

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
&AVSADDR=Y&AVSZIP=N&IAVS=Y&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 Authorization transactions. Values for AVSADDR and AVSZIP are included if you use AVS. [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 52 .	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 53 .	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 53 .	Alpha-numeric	Variable

TABLE 4.1 Transaction response values(Continued)

Field	Description	Type	Length
AUTHCODE	Returned for Sale, Authorization, and Voice Authorization transactions. AUTHCODE is the approval code obtained over the phone from the processing network. AUTHCODE is required when submitting a Force (F) transaction.	Alpha-numeric	6
AVSADDR	AVS address responses are for advice only. This process does not affect the outcome of the authorization. See “Using Address Verification Service” on page 44.	Alpha Y, N, X, or no response	1
AVSZIP	Vddress verification service ZIP code responses are for advice only. This process does not affect the outcome of the authorization. See “Using Address Verification Service” on page 44.	Alpha Y, N, X, or no response	1
IAVS	International AVS address responses are for advice only. This value does not affect the outcome of the transaction. Indicates whether AVS response is international (Y), US (N), or cannot be determined (X). Client version 3.06 or later is required. See “Using Address Verification Service” on page 44.	Alpha Y, N, X, or no response	1

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

TABLE 4.2 Payflow transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
0	Approved

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

RESULT	RESPMSG and Explanation
1	User authentication failed. Error is caused by one or more of the following: <ul style="list-style-type: none"> • Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. • 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 test-payflow.verisign.com to payflow.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 authorization-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.
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 authorization. Contact your merchant bank to obtain an authorization and submit a manual Voice Authorization 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

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

RESULT	RESPMSG and Explanation
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
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
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 authorization.)
106	Host not available
107	Duplicate suppression time-out

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

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

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

RESULT	RESPMSG and Explanation
126	Fraud Protection Services Filter — Flagged for review by filters Important Note: Result code 126 indicates that a transaction triggered a fraud filter. This is not an error, but a notice that the transaction is in a review status. The transaction has been authorized 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
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

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

RESULT	RESPMSG and Explanation
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
1042	Buyer Authentication Service — Validate Authentication failed: PARES format is invalid
1043	Buyer Authentication Service — Validate Authentication failed: Cannot find successful Verify Enrollment
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

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

RESULT	RESPMSG and Explanation
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. See step 3 of [“Preparing the Payflow Client Application” on page 19](#) for information on firewall configuration.

A value of -1 or -2 can also be possible if the PayPal servers are unavailable, or an incorrect server/socket pair has been specified. A value of -1 can also result when there are Internet connectivity errors. Contact customer support regarding any other errors.

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

TABLE 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 authorization failed
-12	Timeout waiting for response
-13	Select failure
-14	Too many connections
-15	Failed to set socket options

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

RESULT	Description
-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
-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