** For testing purposes, use **pilot-payflowpro.verisign.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. In the example, the ParmList is: `"TRXTYPE=S&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant&USER=SuperMerchant&PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&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 does a Sale transaction. "Parameters Used in Credit Card Transactions" on page 19 defines the parameters used to create credit card transactions. "Values Required by All Transaction Types" on page 23 lists the parameters required by each transaction type.
TIMEOUT	Yes	Time-out period for the transaction. The minimum recommended time-out value is 30 seconds. The PayPal client begins tracking from the time that it sends the transaction request to the PayPal 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 (“”).
- Quotation marks (“”) are not allowed within the body of the PARMLIST.
- Separate all name-value pairs in the PARMLIST using an ampersand (&).
- Set the VERBOSITY transaction parameter to MEDIUM (default is LOW) if you want the response to return more detailed information. For details on VERBOSITY, see Appendix B, “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.

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.

Parameters Used in Credit Card Transactions

All credit card processors accept the parameters listed in Table 3.2 (required and optional parameters are noted). “Values Required by All Transaction Types” on page 23 lists the parameters required for each transaction type.

NOTE: Some processors require yet additional parameters. See the following sections:

- Appendix A, “Processors Requiring Additional Transaction Parameters,” provides additional parameter requirements for non-PayPal processors.

- Appendix C, "Additional Reporting Parameters," provides a list of parameters that you can pass for reporting purposes.

TABLE 3.2 Credit-card transaction parameters

Parameter	Description	Required	Type	Max. Length
ACCT	Credit card or purchase card number. This value may not contain spaces, non-numeric characters, or dashes. For example, ACCT=5555555555554444	Yes[1]	Numeric	19
AMT	Amount (US Dollars) U.S. based currency. Specify the exact amount to the cent using a decimal point—use 34.00, not 34. Do not include comma separators—use 1199.95 not 1,199.95. Your Internet Merchant Account provider may stipulate a maximum amount.	Yes[1]	Numeric	10
AUTHCODE	AUTHCODE is returned only for approved Voice Authorisation transactions. AUTHCODE is the approval code obtained over the telephone from the processing network.	req'd for Voice Authorisation only.	Alpha-numeric	6
COMMENT1	Merchant-defined value for reporting and auditing purposes.	No	Alpha-numeric	128
COMMENT2	Merchant-defined value for reporting and auditing purposes.	No	Alpha-numeric	128
CURRENCY	One of the following three-character currency codes: • USD (US dollar) • EUR (Euro) • GBP (UK pound) • CAD (Canadian dollar) • JPY (Japanese Yen) • AUD (Australian dollar) **NOTE:** CURRENCY is applicable only to processors that support transaction-level currency. It is not applicable to Australian Payflow Pro merchants.	No	Alpha	3

TABLE 3.2 Credit-card transaction parameters *(Continued)*

Parameter	Description	Required	Type	Max. Length
CUSTREF	Merchant-defined identifier for reporting and auditing purposes. For example, you can set CUSTREF to the invoice number. You can use CUSTREF when performing Inquiry transactions. To ensure that you can always access the correct transaction when performing an Inquiry, you must provide a unique CUSTREF when submitting any transaction, including retries. See STARTTIME and ENDTIME.	No	Alpha-numeric	12
CVV2	A 3- or 4-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. See "Card Security Code Validation" on page 37.	No	Alpha-numeric	4
ENDTIME	Optional for Inquiry transactions when using CUSTREF to specify the transaction. ENDTIME specifies the end of the time period during which the transaction specified by the CUSTREF occurred. See STARTTIME. ENDTIME must be less than 30 days after STARTTIME. An inquiry cannot be performed across a date range greater than 30 days. If you set ENDTIME, and not STARTTIME, then STARTTIME is defaulted to 30 days before ENDTIME. If neither STARTTIME nor ENDTIME is specified, then the system searches the last 30 days. Format: **yyyymmddhhmmss**	No	Numeric	14
EXPDATE	Expiration date of the credit card in **mmyy** format. For example, 0308 represents March 2008.	Yes[1]	Numeric	4
NAME or FIRSTNAME	Account holder's name. This single field holds all of the person's name information.	No, but recom-mended	Alpha-numeric uppercase	30
ORIGID	The ID of the original transaction that is being referenced. This ID is returned by the PNREF parameter and appears as the Transaction ID in PayPal Manager reports. This value is case-sensitive.	Yes[1]	Alpha-numeric	12

TABLE 3.2 Credit-card transaction parameters *(Continued)*

Parameter	Description	Required	Type	Max. Length
PARTNER	The ID provided to you by the authorised PayPal Reseller who registered you for the Payflow Pro service. If you purchased your account directly from PayPal, use VSA. This value is case-sensitive.	Yes	Alpha-numeric	12
PWD	The 6- to 32-character password that you defined while registering for the account. This value is case-sensitive.	Yes	Alpha-numeric	32
STARTTIME	Optional for Inquiry transactions when using CUSTREF to specify the transaction. STARTTIME specifies the beginning of the time period during which the transaction specified by the CUSTREF occurred. See ENDTIME. If you set STARTTIME, and not ENDTIME, then ENDTIME is defaulted to 30 days after STARTTIME. If neither STARTTIME nor ENDTIME is specified, then the system searches the last 30 days. Format: **yyyymmddhhmmss**	No	Numeric	14
STREET	The cardholder's street address (number and street name).	No	Alpha-numeric	30
SWIPE	Used to pass the Track 1 or Track 2 data (the card's magnetic stripe information) for card-present transactions. Include either Track 1 or Track 2 data—not both. If Track 1 is physically damaged, the POS application can send Track 2 data instead. **NOTE:** The track data includes the disallowed = (equal sign) character. To enable you to use the data, the SWIPE parameter must include a length tag specifying the number of characters in the track data. For this reason, in addition to passing the track data, the POS application must count the characters in the track data and pass that number. Length tags are described in "Using Special Characters in Values" on page 19.	Required only for card-present transac-tions	Alpha-numeric	
TENDER	The tender type (method of payment). C = Credit card	Yes	Alpha	1

TABLE 3.2 Credit-card transaction parameters *(Continued)*

Parameter	Description	Required	Type	Max. Length
TRXTYPE	A single character indicating the type of transaction to perform. Values are: S = Sale transaction C = Credit A = Authorisation D = Delayed Capture V = Void F = Voice Authorisation I = Inquiry	Yes	Alpha	1
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. This value is case-sensitive.	Yes	Alpha-numeric	64
VENDOR	Your merchant login ID that you created when you registered for the Payflow Pro account. The examples in this document use VENDOR = SuperMerchant. This value is case sensitive.	Yes	Alpha-numeric	64
VERBOSITY	LOW or MEDIUM. LOW is the default setting—normalized values. MEDIUM returns the processor's raw response values. See Appendix B, "Verbosity: Viewing Processor-Specific Transaction Results."	No	Alpha	
ZIP	Account holder's 5- to 9-digit ZIP (postal) code. Do not use spaces, dashes, or non-numeric characters.	No	Alpha	9

1. Some transaction types do not require this parameter. See "Values Required by All Transaction Types" on page 23

Values Required by All Transaction Types

All transaction types require values for the following parameters:

TRXTYPE
TENDER
PARTNER
VENDOR

USER
PWD

Each transaction type has additional parameter requirements, as listed in the following sections. Transaction responses are described in Chapter 4, "Responses to Credit Card 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 fulfillment for their products or services. If your business does not provide immediate fulfillment, then credit card association rules recommend that you use an Authorisation and a Delayed Capture transaction. For details, see "Submitting Authorisation/Delayed Capture Transactions" on page 25. 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 "Submitting Authorisation/Delayed Capture Transactions" on page 25.

Additional Parameters for Sale Transactions

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

ACCT
AMT
EXPDATE

NOTE: The pinless debit tender type requires essentially the same parameters as a credit card transaction. In addition to the values required by all transactions, you must pass values for the ACCT and AMT parameters.

Typical Sale Transaction Parameter String

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

```
"TRXTYPE=S&TENDER=C&USER=SuperUser&PWD=SuperUserPassword&VENDOR=SuperUser
&PARTNER=PayPal&ACCT=5105105105105100&EXPDATE=1209&CVV2=123&AMT=99.00&
FNAME=Bill&LNAME=Smith&STREET=123 Main
St.&CITY=Anywhere&STATE=CA&ZIP=12345&COMMENT1=Reservation&INVNUM=1234567
890&PONUM=C12345&CVV2=567&VERBOSITY=MEDIUM"
```

Note that, besides the required parameters that you pass in a Sale transaction, this string includes other typical parameters. The COMMENT1 (and COMMENT2) fields help to track

transaction information. CVV2 is needed for card security code validation. For details on card security code, see the following sections:

- "Submitting Card-Present (SWIPE) Transactions" on page 36
- "Card Security Code Validation" on page 37

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.

A Delayed Capture (TRXTYPE=D) transaction is performed after an Authorisation to capture the original Authorisation amount. The 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 shipped to the buyer, most processing networks implement an Authorisation transaction followed by a Delayed Capture transaction.

When To Use Authorisation/Delayed Capture Transactions

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

NOTE: If you signed up for the PayPal processor with Fraud Protection Services, you must use delayed capture processing for all sale transactions.

If your business provides immediate fulfillment and you are not using the PayPal processor with Fraud Protection Services, you can use a simple Sale transaction instead. For details, see "Submitting Sale Transactions" on page 24. 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 "Submitting Authorisation/Delayed Capture Transactions" on page 25.

IMPORTANT: *Only one Delayed Capture transaction is allowed per Authorisation transaction.*

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.

```
"TRXTYPE=A&TENDER=C&USER=SuperUser&PWD=SuperUserPassword&VENDOR=SuperUser
&PARTNER=PayPal&ACCT=5105105105105100&EXPDATE=1209&CVV2=123&AMT=99.00&
FNAME=Bill&LNAME=Smith&STREET=123 Main
St.&CITY=Anywhere&STATE=CA&ZIP=12345&COMMENT1=Reservation&INVNUM=1234567
890&PONUM=C12345&CVV2=567&VERBOSITY=MEDIUM"
```

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 4, “Responses to Credit Card 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 the 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, EXPDATE, and SWIPE. These parameters retain their original values.)

ACCT	AMT	CITY	COMMENTt1
COMMENT2	COMPANYNAME	BILLTOCOUNTRY	CUSTCODE
CUSTIP	DL	DOB	DUTYAMT
EMAIL	EXPDATE	FIRSTNAME	FREIGHTAMT
INVNUM	LASTNAME	MIDDLENAME	PONUM
SHIPTOCITY	SHIPTOCOUNTRY	SHIPTOFIRSTNAME	SHIPTOLASTNAME
SHIPTOMIDDLENAME	SHIPTOSTATE	SHIPTOSTREET	SHIPTO ZIP
SS	STATE	Street	SWIPE
TAXAMT	TAXEXEMPT	PHONENUM	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 27.

EXAMPLE 3.1 Example Authorisation Transaction Parameter String

Issue Authorisation-only Transaction

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=PayPal
&VENDOR=SuperMerchant&USER=SuperMerchant&ACCT=5555555555554444&EXPDATE=0308
&AMT=123.00&COMMENT1=Second purchase
&COMMENT2=Low risk customer&INVNUM=123456789&STREET=5199 MAPLE&ZIP=94588"
```

EXAMPLE 3.2 Example Authorisation Response

(Response parameters are described in detail in Chapter 4, "Responses to Credit Card Transaction Requests")

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

Step 2 Perform the 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 Capture 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 3.3 Example Delayed Capture Transaction Parameter String

```
"TRXTYPE=D&TENDER=C&PWD=x1y2z3&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&ORIGID=VXYZ00887892"
```

EXAMPLE 3.4 Example Delayed Capture Response

```
RESULT=0&PNREF=VXYZ00895642&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N
```

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 shipment).

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 PayPal 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 Voice Authorisation Transactions

A Voice Authorisation (TRXTYPE=F) transaction is a transaction that is authorised over the telephone from the processing network.

When to Use a Voice Authorisation Transaction

Some transactions cannot be authorised over the internet (for example, high dollar amounts) and require manual authorisation. These transactions generate Result Code 13 and are called Referral transactions.

In these situations, you contact the customer service department of your merchant bank and provide the payment information as requested. If the transaction is approved, the bank provides you with a voice Authorisation code (AUTHCODE) for the transaction. You include this AUTHCODE as a parameter in a Voice Authorisation transaction.

Once a Voice Authorisation transaction has been approved, it is treated like a Sale transaction and is settled with no further action on your part.

Like Sale transactions, approved Voice Authorisation transactions can be voided before settlement occurs.

Required Voice Authorisation Transaction Parameters

To submit a Voice Authorisation, you need to pass the following parameters:

```
AUTHCODE
ACCT
EXPDATE
AMT
```

Voice Authorisation Parameter String

The following is an example Voice Authorisation transaction parameter string:

```
"TRXTYPE=F&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant&USER=SuperMerchant&
PWD=x1y2z3&AUTHCODE=AB34RT56&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00"
```

Submitting Credit Transactions

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

Required Credit Transaction Parameters

The required parameter data for a Credit transaction depends on the **Allow non-referenced credits** security setting for your Payflow Pro account. A *non-referenced* credit is a Credit transaction that does not use the credit card information from an existing transaction. Credit card information must be supplied. As an example, Sally Smith calls you on the telephone to cancel an order from your business. To refund her money, you credit her credit card by submitting a non-referenced Credit transaction.

NOTE: The PayPal processor does not support non-referenced credits.

Guidelines and parameter requirements for Credit transactions differ depending on whether or not non-referenced credits are allowed.

Non-Referenced Credits Not Allowed

When non-referenced credits are not allowed (the setting recommended by PayPal), then Credit transactions are permitted only against existing Sale, Delayed Capture, and Voice Authorisation transactions. To submit a Credit transaction when non-referenced credits are not allowed, 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 4, "Responses to Credit Card Transaction Requests.") If you do not specify an amount, then the amount of the original transaction is credited to the cardholder.

Non-Referenced Credits Allowed

When non-referenced credits are allowed, then Credit transactions are permitted in any amount up to the transaction limit for the credit card account that you specify. To submit a Credit transaction when non-referenced credits are not allowed, you must pass values for the following parameters:

```
ACCT
EXPDATE
AMT
```

IMPORTANT: *The default security setting for Payflow Pro accounts is **Allow non-referenced credits = No**, so sending the ORIGID is the preferred method for performing Credit transactions. Using the ACCT, EXPDATE, or AMT parameters for such accounts leads to Result code 117 (failed the security check). For information on setting the security settings, see PayPal Manager online help.*

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, EXPDATE, and SWIPE. These parameters retain their original values).

NOTE: These fields are not copied for referenced credits: TAXAMT, TAXEXEMPT, DUTYAMT, FREIGHTAMT, and (for American Express only) DESC4.

NOTE: For processors that use the RECURRING parameter: If the RECURRING parameter was set to Y for the original transaction, then the setting is ignored when forming the Credit transaction.

ACCT	AMT	CITY	COMMENT1
COMMENT2	COMPANYNAME	BILLTOCOUNTRY	CUSTCODE
CUSTIP	DL	DOB	EMAIL
EXPDATE	FIRSTNAME	INVNUM	LASTNAME
MIDDLENAME	PONUM	SHIPTOCITY	SHIPTOCOUNTRY
SHIPTOFIRSTNAME	SHIPTOLASTNAME	SHIPTOMIDDLENAME	SHIPTOSTATE
SHIPTOSTREET	SHIPTOZIP	SS	STATE
STREET	SWIPE	PHONENUM	ZIP

Credit Transaction Parameter Strings

This is an example Credit transaction string (non-referenced credits not allowed):

```
"TRXTYPE=C&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&PWD=x1y2z3&ORIGID=VPNE12564395"
```

This is an example Credit transaction string (non-referenced credits allowed):

```
"TRXTYPE=C&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308
&AMT=123.00"
```

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 void Delayed Capture, Sale, Credit, Authorisation, and Voice Authorisation transactions. You cannot void a Void transaction.
- 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 4, "Responses to Credit Card 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, EXPDATE, and SWIPE. These parameters retain their original values).

NOTE: For processors that use the RECURRING parameter: If the RECURRING parameter was set to Y for the original transaction, then the setting is ignored when forming the Void transaction.

ACCT	AMT	CITY	COMMENT1
COMMENT2	COMPANYNAME	BILLTOCOUNTRY	CUSTCODE
CUSTIP	DL	DOB	DUTYAMT
EMAIL	EXPDATE	FIRSTNAME	FREIGHTAMT
INVNUM	LASTNAME	MIDDLENAME	PONUM
SHIPTOCITY	SHIPTOCOUNTRY	SHIPTOFIRSTNAME	SHIPTOLASTNAME
SHIPTOMIDDLENAME	SHIPTOSTATE	SHIPTOSTREET	SHIPTOZIP
SS	STATE	STREET	SWIPE
TAXAMT	TAXEXEMPT	PHONENUM	ZIP

Example Void Transaction Parameter String

This is an example Void transaction parameter string:

```
"TRXTYPE=V&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&PWD=x1y2z3&ORIGID=VPNE12564395"
```

Submitting Inquiry Transactions

An Inquiry transaction (TRXTYPE=I) returns the result and status of a transaction.

When To Use an Inquiry Transaction

You perform an inquiry using a reference to an original transaction—either the PNREF value returned for the original transaction or the CUSTREF value that you specified for the original transaction.

While the amount of information returned in an Inquiry transaction depends upon the VERBOSITY setting, Inquiry responses mimic the verbosity level of the original transaction as much as possible. (For details on VERBOSITY, see Appendix B, "Verbosity: Viewing Processor-Specific Transaction Results.")

Required Parameters When Using the PNREF

To submit an Inquiry transaction when using the PNREF, 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 4, "Responses to Credit Card Transaction Requests.")

Inquiry Transaction Parameter String Using the PNREF

This is an example Inquiry transaction parameter string using the ORIGID parameter set to the PNREF value:

```
"TRXTYPE=I&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&PWD=x1y2z3&ORIGID=VPNE12564395"
```

Required Parameters When Using the CUSTREF

To submit an Inquiry transaction when using the PNREF, you must pass the following parameter:

```
CUSTREF
```

Optionally, specify the STARTTIME and ENDTIME parameters.

CAUTION! *If there are multiple transactions with a particular CUSTREF value, then the Inquiry transaction returns only the last transaction with the specified CUSTREF. So, to ensure that you can always access the correct transaction, you must use a unique CUSTREF when submitting any transaction, including retries.*

Inquiry Transaction Parameter String Using the CUSTREF

This is an example Inquiry transaction parameter string using the CUSTREF:

```
"TRXTYPE=I&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant
&USER=SuperMerchant&PWD=x1y2z3&CUSTREF=Inv00012345"
```

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 web site store 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 shipping 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. With the exception of dollar amount data, which triggers a filter if out of range, reference transactions are not screened by Fraud Protection Services filters.

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 the following transaction types to supply data for a new Sale or Authorisation transaction:

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

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

ACCTTYPE	STREET
MIDDLENAME	BILLTOCOUNTRY
LASTNAME	SWIPE

Example Reference Transaction

In this example, you authorise an amount of $100 for a shipment and charge $66 for the first partial shipment using a normal Delayed Capture transaction. You charge the $34 for the final part of the shipment using a reference transaction to draw credit card and shipping 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, for example:

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=PayPal&VENDOR=SuperMerchant&USER=Sup
erMerchant&ACCT=5555555555554444&EXPDATE=0308&AMT=100.00&INVNUM=123456789&S
TREET=5199 MAPLE&ZIP=94588"
```

Note the value of the PNREF in the response:

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&AVSZ
IP=N
```

Step 2 Capture the authorised funds for a partial shipment 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, for example:

```
"TRXTYPE=D&TENDER=C&PWD=x1y2z3&PARTNER=PayPal&VENDOR=SuperMerchant&USER=Sup
erMerchant&ORIGID=VXYZ01234567&AMT=66.00"

RESULT=0&PNREF=VXYZ01234568&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N
```

Step 3 Submit a new Sale transaction of $34 for the rest of the shipment

Once you have shipped the remainder of the product, you can collect the remaining $34 in a Sale transaction that uses the initial Authorisation as a reference transaction. (This is a Sale transaction because only one Delayed Capture transaction is allowed per Authorisation.) For example:

```
"TRXTYPE=S&TENDER=C&PWD=x1y2z3&PARTNER=PayPal&VENDOR=SuperMerchant&USER=Sup
erMerchant&ORIGID=VXYZ01234567&AMT=34.00"

RESULT=0&PNREF=VXYZ01234569&AUTHCODE=25TEST&AVSADDR=Y&AVSZIP=N
```

NOTE: In the case that your business model uses the Authorisation/Delayed Capture cycle for all transactions, you could have chosen to use an Authorisation/Delayed Capture to collect the $34 in this example. You would generate the Authorisation for the $34 using the initial Authorisation as a reference transaction.

Submitting Card-Present (SWIPE) Transactions

Payflow Pro supports card-present transactions (face-to-face purchases).

Follow these guidelines to take advantage of the lower card-present transaction rate:

- Contact your merchant account provider to ensure that they support card-present transactions.
- Contact PayPal Customer Service to request having your account set up properly for accepting and passing swipe data.
- If you plan to process card-present as well as card-not-present transactions, set up two separate Payflow Pro accounts. Request that one account be set up for card-present transactions, and use it solely for that purpose. Use the other for card-not-present transactions. Using the wrong account may result in downgrades.
- A Sale is the preferred method to use for card-present transactions. Consult with your acquiring bank for recommendations on other methods.

Supported Processing Platforms

PayPal is certified to submit card-present transactions for the following processing platforms:

American Express APA

Citibank Singapore (CSIN)

First Data Resources International (FDI)

Card-present Transaction Syntax

Use the SWIPE parameter to pass the Track 1 or Track 2 data (the card's magnetic stripe information). Include either Track 1 or Track 2 data—not both (up to 80 alphanumeric characters). If Track 1 is physically damaged, the POS application can send Track 2 data instead.

The track data includes the disallowed = (equal sign) character. To enable you to use the data, the SWIPE parameter must include a length tag specifying the number of characters in the track data. For this reason, in addition to passing the track data, the POS application must count the characters in the track data and pass that number. Length tags are described in "Using Special Characters in Values" on page 19. The length tag in the following example is **[40]**.

Do not include the ACCT or EXPDATE parameters in card-present transactions, as this data is included in the SWIPE value.

Example Card-present Transaction Parameter String

This is an example card-present transaction parameter string:

```
"TRXTYPE=S&TENDER=C&PARTNER=PayPal&USER=SuperMerchant&PWD=SuperMerchant&SWI
PE[40]=;4912000033330026=15121011000012345678?&AMT=21.00"
```

Card Security Code Validation

The card security code is a 3- or 4-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: Check with your acquiring bank to determine whether they support card security code validation.

This fraud prevention tool has various names, depending on the payment network. Visa calls it CVV2 and 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.

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

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 American Express, the 4-digit number (**1122** in the example) is printed on the front of the card, above and to the right of the embossed account number. Be sure to explain this to your customers.

Processing Platforms and Credit Cards Supporting Card Security Code

TABLE 3.4 Processing platforms supporting card security code

Processing Platform	American Express	JCB	Diners	Master Card	Visa
American Express APAC	X	—	—	—	—
Citibank Singapore (CSIN)	—	—	—	—	—
First Data Resources International (FDI)	X	X	X	X	X

Even though your processor may be certified for card security code, they may not be certified for all card types (for example, Visa CVV2 or MasterCard CVC2). The list will change as PayPal continues to enhance its service offering.

Card Security Code Results

If you submit the transaction request parameter for card security code (that is, the CVV2 parameter), the cardholder's bank returns a Yes/No response in the CVV2MATCH response parameter, as described in the first table below. Card security code results vary depending on your processing platform, as described in the next table.

TABLE 3.6 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.

TABLE 3.7 Card security code results

Processing Platform	Results
American Express APAC	Card security code mismatches cause a non-approved result (RESULT = 114). No CVV2MATCH value is returned.
First Data International	Transactions that have card security code mismatches can come back as an approved transaction (RESULT = 0). The match or mismatch information is indicated in the CVV2MATCH value. As with AVS, if the Authorisation was successful, you must make a decision based on the CVV2MATCH value whether or not to proceed with the order.

NOTE: Check with your acquiring bank to determine how they handle CVV2MATCH.

Example CVV2 Request Parameter String

This example request parameter string includes the CVV2 parameter:

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=PayPal&VENDOR=SuperMerchant&USER=Sup
erMerchant&&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00&CVV2=567"
```

EXAMPLE 3.1 Example CVV2MATCH Response

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

```
RESULT=0&PNREF=VXW412345678&RESPMSG=APPROVED&AUTHCODE=123456&CVV2MATCH=Y
```

4 Responses to Credit Card Transaction Requests

This chapter describes the contents of a response to a credit card transaction request.

When a transaction finishes, PayPal 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
&CVV2MATCH=Y
```

Contents of a Response to a Credit Card Transaction Request

All transaction responses include values for RESULT, PNREF, RESPMSG. A value for AUTHCODE is included for Voice Authorisation transactions. Table 4.1 describes the values returned in a response string.

TABLE 4.1 Transaction response values

Field	Description	Type	Length
PNREF	PayPal Reference ID, a unique number that identifies the transaction. PNREF is described in "PNREF Format" on page 42.	Alpha-numeric	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 43.	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	1
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 43.	Alpha-numeric	Variable

TABLE 4.1 Transaction response values*(Continued)*

Field	Description	Type	Length
AUTHCODE	Returned for Sale, Authorisation, and Voice Authorisation transactions. AUTHCODE is the approval code obtained over the telephone from the processing network. AUTHCODE is required when submitting a Force (**F**) transaction.	Alpha-numeric	6

PNREF Value

The PNREF is a unique transaction identification number issued by PayPal 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 PayPal Manager.

PNREF Format

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

- VADE0B248932
- 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 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 RESULT values, 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 4.2 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: • 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. All fields are case sensitive. • 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.verisign.com to payflowpro.verisign.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 recognize your merchant account information. Contact your bank account acquirer to resolve this problem.

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
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, expiration 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**
22	**Invalid ABA number**
23	**Invalid account number.** Check credit card number and re-submit.
24	**Invalid expiration 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. All fields are case sensitive.
27	**Insufficient partner permissions**
28	**Insufficient user permissions**
29	**Invalid XML document.** This could be caused by an unrecognized 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**

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
33	**Error in canceling 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**
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 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.

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
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**
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 to 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 Payflow Pro SDK client no longer supported.** Upgrade to the most recent version of the Payflow Pro client.
132	**Card has not been submitted for update**
133	**Data mismatch in HTTP retry request**

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
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**
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**

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
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: For information on firewall configuration, see Chapter 2, “Installing and Configuring the Payflow APIs.”

Details of the response message may vary slightly from that shown in the table, depending on your SDK integration.

TABLE 4.3 RESULT values for communications errors

RESULT	Description
-1	**Failed to connect to host**
-2	**Failed to resolve hostname**
-5	**Failed to initialize 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 initialize SSL certificate**
-23	**Host address not specified**
-24	**Invalid transaction type**
-25	**Failed to create a socket**
-26	**Failed to initialize socket layer**
-27	**Parameter list format error: invalid [ ] name length clause**
-28	**Parameter list format error: name**
-29	**Failed to initialize 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**

TABLE 4.3 RESULT values for communications errors*(Continued)*

RESULT	Description
- 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 initialization 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 initializing from message file: <Details of the error message>**
-113	**Unable to round and truncate the currency value simultaneously**

5 Testing Payflow Pro Credit Card Transactions

To test your application, direct all transactions to **pilot-payflowpro.verisign.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 storefront — 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.
- **Expiration 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

American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Diners Club	30569309025904
Diners Club	38520000023237
JCB	3530111333300000
JCB	3566002020360505
MasterCard	5555555555554444
MasterCard	5105105105105100
Visa	4111111111111111
Visa	4012888888881881

TABLE 5.1 Test credit card numbers

Visa	4222222222222 **NOTE:** Even though this number has a different character count than the other test numbers, it is the correct and functional number.

Result Code Responses

This section describes the result code responses that you receive.

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 lists PayPal result codes that are supported by this testing mechanism.

NOTE: For all Processors except FDI: Credit (**C**) and Force (**F**) transactions will always be approved regardless of dollar amount or card number.

TABLE 5.2 Result codes resulting from amount submitted

Amount	Result (RESPMSG)
$0 – $1000	0 (Approved)
$1001 – $2000	Certain amounts in this range will return specific PayPal result codes, and can be generated by adding $1000 to that result code. For example, for result 13 (Referral), submit the amount 1013. If the amount is in this range but does not correspond to a PayPal result code supported by this testing mechanism, result 12 (Declined) is returned.
$2001+	12 – Decline

Result Codes Returned Based on Transaction Amount

This table lists the result codes that you can generate using the amount of the transaction. To generate a specific code, submit an amount of 1000 plus the code number (for example, submit an amount of **1013** for a result code of **13**).

Alternative Methods for Generating Specific Result Codes

TABLE 5.3 Result codes supporting the amount control

Processing Platform	Result Codes Available for Testing
American Express APAC	0, 12, 13, 104, 1000
Citibank Singapore	0, 4, 5,12,13,23,24,104, 2000
First Data International	0, 3, 4, 5, 12, 13, 23, 24, 26, 30, 50, 99, 100, 102, 104, 1000

Table 5.4 shows another method for obtaining result codes. Non-zero result values from processors are not returned by the servers, and therefore cannot be simulated using the amount. In some cases, you may get certain results using the result code plus 1000 even though this table suggests another means of obtaining the result code.

TABLE 5.4 Obtaining result code

Result	Definition	How to test using Payflow Pro
0	Approved	Use an AMOUNT of $1000 or less Credit (**C**) and Force (**F**) transactions will always be approved regardless of dollar amount or card number
1	User authentication failed	Use an invalid PWD
2	Invalid tender	Use an invalid TENDER, such as G
3	Invalid transaction type	Use an invalid TRXTYPE, such as G
4	Invalid amount	Use an invalid AMOUNT, such as –1
5	Invalid merchant information	Use the AMOUNT 1005 - Applies only to the following processors: Global Payments East and Central, and American Express)
7	Field format error	Submit a Delayed Capture transaction with no ORIGID
12	Declined	Use the AMOUNT 1012 or an AMOUNT of 2001 or more
13	Referral	Use the AMOUNT 1013
19	Original transaction ID not found	Submit a Delayed Capture transaction with an invalid ORIGID
23	Invalid account number	Submit an invalid account number, for example, 000000000000000
24	Invalid expiration date	Submit an invalid expiration date, for example, 0298
25	Transaction type not mapped to this host (Processor)	Submit a transaction for a card or tender you are not currently set up to accept, for example, a Diners card if you aren't set up to accept Diners
29	Invalid XML document	Pass a bad XML document (XMLPay users only)
101	Time-out value too small	Set timeout value to 1

***TABLE 5.4 Obtaining result code**(Continued)*

Result	Definition	How to test using Payflow Pro
103	Error reading response from host (Processor)	Use the AMOUNT 1103
104	Timeout waiting for processor response	Use the AMOUNT 1104
105	Credit error	Attempt to credit an authorisation
108	Void error	Attempt to void a captured authorisation
111	Capture error	Capture an Authorisation transaction twice or attempt to capture a transaction that is not an Authorisation transaction
1000	Generic Host (Processor) Error	Use the AMOUNT 2000 - Does not apply to American Express processor

Testing Card Security Code

If you submit a value for the card security code, the cardholder's bank returns a Yes / No / Not Supported (Y / N / X) response on whether the value matches the number on file at the bank. Card security code is described in "Card Security Code Validation" on page 37.

NOTE: Some processors will decline (result code 12) a transaction if the card security code does not match without returning a `CVV2MATCH` value. Test the results and check with your processor to determine whether they support card security code checking.

For the testing server, the first three characters of the `CVV2` value determine the `CVV2MATCH` result, as shown here.

TABLE 5.5 Testing CVV2MATCH

CVV2 Value	CVV2MATCH Value
000	Null
001-300	Y
301-600	N
601 or higher	X

6 Activating Your Payflow Pro Account

When you are ready to activate your Payflow Pro account to begin submitting live transactions, follow these steps:

1. Log in to PayPal Manager at https://manager.paypal.com.
2. Click the **Click Here to Activate** button and follow the on-screen instructions.
3. Change the URL within your web or desktop application to point to the live PayPal payment servers. Change **pilot-payflowpro.paypal.com** to **payflowpro.paypal.com.**

   Even though the account is now active (live), you can test and process live transactions at the same time, depending on the URL used. For example, a development server can point to pilot-payflowpro.paypal.com while a production server points to payflowpro.paypal.com.

A Processor Details

Citibank Singapore

Contacting Citibank Singapore (CSIN)

Citibank N.A.
1 Temasek Avenue
#11-01 Millenia Tower
Singapore 039192

Supported Card Types

Payflow accounts processing through CSIN can accept the following card types:

- MasterCard
- JCB
- Visa

Supported Currencies

CSIN supports transaction processing in the following currencies:

- Australian Dollar (AUD), ISO code 36
- Singapore Dollar (SGD), ISO code 702
- US Dollar (USD), ISO code 840
- Hong Kong Dollar (HKD), ISO code 344
- Malaysian Ringgit (MYR), ISO code 458
- New Zealand Dollar (NZD), ISO code 554
- Thailand Baht (THB), ISO code 764
- Taiwan Dollar (TWD), ISO code 901
- Indian Rupee (INR), ISO code 356
- Japanese Yen (JPY), ISO code 392
- Great British Pound (GBP), ISO code 826
- EMEA Euro (EUR), ISO code 978

- Kuwaiti Dinar (KWD), ISO code 414
- South Korean Won (KRW), ISO code 410
- Philippines Peso (PHP), ISO code 608
- Canadian Dollar (CAD), ISO code 124
- South African Rand (ZAR), ISO code 710
- China Yuan Renminbi (CNY), ISO code 156
- United Arab Emirates Dirhams (AED), ISO code 784
- Swiss Franc (CHF), ISO code 756
- Swedish Krona (SEK), ISO code 752
- Norweigan Krona (NOK), ISO code 578
- Danish Krona (DKK), ISO code 208
- Icelandic Krona (ISK), ISO code 352
- Indonesian Rupiah (IDR), ISO code 360
- Fijian Dollar (FJD), ISO code 242

Supported Transaction Types

Payflow accounts processing through CSIN can process the following transaction types:

- Sale
- Void
- Authorisation: CSIN provides a reference token that must be provided when the transaction is captured.
- Credit
- Delayed Capture: The capture amount cannot exceed amount of authorisation.

Setting Up the Citibank Singapore Processor

TABLE A.1 Citibank Singapore processor setup

Field Name	Required	Max Length	Default Value	UI Type
Terminal ID	Y	8		Text field
Merchant ID	Y	12 - 15		Text field
Currency Code		60	Select the correct country code	Select box

Settlement Time

Citibank Singapore settles at 9:30 PM Singapore Time. This means any transactions before this time are settled that day.

First Data Resources (FDI)

Contacting First Data International

First Data Client Services - Merchant Service Team
Level 9, 168 Walker Street
NORTH SYDNEY NSW 2060
AUSTRALIA

Supported Card Types

Payflow accounts processing through FDI can accept the following card types:

- Visa
- MasterCard
- JCB
- Diner's Club
- American Express

Supported Currencies

FDI supports transaction processing in the following currencies:

- Australian Dollar (AUD), ISO code 36
- Singapore Dollar (SGD), ISO code 702
- US Dollar (USD), ISO code 840
- Hong Kong Dollar (HKD), ISO code 344
- Malaysian Ringgit (MYR), ISO code 458
- New Zealand Dollar (NZD), ISO code 554
- Thailand Baht (THB), ISO code 764
- Taiwan Dollar (TWD), ISO code 901
- Indian Rupee (INR), ISO code 356
- Japanese Yen (JPY), ISO code 392
- Great British Pound (GBP), ISO code 826
- EMEA Euro (EUR), ISO code 978
- Kuwaiti Dinar (KWD), ISO code 414
- South Korean Won (KRW), ISO code 410

- Philippines Peso (PHP), ISO code 608
- Canadian Dollar (CAD), ISO code 124
- South African Rand (ZAR), ISO code 710
- China Yuan Renminbi (CNY), ISO code 156
- United Arab Emirates Dirhams (AED), ISO code 784
- Swiss Franc (CHF), ISO code 756
- Swedish Krona (SEK), ISO code 752
- Norweigan Krona (NOK), ISO code 578
- Danish Krona (DKK), ISO code 208
- Icelandic Krona (ISK), ISO code 352
- Indonesian Rupiah (IDR), ISO code 360
- Fijian Dollar (FJD), ISO code 242

Supported Transaction Types

Payflow accounts processing through FDI can process the following transaction types:

- Sale
- Void
- Authorisation
- Credit
- Delayed Capture
- Voice Authorisation

Setting Up the FDI Processor

To set up the FDI processor, enter the required fields and click **Next**.

TABLE A.2 FDI processor setup

Field Name	Required	Max Length	Default Value	UI Type
Terminal ID	Y	8		Text field
Merchant ID	Y	15		Text field
Acquirer	Y			Select box
Acquirer Contact		60		Text field
Acquirer Phone		30		Text field

TABLE A.2 FDI processor setup

Field Name	Required	Max Length	Default Value	UI Type
Merchant Type	Y			Select box
Merchant Name	Y	60		Text field
Merchant Address		150		Text field
Merchant City	Y	45		Text field
Postal Code	Y	10		Text field
Merchant Country	Y		AU	Select box

Settlement Time

FDI settles at 6:00 PM Australian Eastern Time. This means any transactions before this time are settled that day.

B Verbosity: Viewing Processor-Specific Transaction Results

Transaction results (especially values for declines and error conditions) returned by each PayPal-supported processor vary in detail level and in format. The Payflow 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 PayPal to normalize the transaction result values. Normalizing the values limits them to a standardized set of values and simplifies the process of integrating the Payflow SDK.

By setting Verbosity to MEDIUM, you can view the processor'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

The following Verbosity settings are supported for PayPal-supported processors. Contact your processor or bank for definitions of the returned values.

- LOW: This is the default setting for PayPal accounts. The following values are returned: {RESULT, PNREF, RESPMSG, AUTHCODE, CVV2MATCH, 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 B.1 Verbosity settings

Field Name	Type	Length	Description
HOSTCODE	Char	7	Response code returned by the processor. This value is not normalized by PayPal.
RESPTEXT	Char	17	Text corresponding to the response code returned by the processor. This text is not normalized by PayPal.
PROCCVV2	Char	1	CVV2 (buyer authentication) response from the processor
PROCCARDSECURE	Char	1	VPAS/SPA response from the 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 B.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 TRANSSSTATE 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 merchant's processor or because the card type is not set up with the merchant's processor) 12 - Unsettled transaction because of incorrect account information 14 = For various reasons, the batch containing this transaction failed settlement 15= Settlement incomplete due to a charge back 16 = Merchant ACH settlement failed; (need to manually collect it) 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 B.2 shows the increments that are possible on basic TRANSSTATE values.

TABLE B.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 Virtual Terminal to submit them for settlement or void them using a manual Void. See PayPal Manager online help for details on using 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.

C Additional Reporting Parameters

This appendix lists parameters whose values can appear in PayPal Manager reports. For example, the *Shipping and Billing* report displays these values. Some of the following parameters may also have other purposes.

TABLE C.1 Additional reporting parameters

Parameter	Description	Required	Type	Max Length
CITY	Cardholder's billing city	No	Alpha	20
COMMENT1	User-defined value for reporting and auditing purposes (PayPal parameter only)	No	Alpha-numeric	128
COMMENT2	User-defined value for reporting and auditing purposes (PayPal parameter only)	No	Alpha-numeric	128
BILLTOCOUNTRY	Cardholder's billing country code	No	Alpha-numeric	30
CUSTCODE	Customer code	No	Alpha-numeric	4
DUTYAMT	Duty amount	No	Alpha-numeric	10
EMAIL	Cardholder's email address	No	Alpha-numeric	64
FIRSTNAME	Cardholder's first name	No	Alpha-numeric	15
FREIGHTAMT	Freight amount	No	Alpha-numeric	10
LASTNAME	Cardholder's last name	No	Alpha-numeric	15
NAME	Cardholder's name	No	Alpha-numeric	15
PONUM	Purchase order number	No	Alpha-numeric	15
SHIPTOCITY	Shipping city	No	Alpha-numeric	30

TABLE C.1 Additional reporting parameters

Parameter	Description	Required	Type	Max Length
SHIPTOFIRSTNAME	First name in the shipping address	No	Alpha-numeric	30
SHIPTOLASTNAME	Last name in the shipping address	No	Alpha-numeric	30
SHIPTOSTATE	Shipping state US = 2 letter state code; outside US, use full name	No	Alpha-numeric	10
SHIPTOSTREET	Shipping street address	No	Alpha-numeric	30
SHIPTOZIP	Shipping postal code (called ZIP code in the USA)	No	Alpha-numeric	9
STATE	Cardholder's billing state code	No	Alpha-numeric	2
STREET	Cardholder's billing street address (used for AVS and reporting)	No	Alpha-numeric	30
TAXAMT	Tax amount	No	Currency	10
ZIP	Account holder's 5-to-9-digit postal code (called ZIP in the USA). Do not use spaces, dashes, or non-numeric characters.	No	Numeric	9

D XMLPay

About XMLPay

XMLPay specifies an XML syntax for payment requests and associated responses in a payment-processing network. Instead of using name/value pairs, the Payflow SDK allows the use of XML documents based on XMLPay 2.0 schema.

The typical user of XMLPay is an internet merchant or merchant aggregator who wants to dispatch credit card or other payment requests to a financial processing network.

Using the data type definitions specified by XMLPay, such a user creates a client payment request and dispatches it in the same fashion as using name/value pairs to an associated XMLPay-compliant server component. Responses are also formatted in XML and convey the results of the payment requests to the client.

Payflow Pro XMLPay Developer's Guide

Payflow Pro XMLPay Developer's Guide defines an XML syntax for payment transaction requests, responses, and receipts in a payment processing network.

You may obtain a copy of this document from the PayPal Manager Documentation page.

NOTE: For specific examples of how to submit XML documents using the Payflow client API, see the Payflow SDK Download package.

Index

R

S

T

U

V

Z

Index