VeriSign
The Value of Trust℠

Payment Service Center

Payflow Pro Developer's Guide

Customer Support:
+61-3-9674-5500, selection option 3
support@verisign.com.au

VeriSign Australia Limited

Payment Service Center Payflow Pro Developer's Guide

VeriSign Australia Pty Ltd

Publication date: December 2004

DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign Australia Pty Ltd has made efforts to ensure the accuracy and completeness of the information in this document. However, VeriSign Australia Pty Ltd makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. VeriSign Australia Pty Ltd assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, VeriSign Australia Pty Ltd assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner. VeriSign Inc. reserves the right to make changes to any information herein without further notice.

TRADEMARKS

VeriSign, the VeriSign logo, VeriSign Intelligence and Control Services, VeriSign Trust Network, Payflow, Payflow Pro, Payflow Link, XMLPay, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Other trademarks and service marks in this document are the property of their respective owners.

This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more

Contents

Summary of Revisions

00000020

The following change has been made to this document since revision 4:

Testing	Information on testing credit card transactions has been further clarified. See Chapter 5, “Testing Payflow Pro Credit Card Transactions.”

DOC-AFF-PMT-GID-0009/Rev. 4

The following changes have been made to this document since revision 3:

Testing	Information on testing credit card transactions has been expanded. See Chapter 5, “Testing Payflow Pro Credit Card Transactions.”
Document restructured	Information on performing credit card transactions and using the return values is now separated into chapters.

1. Introduction

VeriSign 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).

About Payflow Pro

The Payflow Pro client resides on your computer system and is available on all major Web server platforms in a variety of formats to support integration requirements. It is available as a C library (.dll/.so), binary executable, Java library, COM object, Java Native Interface, and Perl Module Interface.

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. It does not require the HTTP protocol to run, which allows for greater flexibility in configuration and reduced processing overhead for higher performance.

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 authorization results to you.

Payflow Pro can process real-time credit card transactions and other transaction types to most of the financial processing centers in the United States & Australia.

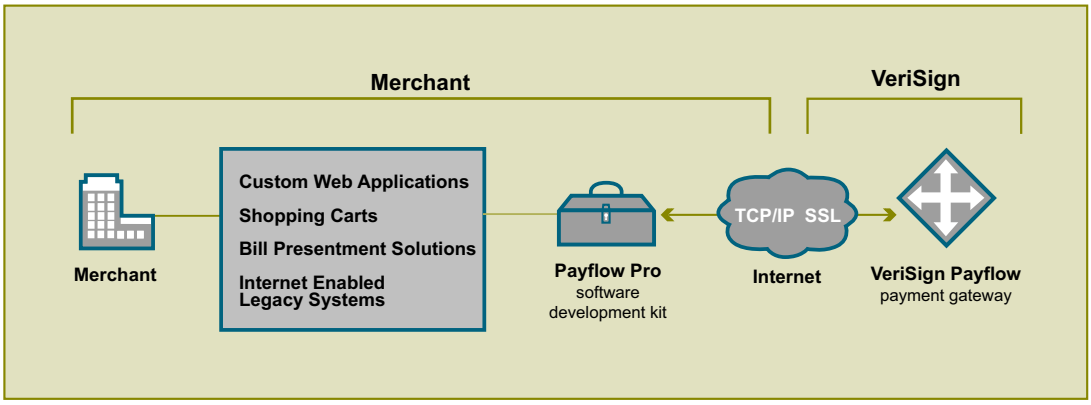

Figure 1-1 Payflow Pro transaction flow

1. The Payflow Pro client encrypts each transaction request using the latest Secure Sockets Layer (SSL) encryption and establishes a secure link with the VeriSign Payflow server over the Internet.
2. The VeriSign 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 authorization.
3. The response (approved/declined, and so on) is received from the financial network and is returned in the same session to the Payflow Pro client.
4. The Payflow Pro client completes each transaction session by transparently sending a transaction receipt to the VeriSign 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. Payflow Pro does not affect or define the time periods of authorizations, 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 authorization.

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.
- **Easy to install and implement.** Downloadable from VeriSign's Web site, Payflow Pro 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.

Pre-integrated Solutions

Payflow Pro is integrated with many third-party shopping carts and e-commerce applications.

- For a list of shopping carts compatible with Payflow Pro, see **http://www.verisign.com.au/payments/partners/carts.shtml**
- Some VeriSign integrations are included with the third-party solution. For a list of e-commerce applications compatible with Payflow Pro, see **http://www.verisign.com.au/payments/partners/carts.shtml#dev**
- Additional VeriSign integrations packages are available from VeriSign Manager's **Download** page (**https://payments.verisign.com.au/manager**):

Payflow Recurring Billing Service

VeriSign's Payflow 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 Recurring Billing Service. Using Payflow Pro to define and manage recurring transactions is fully described in *VeriSign Payflow Recurring Billing Service Guide for Payflow Pro*.

Customer Support

For problems with transaction processing or your connection to VeriSign, contact:

VeriSign Payment Services

Online Information: **http://www.verisign.com.au/payments**
http://www.verisign.com.au/support/payments/

E-mail: support@verisign.com.au
Phone: +613 9674 5500
Fax: +613 9674 5574

About this Document

This document is organized as follows:

- Chapter 2, "Installing and Configuring the Payflow Pro SDK," shows a typical Payflow Pro installation procedure for 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 Account," specifies the steps you follow when you are ready to accept live transactions with Payflow Pro.
- Appendix A, "Additional Transaction Parameters," lists processors and their processor-specific parameters.
- Appendix B, "Additional Reporting Parameters," details the parameters that can be passed to VeriSign for reporting purposes.
- Appendix C, "XMLPay," briefly describes XMLPay and tells where you may obtain a copy of *VeriSign Payment Services XMLPay 4.2 Core Specification*.
- Appendix E, "Frequently Asked Questions," contains answers to the most commonly asked questions about Payflow Pro.

Related Document

VeriSign Manager User's Guide describes the use of VeriSign Manager—the Web-based administration tool that you use to process transactions manually, issue credits, and generate reports.

About Security

It is your responsibility to protect your passwords and other confidential data and to implement security safeguards on your Web site and in your organization, or to ensure that your hosting company or internal Web operations team is implementing them on your behalf. You or your ISP/shopping cart provider should be able to adhere to security requirements as protective as those described at: **http://www.verisign.com.au/support/payments/security/fraudPrevention.shtml**

IMPORTANT! To enable you to test Payflow Pro, VeriSign provides sample transaction scripts that you customize with your VeriSign account information and password. Because the password is initially stored in the text of the program, it is vulnerable.

Do not use VeriSign's 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 Pro SDK

Before You Begin

If you plan to configure and customize the Payflow Pro SDK yourself:

You should be familiar with Web development tools and procedures. If you are not, consider letting one of VeriSign's Web development partners help you. You can find a VeriSign Web development partner at:
http://www.verisign.com.au/payments/partners/carts.shtml#dev

If you require assistance integrating the Payflow Pro SDK:

Consider using a shopping cart that integrates Payflow Pro. You can find more information at:
http://www.verisign.com.au/payments/partners/carts.shtml

Supported Platforms

Payflow Pro is available on all major Web server platforms in a variety of formats to support your integration requirements. It is available as a C library (.dll/.so), binary executable, Java library, COM object, Java Native Interface, and Perl Module Interface.

For a list of supported platforms, see the **Download** section the VeriSign Manager (**https://payments.verisign.com.au/manager**)

Preparing the Payflow Pro Client Application

Follow these steps to download and install the Payflow Pro application.

Step 1 Download the Payflow Pro SDK

From the **Download** section of the VeriSign Manager (**https://payments.verisign.com.au/manager**), download the Payflow Pro SDK appropriate for your platform.

Step 2 Extract the files to a local directory

Step 3 Configure your firewall

Enable outbound traffic for SSL (port 443).

Step 4 Set the certificate path

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

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

Step 5 Read the Readme 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 the process of performing credit card transactions.

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

Using Payflow Pro to define and manage recurring transactions is fully described in *VeriSign Payflow Recurring Billing Service Guide for Payflow Pro*.

In This Chapter

About Credit Card Processing

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

For an authorization, VeriSign 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 Address Verification Service and 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 VeriSign. If the authorization 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 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, VeriSign 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 acquiring bank works with a VeriSign-supported credit card processor, such as First Data. To use Payflow Pro to accept live credit cards, you must provide certain details about your account to VeriSign during the "Activation" part of the enrollment process.

Note An Internet Merchant Account is separate from a merchant account used for in-person retail transactions due to the different risk profile for card-not-present (e-commerce) transactions.

VeriSign has partnered with several Internet Merchant Account providers to make applying easy. Contact your VeriSign representative for more information.

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 authorization and (if successful) then flags the transaction for settlement. Two-step: Perform an Authorization-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 are described in this chapter.)

  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 Address Verification Service (AVS) and card security code (CSC).

  For AVS, if the data is submitted with the initial transaction, the issuer checks the street address and/or the ZIP (postal) code against the billing address on file for the consumer. AVS is described on page 32.

Note AVS is not available in Australia

  CSC refers to a 3- or 4-digit number that appears on the back of credit cards. (CSC is known by other names, such as CVV2 and CID, depending on the type

of card.) If CSC data is submitted, the issuer can notify you whether the number matches the number assigned to the card.

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

- Store information in your local database or use VeriSign 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 VeriSign with the transaction and report on it later.

  Note VeriSign 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 VeriSign 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 VeriSign Manager. Either way, VeriSign recommends that you monitor transaction activity using VeriSign Manager.
- You may want to discuss, with your Internet Merchant Acquirer, practices that help you to obtain the most advantageous rates.

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 VeriSign's Buyer Authentication Service, then the ECI values reflects the Authentication status. See *VeriSign Fraud Protection Services Guide.*

Credit Card Transaction Format

Note The examples in this chapter use the syntax of the pfpro executable client. Other Payflow Pro clients differ in where and how the parameter values are set, but the meaning and uses are the same.

Use the following syntax when calling the Payflow Pro client (pfpro) to process a transaction. Table 3-1 describes the arguments to the command.

```
pfpro <HostAddress> <HostPort> "<ParmList>" <TimeOut>
<ProxyAddress> <ProxyPort> <ProxyLogon> <ProxyPassword>
```

For example:

```
Pfpro test-payflow.verisign.com.au 443
"TRXTYPE=S&TENDER=C&PARTNER=VSA&VENDOR=SuperMerchant&USER=Su
perMerchant&PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&AM
T=123.00" 30
```

Table 3-1 Arguments to the pfpro executable client

Argument	Required	Description
HOSTADDRESS	Yes	VeriSign's host name. For live transactions, use **payflow.verisign.com.au** For testing purposes use **test-payflow.verisign.com.au**
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=VSA&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 17 defines the parameters used to create credit card transactions. "Values Required by All Transaction Types" on page 21 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 VeriSign client begins tracking from the time that it sends the transaction request to the VeriSign server.

Table 3-1 Arguments to the pfpro executable client (Continued)

Argument	Required	Description
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

Command Syntax Guidelines

Follow these guidelines:

- The command must be a single string with no line breaks.
- 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 (&).
- Payflow Pro supports UTF-8 format for values passed in name/value pairs.
- Calling pfpro without the required parameters results in an error message.

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 l*ength 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.

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 21 lists the parameters required for each transaction type.

Note Some processors require yet additional parameters. See Appendix A, “Additional Transaction Parameters,” for details on your processor’s requirements. Appendix B, “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	The credit card or purchase card number may not contain spaces, non-numeric characters, or dashes. For example, ACCT=5555555555554444	Yes[1]	Numeric	19
AMT	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 processor and/or Internet merchant account provider may stipulate a maximum amount.	Yes[1]	Numeric	10
AUTHCODE	AUTHCODE is returned only for approved Voice Authorization transactions. AUTHCODE is the approval code obtained over the phone from the processing network.	No, except for Voice Authorizations.	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

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.	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 upper-case	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 VeriSign Manager reports. ORIGID is case-sensitive.	Yes[1]	Alpha-numeric	12

Table 3-2 Credit-card transaction parameters (Continued)

Parameter	Description	Required	Type	Max. Length
PARTNER	The authorized VeriSign Reseller that registered you for the Payflow Pro service provided you with a Partner ID. If you registered yourself, use VSA. Case-sensitive.	Yes	Alpha-numeric	12
PWD	Case-sensitive 6- to 32-character password that you defined while registering for the account.	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). The STREET address is verified by the AVS service (described in page 32.)	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. 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 16.	Required only for card-present transactions.	Alpha-numeric	
TENDER	The tender type (method of payment). Use the value **C** for credit card transactions.	Yes	Alpha	1

Table 3-2 Credit-card transaction parameters (Continued)

Parameter	Description	Required	Type	Max. Length
TRXTYPE	The kind of transaction, for example, Sale or Credit. Described in "Values Required by All Transaction Types" on page 21.	Yes	Alpha	1
USER	By default, the username is the same as your Vendor name (see below). However, you can create additional users through VeriSign Manager. This value is case sensitive.	Yes	Alpha-numeric	64
VENDOR	Your login name. The examples in this document use VENDOR=SuperMerchant. This value is case-sensitive. You created the login name while registering for your Payflow account.	Yes	Alpha-numeric	64
VERBOSITY	LOW or MEDIUM. LOW is the default setting—normalized values. MEDIUM returns the processor's raw response values. See "Viewing Processor-specific Transaction Results: Verbosity" on page 21.	No	Alpha	
ZIP	Account holder's 5- to 9-digit ZIP (postal) code. Do not use spaces, dashes, or non-numeric characters. The postal code is verified by the AVS service and IAVS services (described on page 32). The ZIP code is verified by the AVS service (described in page 32.)	No	Alpha	9
1. Some transaction types do not require this parameter. See "Values Required by All Transaction Types" on page 21.				

Viewing Processor-specific Transaction Results: Verbosity

Transaction results (especially values for declines and error conditions) returned by each VeriSign-supported processor vary in detail level and in format. To simplify the process of integrating Payflow Pro, VeriSign *normalizes* the transaction result values, that is, limits them to a standardized set of values.

You can view the processor's raw response values by setting the Payflow Pro **Verbosity** parameter to MEDIUM (the default setting—normalized values—is LOW).

Values Required by All Transaction Types

All transaction APIs require values for the TRXTYPE, TENDER, PARTNER, VENDOR, USER, and PWD parameters. Each transaction API has additional parameter requirements, as listed here. Transaction responses are described in Chapter 4, "Responses to Credit Card Transaction Requests."

Submitting Sale Transactions

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

Additional Required Parameters for Sale Transactions

The set: [ACCT, EXPDATE, and AMT]

— or —

Set ORIGID to the PNREF (Transaction ID in VeriSign Manager reports) value returned for the original transaction. When you use ORIGID, the Sale transaction uses the transaction referred to by the ORIGID as a reference transaction. See "Submitting Reference Transactions" on page 30.

Example Sale Transaction Parameter List

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

Submitting Credit Transactions

The Credit API (TRXTYPE=C) returns the specified amount to the account holder. It is not necessary to provide the credit card number (ACCT) if you have the Transaction ID (PNREF) that was returned for the original transaction. If you issue a credit using the PNREF and do not specify an amount, then the amount of the original transaction is used.

IMPORTANT! For Test servers, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric (Example: V53A17230645). For Live servers, all of the first four characters are alpha characters, for example: VPNE12564395.

Additional Required Parameters for Credit Transactions

Set ORIGID to the PNREF (Transaction ID) value returned for the original transaction.

— or —

The set: [ACCT, EXPDATE, and AMT]

IMPORTANT! Because the default security setting for Payflow Pro accounts requires API calls to use the ORIGID parameter, this 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 the chapter on configuring account security in *VeriSign Manager User's Guide*.

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 (except Account number, Expiration date, or Swipe data).

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.

Account number	Amount	City	Comment1
Comment2	Company Name	Country	Cust_Code
CustIP	DL Num	DOB	Duty amount
EMail	Expiration date	First name	Freight amount
Invoice number	Last name	Middle Name	Purchase order number
Ship To City	Ship To Country	Ship To First Name	Ship To Last Name
Ship To Middle Name	Ship To State	Ship To Street	Ship To ZIP
SS Num	State	Street	Suffix
Swipe data	Tax amount	Tax exempt	Telephone
Title	ZIP		

Example Credit Transaction Parameter List

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

— or —

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

Submitting Void Transactions

The Void API (TRXTYPE=V) prevents a transaction from being settled, but does not release the authorization (hold on funds) on the cardholder's account. Follow these guidelines:

- You can void Delayed Capture, Sale, Credit, Authorization, and Voice Authorization transactions. You cannot void a Void transaction.
- The Void must occur prior to settlement.

Additional Required Parameters for Void Transactions

Set ORIGID to the PNREF (Transaction ID in VeriSign Manager reports) value returned for the original transaction.

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 (except Account number, Expiration date, or Swipe data).

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.

Account number	Amount	City	Comment1
Comment2	Company Name	Country	Cust_Code
CustIP	DL Num	DOB	Duty amount
EMail	Expiration date	First name	Freight amount
Invoice number	Last name	Middle Name	Purchase order number
Ship To City	Ship To Country	Ship To First Name	Ship To Last Name
Ship To Middle Name	Ship To State	Ship To Street	Ship To ZIP

SS Num	State	Street	Suffix
Swipe data	Tax amount	Tax exempt	Telephone
Title	ZIP		

Example Void Transaction Parameter List

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

Submitting Voice Authorization Transactions

Some transactions cannot be authorized over the Internet (for example, high dollar amounts)—processing networks generate Referral (Result Code 13) transactions for such requests.

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 authorization code (AUTHCODE) for the transaction. You include this AUTHCODE as part of a Voice Authorization (TRXTYPE=F) transaction.

IMPORTANT! For Test servers, the AUTHCODE contains alpha-numeric characters (for example, 123PNI). For Live servers, the AUTHCODE contains only numeric digits (for example, 123456).

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

Like Sale or Delayed Capture transactions, approved Voice Authorization transactions can be voided.

Additional Required Parameters for Voice Authorization Transactions

AUTHCODE

ACCT

EXPDATE

AMT

Example Voice Authorization Transaction Parameter List

```
"TRXTYPE=F&TENDER=C&PARTNER=VSA&VENDOR=SuperMerchant&USER=Su
perMerchant&PWD=x1y2z3&AUTHCODE=AB34RT56&ACCT=55555555555544
44&EXPDATE=0308&AMT=123.00"
```

Submitting Inquiry Transactions

An Inquiry transaction (TRXTYPE=I) returns the result and status of a transaction. You perform inquiries using a reference to the original transaction—either the PNREF value returned for the original transaction or the CUSTREF value that you specified for the original transaction.

Inquiries based on a CUSTREF value return data on the most recent non-Inquiry transaction rather than the first 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.

Using the PNREF to Perform Inquiry Transactions

Set ORIGID to the PNREF (Transaction ID in VeriSign Manager reports) value returned for the original transaction.

Example Inquiry Transaction Parameter List, Using the ORIGID Parameter set to the PNREF Value

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

Using the CUSTREF to Perform Inquiry Transactions

Specify the CUSTREF value and, optionally, the STARTTIME and ENDTIME parameters.

CAUTION If there are multiple transactions with a particular CUSTREF value, then the Inquiry transaction returns only the first 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.

Example Inquiry Transaction Parameter List, Using the CUSTREF

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

Submitting Authorization/Delayed Capture Transactions

Visa/MasterCard regulations prohibit merchants from capturing credit card transaction funds until product has shipped to the buyer. Because of this rule, most processing networks implement a two-stage transaction solution. VeriSign refers to this as delayed capture processing. This process consists of an authorization (TRXTYPE=A) transaction followed (when the merchant is ready to collect funds) by a Delayed Capture (TRXTYPE=D) transaction.

An Authorization transaction does not transfer funds, rather it places a hold on the cardholder's open-to-buy limit, lowering the cardholder's limit by the amount of the transaction. A delayed capture transaction then captures the original authorization amount. The transaction is scheduled for settlement during the next settlement period.

IMPORTANT! Only one Delayed Capture transaction is allowed per Authorization transaction.

Additional Required Parameters for Authorization Transactions

The set: [ACCT, EXPDATE, and AMT]

— or —

Perform a reference transaction by specifying the ORIGID of an existing transaction. See "Submitting Reference Transactions" on page 30.

Additional Required Parameters for Delayed Capture Transactions

Set ORIGID to the PNREF (Transaction ID in VeriSign Manager reports) value returned for the original transaction. If the amount of the capture differs from the amount of the authorization, then you must specify a value for AMT.

Fields Copied From the Authorization Transaction into the Delayed Capture Transaction

The following fields are copied from the Authorization 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 (except Account number, Expiration date, or Swipe data).

Account number	Amount	City	Comment1
Comment2	Company Name	Country	Cust_Code
CustIP	DL Num	DOB	Duty amount
EMail	Expiration date	First name	Freight amount
Invoice number	Last name	Middle Name	Purchase order number
Ship To City	Ship To Country	Ship To First Name	Ship To Last Name
Ship To Middle Name	Ship To State	Ship To Street	Ship To ZIP
SS Num	State	Street	Suffix
Swipe data	Tax amount	Tax exempt	Telephone
Title	ZIP		

Step 1 Perform the Authorization transaction

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

The return data for an Authorization transaction is the same as for a Sale transaction. To capture the authorized funds, perform a Delayed Capture transaction that includes the value returned for PNREF, as described in Step 2 on page 29.

IMPORTANT! For Test servers, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric (Example: V53A17230645). For Live servers, all of the first four characters are alpha characters (letters), for example: VPNE12564395.

Example Authorization Transaction Parameter List

Issue Authorization-only Transaction

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=VSA
&VENDOR=SuperMerchant&USER=SuperMerchant&ACCT=55555555555544
44&EXPDATE=0308&AMT=123.00&COMMENT1=Second purchase
&COMMENT2=Low risk customer&INVNUM=1234567890&STREET=5199
MAPLE&ZIP=94588"
```

Example Authorization Response

```
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 from the original authorization transaction. (There is no need to retransmit the credit card or billing address information—it is stored at VeriSign.)

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

Example Delayed Capture Transaction Parameter List

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

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 authorization 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 authorization 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 authorization-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 VeriSign server to successfully process it. Conversely, if a capture for a previous authorization succeeds, subsequent attempts to capture it again will return an error.

Submitting Reference Transactions

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 *VeriSign Manager User's Guide* for instructions on setting this and other VeriSign Manager security features.

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

IMPORTANT! When VeriSign 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.

Reference transactions are not screened by Fraud Protection Services filters.

You can also initiate reference transactions from VeriSign Manager. See *VeriSign Manager User's Guide* for details.

Transaction Types that can be Used as the Original Transaction

You can reference the following transaction types to supply data for new Sale or Authorization transactions:

Authorization (To capture the funds for an approved Authorization transaction, be sure to perform a Delayed Capture transaction—**not** a Reference transaction.)

Credit

Delayed Capture

Sale

Voice Authorization (The Voice Authorization code is not copied to the new transaction)

Void

Fields Copied From Reference Transactions

The following fields are copied from the referenced transaction into the new Sale or Authorization 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.

Fields Copied From Original Transactions

Account Type	Street
Account Number	City
Expiration Date	State
First Name	ZIP
Middle Name	Country
Last Name	Swipe Data

Example Reference Transaction

In this example, you authorize 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 authorization transaction.

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

You use an authorization transaction for the full amount of the purchase of $100:

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=VSA&VENDOR=SuperMerchant
&USER=SuperMerchant&ACCT=5555555555554444&EXPDATE=0308&AMT=100.
00&INVNUM=1234567890&STREET=5199 MAPLE&ZIP=94588"
```

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

Step 2 Capture the authorized 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.

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

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

Step 3 Submit a new sales 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 authorization as a reference transaction. (This is a sale transaction because only one delayed capture transaction is allowed per authorization.)

```
"TRXTYPE=S&TENDER=C&PWD=x1y2z3&PARTNER=VSA&VENDOR=SuperMerchant
&USER=SuperMerchant&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 authorization/delayed capture cycle for all transactions, you could have chosen to use an authorization/delayed capture to collect the $34 in this example. You would generate the authorization for the $34 using the initial authorization as a reference transaction.

Using Address Verification Service (AVS)

To qualify for the lowest bank rate, you must pass Address Verification Service (AVS) information—street address and ZIP (postal) code.

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

Note AVS & IAVS are not available in Australia.

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

The International AVS response (**IAVS**) indicates whether AVS response is international (**Y**), USA (**N**), or cannot be determined (**X**). Client version 3.06 or later is required.

Credit Cards Supporting AVS

American Expres, Discover, MasterCard, and Visa support AVS.

Tip See your processor's information in Appendix A, "Additional Transaction Parameters," for information on their handling of AVS.

Example AVS Request Parameter List

This example request include the AVS request parameters STREET and ZIP:

```
"TRXTYPE=A&TENDER=C&PWD=x1y2z3&PARTNER=VSA&VENDOR=SuperMerch
ant&USER=SuperMerchant&&ACCT=5555555555554444&EXPDATE=0308&A
MT=123.00&STREET=5199 Maple&ZIP=98765"
```

Example AVS Response

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

```
RESULT=0&PNREF=VXW412345678&RESPMSG=APPROVED&AUTHCODE=123456
&AVSADDR=Y&AVSZIP=N&IAVS=X
```

Card Security Code (CSC) Validation

The card security code (CSC) is a 3- or 4-digit number (not part of the credit card number) that is printed on the credit card. Because the CSC appears only on the card and not on receipts or statements, the CSC provides some assurance that the physical card is in the possession of the buyer.

Tip This fraud prevention tool has various names, depending on the payment network. Visa calls it CVV2, MasterCard calls it CVC2, and American Express and Discover call it CID. To ensure that your customers see a consistent name, VeriSign recommends use of the term Card Security Code (CSC) on all end-user materials.
On most cards, the CSC is printed on the back of the card (usually in the signature field). All or part of the card number appears before the CSC (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.
See:
http://www.verisign.com.au/support/payments/general/cardSecurityCode.shtml for the latest information.

Credit Cards Supporting CSC

MasterCard and Visa support CSC.

CSC Results

If you submit the CVV2 parameter, the cardholder's bank returns a Yes/No response in the CVV2MATCH response value as follows:

Table 3-3 CVV2MATCH response values

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

Transactions that have CSC 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 authorization was successful, you must make a decision based on the CVV2MATCH value whether or not to proceed with the order.

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 VeriSign to set up a separate Payflow Pro account for card-present transactions.

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 16. The length tag in the following example is `[40]`.

Do not include the `ACCT` or `EXPDATE` parameters in card-present transactions.

Example Card-present Transaction Parameter List

```
"TRXTYPE=S&TENDER=C&PARTNER=VSA&USER=SuperMerchant&PWD=Su
perMerchant&SWIPE[40]=;4912000033330026=05121011000012345
678?&AMT=21.00"
```

Logging Transaction Information

VeriSign maintains a record of all transactions executed on your account. This record is not the official bank statement. The credit card transaction summary that you receive from your acquiring bank is the official record.

Use VeriSign Manager at **https://payments.verisign.com.au/manager** to view this record and use the information to help reconcile your accounting records.

VeriSign strongly recommends that you log all transaction results on your own system and that you do *not* store credit card information.

At a minimum, log the following data:

- PNREF

  IMPORTANT! For Test servers, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric (for example, V53A17230645). For Live servers, all of the first four characters are alpha characters (for example, VPNE12564395).

  If you have any questions regarding a transaction, refer to or search on the PNREF. In VeriSign Manager reports, the PNREF value appears in the Transaction ID column.

- Transaction Date
- Transaction Amount
- AUTHCODE

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, VeriSign 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	VeriSign Reference ID, a unique number that identifies the transaction. PNREF is described in “PNREF Value (Payflow Pro Merchants)” on page 39.	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 39.	Numeric	Variable

Table 4-1 Transaction response values (Continued)

Field	Description	Type	Length
CVV2MATCH	Result of the card security code (CVV2) check. This value does not affect the outcome of the transaction.	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 39.	Alpha-numeric	Variable
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 (AVS)" on page 32.	Alpha Y, N, X, or no response	1
AVSZIP	AVS ZIP code responses are for advice only. This process does not affect the outcome of the authorization. See "Using Address Verification Service (AVS)" on page 32.	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 (AVS)" on page 32.	Alpha Y, N, X, or no response	1

PNREF Value (Payflow Pro Merchants)

The Payment Network Reference ID value (PNREF) is a unique transaction identification number issued by VeriSign that identifies the transaction for billing, reporting, and transaction data purposes. The PNREF value appears in the Transaction ID column in VeriSign Manager reports.

- The PNREF value is used as the TRANSID 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 TRANSID value (original transaction ID) value in reference transactions for authorization (TRXTYPE=A) and Sale (TRXTYPE=S).

PNREF Format

The PNREF value is a 12-character alpha-numeric string. The content depends on whether the value represents a test or live transaction, as follows:

- For Test servers, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric, for example V53A17230645.
- For Live servers, all of the first four characters are alpha characters (letters), for example: VPNE12564395.

RESULT Codes and RESPMSG Values

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

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

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

RESULT Values for Transaction Declines or Errors

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

Table 4-2 VeriSign 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: 1) Invalid User, Merchant Login, Partner, or Password entered during login. Login information is case-sensitive. 2) Invalid Processor information entered. Contact merchant bank to verify. 3) "Allowed IP Address" security feature implemented. 4) Test account submitting transactions to live VeriSign servers.
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**
5	**Invalid merchant information.** Processor does not recognize your merchant account information. Contact your bank account acquirer to resolve this problem.
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 and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call the credit card issuer to resolve.
13	**Referral.** Transaction was declined but could be approved with a verbal authorization from the bank that issued the card. Submit a manual Voice Authorization transaction and enter the verbal auth code.

Table 4-2 VeriSign transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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.** Not signed up for this tender 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**
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**

Table 4-2 VeriSign transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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**
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**
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 VeriSign Manager *Security Settings* page. If the transaction exceeded the Maximum Amount security setting, then no values are returned for AVS or CSC. See *VeriSign Manager User's Guide* for information on the *Security Settings* page. ▪ AVS validation failed. The AVS return value should appear in the RESPMSG. ▪ CSC validation failed. The CSC return value should appear in the RESPMSG.

Table 4-2 VeriSign transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
118	**Invalid keywords found in string fields**
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 authorized but requires you to review and to manually accept the transaction before it will be allowed to settle. This result occurred due to that fact that all new Payflow accounts include a "test drive" of the Fraud Protection Services at no charge. The filters are on by default, and a suspicious transaction triggered Result code 126. You can modify these settings based on your business needs. 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 chapter entitled "Assessing Transactions that Triggered Filters" in *Fraud Protection Services Guide* or *User's Guide for Payflow Link Guide With Fraud Protection Services*.
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.
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

Table 4-2 VeriSign transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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). To enroll, log in to VeriSign Manager, click Security, and then click the Buyer Authentication Service banner on the page.
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

Table 4-2 VeriSign transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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. Either the VeriSign server is unavailable, or incorrect server/socket pairs have been specified. A value of -1 can also result when there are Internet connectivity errors. Refer other errors to VeriSign at **support@verisign.com.au.**

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
-99	Out of memory

5. Testing Payflow Pro Credit Card Transactions

To test your application, direct all transactions to **test-payflow.verisign.com.au**. Transactions directed to this URL are processed through VeriSign'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 VeriSign Manager.

Differences Between Responses Returned by Live (Production) Servers and Test Servers

For Test servers, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric, for example V53A17230645.

For Live servers, all of the first four characters in the PNREF value are alpha characters (letters), for example: VPNE12564395.

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
Amex Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904
Diners Club	38520000023237
JCB	3530111333300000
JCB	3566002020360505
MasterCard	5555555555554444
MasterCard	5105105105105100
Visa	4111111111111111
Visa	4012888888881881
Visa	4222222222222 **Note**: Even though this number has a different character count than the other test numbers, it is the correct and functional number.

Testing Result Codes 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 5-3 lists VeriSign result codes that are supported by this testing mechanism.

Note Note For all hosts except First Data International: 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 VeriSign 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 VeriSign result code supported by this testing mechanism, result 12 (Declined) is returned.
$2001+	12 – Decline

VeriSign Result Codes Returned Based on Transaction Amount

This table lists the VeriSign 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**).

Table 5-3 VeriSign result codes supporting the amount control

Processor	Result Codes available for testing
FDMS Nashville	0, 12, 13, 104
Paymentech	0, 12, 13, 104
Vital	0, 4, 12, 13, 23, 104, 114, 1000
Nova	0, 12, 13, 104
FDMS South	0, 12, 13, 104

Table 5-3 VeriSign result codes supporting the amount control (Continued)

Processor	Result Codes available for testing
Amex	0, 12, 13, 104, 1000
PBS	0, 4, 7, 12, 13, 24, 23, 1000
KSNet	0, 12, 104
Citibank	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
Global Payments East (NDCE)	0, 4, 5, 12, 13, 23, 24, 30, 100, 104, 114, 1000
Global Payments Central (MAPP)	0, 4, 5, 8, 12, 13, 23, 24, 104, 111, 114, 1000

Alternative Methods for Generating Specific Result Codes

This table shows another method for obtaining VeriSign result codes. Non-zero results from processors are not returned by VeriSign's 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 VeriSign result code

Result	Definition	How to test using Payflow Pro
0	Approved	Use an AMOUNT of $1000 or less For all hosts except FDRA: 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 an AMOUNT of 1005.

Table 5-4 Obtaining VeriSign result code (Continued)

7	Field format error	Submit a Delayed Capture transaction with no ORIGID
10	Too many line items	OBSOLETE.
12	Declined	Use an AMOUNT of 1012 or an AMOUNT of 2001 or more
13	Referral	Use an AMOUNT of 1013
19	Original transaction ID not found	Submit a Delayed Capture transaction with an invalid ORIGID
22	Invalid ABA number	Applies only to ACH transactions – submit an invalid ABA number (8 digits)
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	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).
30	Duplicate Transaction	Use an AMOUNT of 1030..
50	Insufficient funds available	Use an amount of 1050.
99	General error	Use an AMOUNT of 1099.
100	Invalid transaction returned from host	Use an AMOUNT of 1100. .
101	Time-out value too small	Set timeout value to 1.
103	Error reading response from host	Use an AMOUNT of 1103.
104	Timeout waiting for processor response	Use an AMOUNT of 1104.
105	Credit error	Attempt to credit an authorization.
108	Void error	Attempt to void a captured authorization.
111	Capture error	Capture an Authorization transaction twice or attempt to capture a transaction that is not an Authorization transaction.

Table 5-4 Obtaining VeriSign result code (Continued)

112	Failed AVS check	You cannot generate this RESULT value by submitting an amount of 1112, but must submit a value for AVS that will fail. In production, this error occurs only if your account is configured by VeriSign customer service to use the "AVS Deny" feature.
113	Cannot exceed sales cap	Applies to ACH transactions only.
114	CVV2 Mismatch	Use an AMOUNT of 1114.
1000	Generic Host Error	Use an AMOUNT of 2000.

Testing Address Verification Service (AVS)

The VeriSign testing server simulates AVS by returning a value for **AVSADDR** based on the first three characters of the submitted value for **STREET**.

The testing server returns a value for **AVSZIP** based on the submitted **ZIP** value as shown in the table.

Note AVS & IAVS are not available in Australia.

If **STREET** starts with 667 or higher or begins with a non-numeric character, then the simulator returns **AVSADDR=X, AVSZIP=X**.

Table 5-5 Testing AVSADDR

Submitted Value for STREET	Example STREET Value	AVSADDR Result
000-333	24285 Elm	Y
334-666	49354 Main	N
667 or higher or begins with a non-numeric character	79232 Maple	X

Table 5-6 Testing AVSZIP

Submitted Value for ZIP	Example ZIP Value	AVSZIP Result
00000-50000	00382	Y
50001-99999	94303	N
Any value (if street address is 667 or higher or begins with a non-numeric character)	STREET=79232 Maple, ZIP=20304	X

Testing Card Security Code (CVV2)

If you submit a value for the card security code (**CVV2**), 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. CSC is described in

---

Tip Some processors decline failed card security code without returning a . Test the results and check with your processor to determine whether they support CSC checking.

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

Table 5-7 Testing CVV2MATCH

CVV2 Value	CVV2MATCH Value
000	Null

Table 5-7 Testing CVV2MATCH

001-300	Y
301-600	N
601 or higher	X

6. Activating Your Payflow Account

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

1. Log in to VeriSign Manager (**https://payments.verisign.com.au/manager**).
2. Click the **Click Here to Activate Your Account** button and follow the on-screen instructions.
3. Point your clients to the Active Payflow Pro servers. In your client applications, change **test-payflow.verisign.com.au** to **payflow.verisign.com.au**

APPENDIX 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

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

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

Table A-1

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 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
- Australian Bank card
- JCB
- Diners Club
- American Express

Supported Currencies

FDI supports transaction processing in the following currencies.

- Australian Dollar (AUD), ISO code 36
- United States Dollar (USD), ISO code 840
- New Zealand Dollar (NZD), ISO code 554
- Japanese Yen (JPY), ISO code 392
- Great Britain Pound (GBP), ISO code 826
- EMEA Euro (EUR), ISO code 978
- Kuwaiti Dinar (KWD), ISO code 414
- South Korean Won (KRW), ISO code 410
- Singapore Dollar (SGD), ISO code 702
- Hong Kong Dollar (HKD), ISO code 344

- Taiwan Dollar (TWD), ISO code 901
- Malaysian Ringgit (MYR), ISO code 458
- Thailand Baht (THB), ISO code 764
- 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

Supported Transaction Types

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

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

Setting up the FDI Processor

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

Table A-2

Field name	Required	Max Length	Default Value	UI Type
Merchant ID	Y	15		Text Field
Terminal ID	Y	8		Text Field
Acquirer	Y			Select Box
Acquirer Contact		60		Text Field
Acquirer Phone		30		Text Field
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 that any transactions before this time are settled that day.

B. Additional Reporting Parameters

This appendix lists parameters whose values can appear in VeriSign Manager reports. For example, the *Shipping and Billing* report displays these values. Some of the following parameters may also have other purposes. The `STREET` and `ZIP` parameters, for instance, are also used for AVS.

Note For regular credit card transactions, reporting parameters are normally not passed to the processor. See Appendix A, "Additional Transaction Parameters" to learn which fields are sent to your processor.

Table B-1 VeriSign 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 (VeriSign parameter only)	No	Alpha-numeric	128
COMMENT2	User-defined value for reporting and auditing purposes (Verisign parameter only)	No	Alpha-numeric	128
COMPANYNAME	Cardholder's company	No	Alpha-numeric	30
COUNTRY	Cardholder's billing country code	No	Alpha-numeric	3
CUSTCODE	Customer code	No	Alpha-numeric	30

Table B-1 VeriSign reporting parameters (Continued)

Parameter	Description	Required	Type	Max Length
DUTYAMT	Duty amount	No	Alpha-numeric	10
EMAIL	Cardholder's e-mail address	No	Alpha-numeric	64
FIRSTNAME	Cardholder's first name	No	Alpha	15
FREIGHTAMT	Freight amount	No	Currency	10
LASTNAME	Cardholder's last name	No	Alpha	15
NAME	Cardholder's name	No	Alpha-numeric	15
PONUM	Purchase Order Number	No	Alpha-numeric	15
SHIPTOCITY	Shipping city	No	Alpha-numeric	30
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

Table B-1 VeriSign reporting parameters (Continued)

Parameter	Description	Required	Type	Max Length
TAXAMT	Tax amount	No	Currency	10
ZIP	Account holder's 5- to 9-digit postal code (called ZIP code in the USA). Do not use spaces, dashes, or non-numeric characters. The postal code is verified by the AVS service.	No	Numeric	9

C. 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, Payflow Pro allows for the use of XML documents via XMLPay.

The typical user of XMLPay is an Internet merchant or merchant aggregator who wants to dispatch credit card, corporate purchase card, Automated Clearinghouse (ACH), 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.

XMLPay 2.0 Core Specification Document

VeriSign XMLPay 4.2 Core Specification 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 **Downloads** page of VeriSign Manager (**https://payments.verisign.com.au/manager**).

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

E. Frequently Asked Questions

- **Where do I find online information about Payflow Pro?**

  See: **http://www.verisign.com.au/support/payments/payflowpro/**

- **How do I download the VeriSign SDK?**

  Log in to VeriSign Manager and click **Downloads**. All VeriSign SDKs are listed by server platform and operating system. All SDKs are contained in downloadable WinZip files. You can download WinZip at **http://www.winzip.com**.

- **Do I need the VeriSign SDK if I already have a shopping cart?**

  Refer to your shopping cart documentation to verify its compatibility with VeriSign. Your shopping cart documentation should specify if it is pre-integrated or requires a VeriSign SDK plug-in. Shopping cart SDKs are available on VeriSign's Manager's **Downloads** page.

- **How do I know my transactions are connecting to VeriSign?**

  We send your server a 12-character PNREF (for example, VXES98765432) for every transaction submitted to our servers. The PNREF appears in VeriSign Manager Reports as the Transaction ID.

  For Test transactions, the first and fourth characters in the PNREF value are alpha characters (letters), and the second and third characters are numeric (Example: V53A17230645). For Live transactions, all of the first four characters are alpha characters, for example: VPNE12564395.

- **How do I process test transactions?**

  Once you have registered with VeriSign and have completed the integration/configuration of your storefront use the following information to begin testing transactions:

  HostAddress: *test-payflow.verisign.com.au*
  HostPort: *443*
  PARTNER: *VSA*
  VENDOR: *Your case-sensitive login*
  USER: *Your case-sensitive login*
  PWD: *Your case-sensitive password*

- **How do I process live transactions?**

  Once you have successfully processed test transactions, use the following information to reconfigure your storefront:
  HostAddress: *payflow.verisign.com.au*
  HostPort: *443*
  PARTNER: *VSA*
  VENDOR: *Your case-sensitive login*
  USER: *Your case-sensitive login*
  PWD: *Your case-sensitive password*

- **Is the SDK thread-safe?**

  Yes. All of our SDKs are thread-safe.

- **Can you provide guidelines about using the various Payflow SDKs to process transactions in a multi-threaded environment?**

  First, pfproInit() must be called at the start of the main thread, and pfproCleanup() must be called at its finish. You can create multiple threads, each with multiple contexts, and send any number of transactions using each context. However, all threads must be created and completed between the calls to pfproInit() and pfproCleanup().

  While it is possible to submit multiple transactions using a single context, we strongly recommend that you create a new context for each transaction.

  Example pseudo code:

  1. CreateObject - to create the COM object
  2. CreateContext - to setup the context and communication parameters

3 (Build a string containing all transaction parameters)

4 SubmitTransaction - Process the transaction

5 (Parse the string returned for result information)

6 DestroyContext - Destroy the context.

Index