CyberSource Secure Acceptance Silent Order POST

Development Guide

October 2017

CyberSource®

the power of payment

CyberSource Contact Information

For general information about our company, products, and services, go to
http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or
call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center:
http://www.cybersource.com/support

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
October 2017	■ Added a note concerning the JCN gateway to the following field (see "API Request Fields," page 58): ● bill_to_address_line1
August 2017	■ Added the "Enabling Japanese Payment Options" section. See "Enabling Japanese Payment Options," page 21. ■ Added the Nicos, Orico, and Private label card types. See card_type , page 64. ■ Added the following request fields (see Table 6, "API Request Fields," on page 58): ● jpo_payment_installments ● jpo_payment_method ■ Added the following reply fields (see Table 7, "API Reply Fields," on page 90): ● req_jpo_payment_installments ● req_jpo_payment_method
June 2017	This revision contains only editorial changes and no technical updates.
April 2017	■ Update the "Custom Email Receipt" section. See "Custom Email Receipt," page 28. ■ Updated the following request fields (see Table 6, "API Request Fields," on page 58): ● bill_to_address_postal_code ● consumer_id ■ Added the following reply fields (see Table 7, "API Reply Fields," on page 90): ● req_bill_to_address_postal_code ● req_consumer_id
March 2017	■ Updated the following request fields (see Table 6, "API Request Fields," on page 58): ● e_commerce_indicator ● echeck_routing_number ● signed_date_time

Release	Changes
January 2017	▪ Added the following request fields (see Table 6, "API Request Fields," on page 58):
	● issuer_additional_data
	● recipient_account_id
	● recipient_date_of_birth
	● recipient_surname
	● recipient_postal_code
	▪ Added the following reply fields (see Table 7, "API Reply Fields," on page 90):
	● req_issuer_additional_data
	● req_recipient_account_id
	● req_recipient_date_of_birth
	● req_recipient_surname
	● req_recipient_postal_code

About This Guide

Audience and Purpose

This guide is written for merchants who want to customize and control their own customer checkout experience, including receipt and response pages. You will have full control to store and control customer information before sending it to CyberSource to process transactions. You will use the Business Center to review and manage all of your orders.

Using Secure Acceptance Silent Order POST requires moderate scripting skills. You must create a security script and modify your HTML form to pass order information to CyberSource.

Web Site Requirements

Your web site must meet the following requirements:

- Have shopping-cart or customer order creation software.

- Contain product pages in one of the supported scripting languages (see "Sample Scripting Languages," page 31).

- The IT infrastructure must be Public Key Infrastructure (PKI) enabled to use SSL-based form POST submissions.

- The IT infrastructure must be able to digitally sign customer data prior to submission to Secure Acceptance.

Conventions

Note, Important, and Warning Statements

Note

A *Note* contains helpful suggestions or references to material not contained in the document.

Important

An *Important* statement contains information essential to successfully completing a task or learning a concept.

Warning

A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

Text and Command Conventions

Convention	Usage
Bold	■ Field and service names in text; for example: Include the **transaction_type** field. ■ Items that you are instructed to act upon; for example: Click **Save**.
`Screen text`	■ Code examples and samples. ■ Text that you enter in an API environment; for example: Set the **transaction_type** field to `create_payment_token`.

Related Documents

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Table 1   Related Documents

Subject	Description
Credit Card	The following documents describe how to integrate credit card processing into an order management system: ■ *Credit Card Services Using the SCMP API* (PDF | HTML) ■ *Credit Card Services Using the Simple Order API* (PDF | HTML)
Decision Manager	The following documents describes how to integrate and use the Decision Manager services. ■ *Decision Manager Developer Guide Using the SCMP API* (PDF | HTML) ■ *Decision Manager Developer Guide Using the Simple Order API* (PDF | HTML)
eCheck	The following documents describe how to integrate and use the eCheck services: ■ *Electronic Check Services Using the SCMP API* (PDF | HTML) ■ *Electronic Check Services Using the Simple Order API* (PDF | HTML)
Level II and Level III	*Level II and Level III Processing Using Secure Acceptance* (PDF | HTML)—describes each Level II and Level III API field and processing Level II and Level III transactions using Secure Acceptance.
Payer Authentication	The following documents describe how to integrate and use the payer authentication services: ■ *Payer Authentication Using the SCMP API* (PDF | HTML) ■ *Payer Authentication Using the Simple Order API* (PDF | HTML)
Payment Security Standards	Payment Card Industry Data Security Standard (PCI DSS)—web site offers standards and supporting materials to enhance payment card data security.
Payment Tokenization	The following documents describe how to create customer profiles and use payment tokens for on-demand payments: ■ *Payment Tokenization Using the Business Center* (PDF | HTML) ■ *Payment Tokenization Using the SCMP API* (PDF | HTML) ■ *Payment Tokenization Using the Simple Order API* (PDF | HTML)
PayPal Express Checkout	The following documents describes how to integrate and use the PayPal Express Checkout services: ■ *PayPal Express Checkout Services Using the SCMP API* (PDF | HTML) ■ *PayPal Express Checkout Services Using the Simple Order API* (PDF | HTML).

Table 1   Related Documents (Continued)

Subject	Description
Recurring Billing	The following documents describe how to create customer subscriptions and use payment tokens for recurring and installment payments: ■ *Recurring Billing Using the Business Center* (PDF | HTML) ■ *Recurring Billing Using the SCMP API* (PDF | HTML) ■ *Recurring Billing Using the Simple Order API* (PDF | HTML)
Reporting	*Reporting Developer Guide* (PDF | HTML)—describes how to view and configure Business Center reports.
Secure Acceptance	The following documents describe how to create a Secure Acceptance profile and render the Secure Acceptance Web/Mobile checkout, along with processing a transaction with the service fee included: ■ *Secure Acceptance Web/Mobile Configuration Guide* (PDF | HTML) ■ *Secure Acceptance Silent Order POST Service Fee Guide* (PDF)

Customer Support

For support information about any CyberSource service, visit the Support Center:

http://www.cybersource.com/support

Using Secure Acceptance Silent Order POST

CyberSource Secure Acceptance Silent Order POST provides a seamless customer checkout experience that keeps your branding consistent. You can create a Secure Acceptance Silent Order POST profile and configure the required settings to set up your customer checkout experience.

Secure Acceptance Silent Order POST can significantly reduce your Payment Card Industry Security Standard (PCI DSS) obligations by sending payment data directly from your customer's browser to CyberSource servers. Your web application infrastructure does not come into contact with the payment data and the transition is *silent*.

Warning Secure Acceptance is designed to process transaction requests directly from the customer browser so that sensitive payment data does not pass through your servers. If you do intend to send payment data from your servers, use the SOAP Toolkit API or the Simple Order API. Sending server-side payments using Secure Acceptance incurs unnecessary overhead and could result in the suspension of your Secure Acceptance profile and subsequent failure of transactions.

To create your customer checkout experience you will take these steps:

1 Create and configure Secure Acceptance Silent Order POST profiles.

2 Update the code on your web site to POST payment data directly to CyberSource from your secure payment form (see "Sample Transaction Process Using JSP," page 31). CyberSource processes the transaction on your behalf by sending an approval request to your payment processor in real time. See "Secure Acceptance Transaction Flow," page 13.

3 Use the reply information to generate an appropriate transaction response page to display to the customer. You can view and manage all orders in the Business Center. You can configure the payment options, response pages, and customer notifications. See "Creating a Silent Order POST Profile," page 17.

Secure Acceptance Profile

A Secure Acceptance profile consists of settings that you configure to create a customer checkout experience. You can create and edit multiple profiles, each offering a custom checkout experience. For example, you might want to offer different payment options for different geographic locations.

Secure Acceptance Transaction Flow

The Secure Acceptance Silent Order POST transaction flow is illustrated in Figure 1 and described below.

Figure 1   Secure Acceptance Silent Order POST Transaction Flow
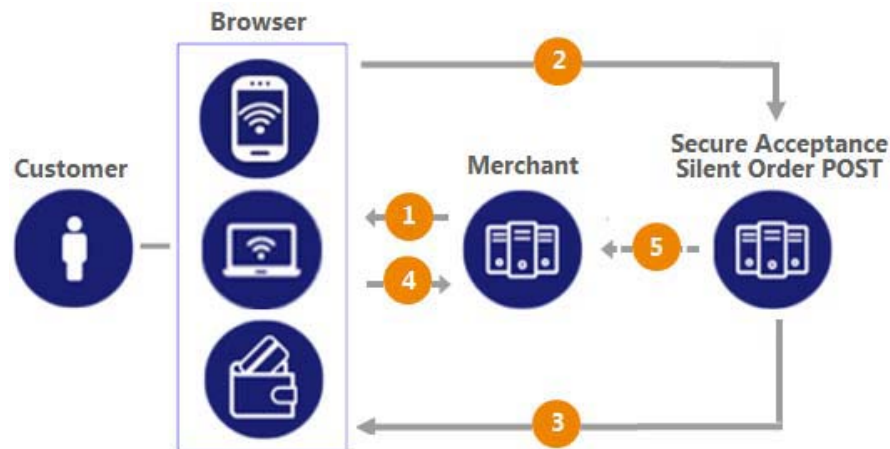
1   Display the checkout page on your customer's browser with a form to collect their payment information and include a signature to validate their order information (signed data fields).

2   The customer enters and submits their payment details (the unsigned data fields). The transaction request message, the signature, and the signed and unsigned data fields are sent directly from your customer's browser to the CyberSource servers. The unsigned data fields do not pass through your network.

CyberSource reviews and validates the transaction request data to confirm it has not been tampered with and that it contains valid authentication credentials. CyberSource processes the transaction and creates and signs the reply message. The reply message is sent to the customer's browser as an automated HTTPS form POST.

⚠
!
Important
If the reply signature does not match the request signature treat the POST as malicious and disregard it.

---

3 The reply HTTPS POST data contains the transaction result in addition to the masked payment data that was collected outside of your domain. Validate the reply signature to confirm that the reply data has not been tampered with.

If the transaction type is sale, it is immediately submitted for settlement. If the transaction type is authorization, use the CyberSource Simple Order API to submit a capture request when goods are shipped.

4 CyberSource recommends implementing the merchant POST URL notification (see "Receiving Merchant Notifications," page 26) as a backup means of determining the transaction result. This method does not rely on your customer's browser. You receive the transaction result even if your customer lost connection after confirming the payment.

Payment Tokens

> ⚠️ **Important**
>
> Contact CyberSource Customer Support to activate your merchant account for the use of the payment tokenization services. You cannot use payment tokenization services until your account is activated and you have enabled payment tokenization for Secure Acceptance (see "Creating a Silent Order POST Profile," page 17).

Payment tokens are unique identifiers that replace sensitive card information and that cannot be mathematically reversed. CyberSource securely stores all the card information, replacing it with the payment token. The token is also known as a *subscription ID*, which you store on your server.

The payment tokenization solution is compatible with the Visa and Mastercard Account Updater service. All payment information stored with CyberSource is automatically updated by participating banks, thereby reducing payment failures. See the *Account Updater User Guide* (PDF | HTML).

The payment token identifies the card and retrieves the associated billing, shipping, and card information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

Table 2   Types of Payment Tokens

Type	Description
22 digit	The default payment token.
16 digit	Displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 checks.
16 digit	Displays *99* as the two leading digits and passes Luhn mod-10 checks. If your business rules prohibit using 99 as the leading digits, you must modify your system to accept the other 16-digit payment token.

Subscription Payments

A customer subscription contains information that you store in the CyberSource database and use for future billing. At any time, you can send a request to bill the customer for an amount you specify, and CyberSource uses the payment token to retrieve the card, billing, and shipping information to process the transaction. You can also view the customer subscription in the CyberSource Business Center. See "Viewing Transactions in the Business Center," page 55"Viewing Transactions in the Business Center," page 55.

A customer subscription includes:

- Customer contact information, such as billing and shipping information.

- Customer payment information, such as card type, masked account number, and expiration date.

- Customer order information, such as the transaction reference number and merchant-defined data fields.

Table 3   Types of Subscriptions

Type of Subscription	Description
Recurring	A recurring billing service with no specific end date. You must specify the amount and frequency of each payment and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer an online service that the customer subscribes to and can charge a monthly fee for this service. See "Process a Payment Token Transaction," page 42.
Installment	A recurring billing service with a fixed number of scheduled payments. You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer a product for 75.00 and let the customer pay in three installments of 25.00. See "Installment Payments," page 48.

Level II and III Data

Secure Acceptance supports Level II and III data. Level II cards, also know as *Type II cards*, provide customers with additional information on their credit card statements. Business/corporate cards along with purchase/procurement cards are considered Level II cards.

Level III data can be provided for purchase cards, which are credit cards used by employees to make purchases for their company. You provide additional detailed information—the Level III data—about the purchase card order during the settlement process. The Level III data is forwarded to the company that made the purchase, and it enables the company to manage its purchasing activities.

For detailed descriptions of each Level II and Level III API field, see *Level II and Level III Processing Using Secure Acceptance* (PDF | HTML). This guide also describes how to request sale and capture transactions.

Go-Live with Secure Acceptance

> ⚠️
> **Important**
>
> CyberSource recommends that you submit all banking information and required integration services in advance of going live. Doing so will speed up your merchant account configuration.

When you are ready to implement Secure Acceptance in your live environment, you must contact CyberSource Customer Support and request Go-Live. When all the banking information has been received by CyberSource the Go-Live procedure may require three days to complete. No Go-Live implementations take place on a Friday.

Creating a Silent Order POST Profile

⚠️ **Important**	Contact CyberSource Customer Support to enable your account for Secure Acceptance. You must activate a profile in order to use it (see "Activating a Profile," page 30).

To create a Silent Order POST profile:

Step 1   Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com
- Test transactions: https://ebctest.cybersource.com

Step 2   In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3   Enter or check the following profile details.

Table 4   Profile Details

Profile Detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 20 alphanumeric characters.
Description	The profile description cannot exceed 255 characters.
Integration Method	Check **Silent Order POST**.
Company Name	The company name is required and cannot exceed 40 alphanumeric characters.
Company Contact Name	Enter company contact information: name, email, and phone number.
Company Contact Email	
Company Phone Number	
Payment Tokenization	Check **Payment Tokenization**. For more information, see Chapter 5, "Processing Transactions," on page 36.
Decision Manager	Check **Decision Manager**. For more information, see Chapter 4, "Using Decision Manager," on page 34.
Enable Verbose Data	Check **Enable Verbose Data**. For more information, see Chapter 4, "Using Decision Manager," on page 34.
Generate Device Fingerprint	Check **Generate Device Fingerprint**. For more information, see Chapter 4, "Using Decision Manager," on page 34.

Step 4 Click **Create**. The Configuring Payment Settings page appears. See "Configuring Payment Methods" for more information.

Configuring Payment Methods

<table>
<tr><td>

!

Important
</td><td>You must configure at least one payment method before you can activate a profile.</td></tr>
</table>

Adding a Card Type

For each card type you select, you can also manage currencies and payer authentication options. Select only the types of credit cards and currencies that your merchant account provider authorizes.

To add a card type:

Step 1 Click **Payment Settings**. The Payment Settings page appears.

Step 2 Click **Add/Edit Card Types**. The Add/Edit Card Types page appears.

Step 3 Check each card type that you want to offer to the customer as a payment method. The card types must be supported by your payment processor.

Step 4 Click **Update**.

Step 5 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 6 Click **Update**. The card types are added as an accepted payment type.

Step 7 Click **Save**.

Enabling Payer Authentication

![Important] Before you can use CyberSource Payer Authentication, you must contact CyberSource Customer Support to provide information about your company and your acquiring bank so that CyberSource can configure your account. Your merchant ID must be enabled for payer authentication. For more information about Payer Authentication, see "Related Documents," page 10.

Payer authentication is the CyberSource implementation of 3D Secure and deters unauthorized card use and provides added protection from fraudulent chargeback activity.

For Secure Acceptance, CyberSource supports the following kinds of payer authentication:

- American Express SafeKey
- Mastercard SecureCode
- Verified by Visa
- J/Secure by JCB

For each transaction, you receive detailed information in the replies and in the transaction details page of the Business Center. You can store this information for 12 months. CyberSource recommends that you store the payer authentication data because you may be required to display this information as enrollment verification for any payer authentication transaction that you re-present because of a chargeback.

Your merchant account provider may require that you provide all data in human-readable format. Make sure that you can decode the PAReq and PARes.

![Note] The language used on each Payer Authentication page is determined by your issuing bank and overrides the locale you have specified. If you use the test card numbers for testing purposes the default language used on the Payer Authentication page is English and overrides the locale you have specified. See "Testing and Viewing Transactions," page 54.

To configure payer authentication:

Step 1 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 2 Check **Payer Authentication** for each card type that you want to offer to the customer as a payment method. The card types that support payer authentication are:

- Amex
- JCB
- Mastercard

- Maestro (UK Domestic or International)
- Visa

Step 3   Click **Update**.

Adding a Currency

<table>
<tr><td>⚠
Important</td><td>By default, all currencies are listed as disabled. You must select at least one currency. Contact your merchant account provider for a list of supported currencies. If you select the Elo or Hipercard card type, only the Brazilian Real currency is supported.</td></tr>
</table>

To add a supported currency for each card type:

Step 1   Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 2   Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 3   Click **Update**.

Enabling Automatic Authorization Reversals

For transactions that fail to return an Address Verification System (AVS) or a Card Verification Number (CVN) match, you can enable Secure Acceptance to perform an automatic authorization reversal. An automatic reversal releases the reserved funds held against a customer's card.

To enable automatic authorization reversals:

Step 1   Check **Fails AVS check**. Authorization is automatically reversed on a transaction that fails an AVS check.

Step 2   Check **Fails CVN check**. Authorization is automatically reversed on a transaction that fails a CVN check.

Step 3   Click **Save**.

When the AVS and CVN options are disabled and the transaction fails an AVS or CVN check, the customer is notified that the transaction was accepted. You are notified to review the transaction details (see "Types of Notifications," page 123).

Enabling Japanese Payment Options

Configure your profile to process Japanese transactions. For more information, see the request fields: **jpo_payment_method** (jpo_payment_method, page 76) and **jpo_payment_installments** (jpo_payment_installments, page 75).

To enable Japanese payment options:

Step 1   Check **Enable Japanese Payment Options**.

Step 2   Click **Save**.

Enabling eChecks

An eCheck is a payment made directly from your customer's U.S. or Canadian bank account. As part of the checkout process, you must display a terms and conditions statement for eChecks. For more information, see TeleCheck Check Acceptance.

A customer must accept the terms and conditions before submitting an order. Within the terms and conditions statement it is recommended to include a link to the table of returned item fees. The table lists by state the amount that your customer has to pay when a check is returned.

To enable the eCheck payment method:

Step 1   Check **eCheck payments enabled**.

Step 2   Click the pencil icon in the currencies table. The Electronic Check Settings page appears.

Step 3   Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 4   Click **Update**.

Step 5   Click **Save**.

Enabling PayPal Express Checkout

![!] **Important**   PayPal Express Checkout is not supported on a Secure Acceptance iFrame integration.

Contact CyberSource Customer Support to have your CyberSource account configured for this feature. You must also create a PayPal business account; see P*ayPal Express Checkout Services Using the SCMP API* (PDF | HTML) or *PayPal Express Checkout Services Using the Simple Order API* (PDF | HTML).

Add the PayPal Express Checkout payment method to your checkout and redirect the customer to their PayPal account login.When logged into their Paypal account they can review orders, and edit shipping or payment details before completing transactions.

To enable the PayPal Express Checkout payment method:

Step 1   Check **Paypal Express Checkout enabled**.

Step 2   **Allow customers to select or edit their shipping address within PayPal**—check this option to allow customers to edit their shipping address details that were provided in the transaction request to Secure Acceptance. Customers select a new address or edit the address when they are logged in to their PayPal account.

Step 3   When the transaction type is authorization, check one of the following options:

■   **Request a PayPal authorization and include the authorization reply values in the response**—check this option to create and authorize the PayPal order.

![!] **Important**   The customer funds are not captured using this option. You must request a PayPal capture; see P*ayPal Express Checkout Services Using the SCMP API* (PDF | HTML) or *PayPal Express Checkout Services Using the Simple Order API* (PDF | HTML). If the transaction type is **sale**, Secure Acceptance authorizes and captures the customer funds.

■ **Request a PayPal order setup and include the order setup reply values in the response**—check this option to create the PayPal order.

> ⚠️ **Important**
>
> The customer funds are not authorized or captured using this option. You must request a PayPal authorization followed by a PayPal capture request; see P*ayPal Express Checkout Services Using the SCMP API* (PDF | HTML) or *PayPal Express Checkout Services Using the Simple Order API* (PDF | HTML). If the transaction type is **sale**, Secure Acceptance authorizes and captures the customer funds.

Step 4   Click **Save**.

Enabling the Service Fee

> ⚠️ **Important**
>
> Contact CyberSource Customer Support to have your CyberSource account configured for this feature. Service fees are supported only if Wells Fargo is your acquiring bank and FDC Nashville Global is your payment processor.
>
> The service fee setting applies to the card and eCheck payment methods. To apply the service fee to only one payment method, create two Secure Acceptance profiles with the appropriate payment methods enabled on each: one with the service fee feature enabled and one with the service fee feature disabled.

As part of the checkout process, you must display a terms and conditions statement for the service fee. A customer must accept the terms and conditions before submitting an order.

To enable the service fee:

Step 1   Check **Service Fee applies on transactions using this profile**. The service fee terms and conditions URL and the service fee amount are added to the customer review page.

> ⚡ **Warning**
>
> Transactions fail if you disable this feature. Do not disable this feature unless instructed to do so by your account manager.

Step 2   Enter the Consent Page URL.

CyberSource POSTs the order information and the service fee amount to the consent page URL. The customer is directed from your checkout page to the consent page URL to accept or decline the service fee amount. See the *Secure Acceptance Silent Order POST Service Fee Guide* for detailed information.

Step 3   Click **Save**.

> ⚠️
> **Important**
>
> After you save the profile you cannot disable the service fee functionality for that profile. All transactions using the profile will include the service fee amount.

Creating a Security Key

> ⚠️
> **Important**
>
> You must create a security key before you can activate a profile.

> 📝
> **Note**
>
> You cannot use the same security key for both test and live transactions. You must download a security key for both versions of Secure Acceptance:
>
> - For live transactions: https://ebc.cybersource.com
> - For test transactions: https://ebctest.cybersource.com

On the Profile Settings page, click **Security**. The Security Keys page appears. The security script signs the request fields using the secret key and the HMAC SHA256 algorithm. To verify data, the security script generates a signature to compare with the signature returned from the Secure Acceptance server. You must have an active security key to activate a profile. A security key expires in two years and protects each transaction from data tampering.

To create and activate a security key:

Step 1   Click **Security**. The Security page appears.

Step 2   Click **Create New Key**. The Create New Key page appears.

Step 3   Enter a key name (required).

Step 4   Choose signature version **Version 1**.

Step 5   Choose signature method **HMAC-SHA256**.

Step 6   Click **Generate Key**. The Create New Key window expands and displays the new access key and secret key. This window closes after 30 seconds.

Step 7 Copy and save the access key and secret key.

- Access key: Secure Sockets Layer (SSL) authentication with Secure Acceptance Silent Order POST. You can have many access keys per profile. See "Sample Scripting Languages," page 31.

- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See "Sample Scripting Languages," page 31.

⚠ **Important**	Remember to delete the copied keys from your clipboard or cached memory.

By default, the new security key is active. The other options for each security key are:

- Deactivate: deactivates the security key. The security key is inactive.
- Activate: activates an inactive security key.
- View: displays the access key and security key.

✏ **Note**	When you create a security key, it is displayed in the security keys table. You can select a table row to display the access key and the secret key for that specific security key.

Step 8 Click **Return to Profile home**. The Configuring Profile Settings page appears.

Receiving Merchant Notifications

Secure Acceptance sends merchant and customer notifications in response to transactions. You can receive a merchant notification by email or as an HTTPS POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

> ⚠️ **Important**
>
> CyberSource recommends that you implement the merchant POST URL to receive notification of each transaction. You need to parse the transaction response sent to the merchant POST URL and store the data within your systems. This ensures the accuracy of the transactions and informs you if the transaction was successfully processed.

To configure merchant notifications:

Step 1   Click **Notifications**. The Notifications page appears.

Step 2   Choose a merchant notification in one of two ways:

- Check **Merchant POST URL**. Enter the HTTPS URL. CyberSource sends transaction information to this URL. For more information, see "API Reply Fields," page 89.

> ⚠️ **Important**
>
> Only an HTTPS URL should be used for the merchant POST URL. Use port 443 in the URL. Contact CyberSource Customer Support if you encounter any problems.

- Check **Merchant POST Email**. Enter your email address.

> ⚠️ **Important**
>
> CyberSource sends transaction response information to this email address including payment information, return codes, and all relevant order information. See "API Reply Fields," page 89.

Step 3   Choose the card number digits that you want displayed in the merchant or customer receipt:

- Return credit card BIN: displays the card's Bank Identification Number (BIN), which is the first six digits of the card number. All other digits are masked: 123456xxxxxxxxxx

- Return last four digits of credit card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234

- Return BIN and last four digits of credit card number: displays the BIN and the last four digits of the card number. All other digits are masked: 123456xxxxxx1234

Step 4   Continue to configure the customer notifications (see "Sending a Customer Receipt," page 27) or click **Save**. The Profile Settings page appears.

Sending a Customer Receipt

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers may reply with questions regarding their purchases, so use an active email account. The email format is HTML unless your customer email is rich text format (RTF).

Customer Notification Details

To configure customer notifications:

Step 1   Check **Email Receipt to Customer.**

Step 2   Enter the email address to be displayed on the customer receipt. The customer will reply to this email with any queries.

Step 3   Enter the name of your business. It is displayed on the customer receipt.

Step 4   Check **Send a copy to**. This setting is optional.

Step 5   Enter your email address to receive a copy of the customer's receipt.

> **Note**   Your copy of the customer receipt will contain additional transaction response information.

Step 6   Click **Save**. The Configuring Profile Settings page appears.

Company Logo

To add a company logo to the customer receipt and email:

Step 1 Check **Email Receipt to Customer.**

Step 2 Check **Display Notification Logo**.

Step 3 Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email.

> ⚠️
> **Important**
> The logo filename must not contain any special characters, such as a hyphen (-).

Step 4 Click **Save**.

Custom Email Receipt

> ⚠️
> **Important**
> CyberSource recommends that you implement a DNS configuration to enable CyberSource to send email receipts on your behalf.

To create a customer email receipt:

Step 1 Check **Email Receipt to Customer.**

Step 2 Check which email receipt you would like to send to a customer:

- Standard email receipt: this email is automatically translated based on the locale used for the transaction.

- Custom email receipt: this email can be customized with text and data references. The email body section containing the transaction detail appears between the header and footer. Custom text is not translated when using different locales.

    - Check **custom email subject** and enter up to 998 characters. When the maximum amount of characters is exceeded, the subject heading defaults to "*Order Confirmation*".

    You can insert email smart tags to the email subject, header, and footer sections to include specific information. Select each specific smart tag from the drop-down list and click **Insert**.

Step 3   Click **Save**.

Displaying a Response Page

![Important] You must configure the customer response page before you can activate a profile.

Important

You must choose to display a response page to the customer at the end of the checkout process. Enter a URL for your own customer response page. This page is displayed to the customer after the transaction is processed. Review declined orders as soon as possible because you may be able to correct problems related to address or card verification, or you may be able to obtain a verbal authorization. You can also choose to display a web page to the customer after the checkout process is completed.

Transaction Response Page

To display a response page:

Step 1   Click **Customer Response Pages**. The Customer Response Pages page appears

Step 2   Enter the URL for your customer response page. Use port 80, 443, or 8080 in the URL.

![Note] Only port 443 should be used with an HTTPS URL. Parse the results from the URL according to the reason code, and redirect your customer to the appropriate response page. For more information, see "Types of Notifications," page 123.

Note

Step 3   Click Save. The Profile Settings page appears.

Activating a Profile

![Important] You must complete the required settings in each of these sections before activating a profile:

- "Configuring Payment Methods"

- "Creating a Security Key"

- "Displaying a Response Page"

To activate a profile:

Step 1   On the Profile Settings page, click **Promote to Active**. The profile is now active and listed as an active profile on the Manage Profiles page.

![Note] The All Profiles link appears on the Profile Settings page. Click **All Profiles** to view the Manage Profiles list. See "Updating a Secure Acceptance Profile."

Additional Options for a Profile

- Deactivate—deactivates the active profile. The profile is now listed in the inactive profile list. This option is available only for an active profile.

- Create Editable Version—duplicates the active profile and creates an editable version. The editable version is listed in the inactive profile list. This option is available only for an active profile.

- Promote to Active—activates the inactive profile. This option is available only for an inactive profile.

Sample Scripting Languages

Secure Acceptance can support any dynamic scripting language that supports HMAC256 hashing algorithms.

Select to download the sample script for the scripting language that you use:

- JSP
- ASP.NET (C#)
- Ruby
- PHP
- Perl
- VB

Sample Transaction Process Using JSP

1   *signedatafields.jsp* file—paste your access key and profile ID into their respective fields. The customer enters billing, shipping, and other information. POST the fields to your server to sign and create the signature. The fields must be included in the **signed_field_names** field as a CSV list.

2   *security.jsp* file—security algorithm signs fields and creates a signature using the **signed_field_names** field. The security script must be modified to include the Secret Key that you generated on "Creating a Security Key," page 24. Enter your security key in the **SECRET_KEY** field.

The security algorithm in each security script sample is responsible for:

- Request authentication—the signature is generated on the merchant server by the keyed-hash message authentication code (HMAC) signing the request parameters using the shared secret key. This process is also carried out on the Secure Acceptance server, and the two signatures are compared for authenticity.

- Response authentication—the signature is generated on the Secure Acceptance server by HMAC signing the response parameters, using the shared secret key. This process is also carried out on the merchant server, and the two signatures are compared for authenticity.

3   *unsigneddatafields.jsp* file—customer enters their payment information: card type, card number, and card expiry date. Include these fields in the **unsigned_field_names** field. POST the transaction to the Secure Acceptance endpoint.

Updating a Secure Acceptance Profile

Profile status can be active or inactive:

■   Active: the live Secure Acceptance profile. This is your current profile, and it is read-only. You can have more than one active profile.

■   Inactive: the version of a new profile before activation, or the editable version of an active profile. Update and activate this profile to replace the current active profile.

> ⚠️
> **Important**
>
> If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center.

To update a profile:

Step 1   Log in to the Business Center:

■   Live transactions: https://ebc.cybersource.com

■   Test transactions: https://ebctest.cybersource.com

Step 2   In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3   Check the active or inactive profile.

The options for an active profile are:

■   Deactivate: deactivates the active profile. The profile is then listed in the inactive profile list.

■   Edit: select edit and update the active profile. An editable version of the active profile appears in the inactive profile list. To activate this inactive profile, click **Promote to Active**.

■   Copy: duplicates the active profile. The duplicate profile (editable version) is listed in the inactive profile list.

The options for an inactive profile are:

■   Promote to Active: promotes the inactive profile to the active profile list. It replaces the current active profile, and it is removed from the inactive profile list.

■   Delete: deletes the inactive profile.

■   Copy: duplicates the inactive profile. The duplicate profile (editable version) is listed in the inactive profile list.

Note	You can also click the pencil icon to edit an inactive profile.

Step 4   Click **Continue**. The Profile Settings page appears.

Step 5   Update the inactive profile (editable version). See "Updating a Secure Acceptance Profile."

Step 6   Activate the inactive profile. See .

! **Important**	When you activate an inactive profile, it replaces the current active profile and is removed from the inactive profile list on the Manage Profiles page.

Step 7   Click **All Profiles** to view the active and inactive profiles you have created.

! **Important**	If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center and choose **Tools & Settings > Secure Acceptance > Profiles**.

Using Decision Manager

> ⚠️ **Important** Contact CyberSource Customer Support to enable the Decision Manager verbose data mode for your merchant account and for detailed information regarding the device fingerprint.

Decision Manager is a hosted fraud management tool that enables you to identify legitimate orders quickly and that reduces the need to manually intervene in your order review process. You can accurately identify and review potentially risky transactions while minimizing the rejection of valid orders. With Secure Acceptance, you can use Decision Manager to screen orders containing travel data. Include the complete route or the individual legs of the trip, or both. If you include both, the value for the complete route is used.

Decision Manager also obtains data about the geographical location of a customer by linking the IP address extracted from the customer's browser to the country and the credit card. Add the customer's IP address to the **customer_ip_address** field and include it in the request.

Verbose mode returns detailed information about the order, and it returns the decision of each rule that the order triggered. Rules that are evaluated as true are returned with the appropriate results and field names, but rules that are evaluated as false are not returned.

The optional decision manager fields are:

- consumer_id
- complete_route
- customer_cookies_accepted
- customer_gift_wrap
- customer_ip_address
- departure_time
- date_of_birth
- device_fingerprint_id—the CyberSource-generated device fingerprint ID overrides the merchant-generated device fingerprint ID. See device_fingerprint_id, page 67.
- journey_leg#_orig
- journey_leg#_dest
- journey_type

- merchant_defined_data#

- item_#_passenger_forename

- item_#_passenger_email

- item_#_passenger_id

- item_#_passenger_surname

- item_#_passenger_status

- item_#_passenger_type

- returns_accepted

For detailed descriptions of all request fields, see "Request-Level Fields," page 58. For detailed descriptions of all the Decision Manager reply fields, see *Decision Manager Developer Guide Using the SCMP API* (PDF | HTML).

Processing Transactions

Endpoints and Transaction Types

Table 5 **Endpoints**

Process Transaction Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/silent/pay
Live Transactions	https://secureacceptance.cybersource.com/silent/pay
Supported transaction types	■ authorization
	■ authorization,create_payment_token
	■ authorization,update_payment_token
	■ sale
	■ sale,create_payment_token
	■ sale,update_payment_token

Create Payment Token Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/silent/token/create
Live Transactions	https://secureacceptance.cybersource.com/silent/token/create
Supported transaction type	create_payment_token

Update Payment Token Endpoints

Test Transactions	https://testsecureacceptance.cybersource.com/silent/token/update
Live Transactions	https://secureacceptance.cybersource.com/silent/token/update
Supported transaction type	update_payment_token

iFrame Transaction Endpoints (see "iFrame Implementation," page 127).

Test Transactions	https://testsecureacceptance.cybersource.com/silent/embedded/pay
Live Transactions	https://secureacceptance.cybersource.com/silent/embedded/pay

Table 5 Endpoints (Continued)

Supported transaction type	■ authorization
	■ authorization,create_payment_token
	■ authorization,update_payment_token
	■ sale
	■ sale,create_payment_token
	■ sale,update_payment_token
iFrame Create Payment Token Endpoints (see "iFrame Implementation," page 127).	
Test Transactions	https://testsecureacceptance.cybersource.com/silent/embedded/token/create
Live Transactions	https://secureacceptance.cybersource.com/silent/embedded/token/create
Supported transaction type	create_payment_token
iFrame Update Payment Token Endpoints (see "iFrame Implementation," page 127).	
Test Transactions	https://testsecureacceptance.cybersource.com/silent/embedded/token/update
Live Transactions	https://secureacceptance.cybersource.com/silent/embedded/token/update
Supported transaction type	update_payment_token

Create a Payment Token

Credit Card

> ⚠️ **Important**
>
> Include the appropriate endpoint that supports the **create_payment_token** transaction type (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.

> 📝 **Note**
>
> Include all request fields in the **signed_field_names** field with the exception of the **card_number** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 1   Request: Create a standalone payment token

```
reference_number=123456789
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_city=Mountain View
bill_to_address_postal_code=94043
bill_to_address_state=CA
bill_to_address_country=US
```

Example 2   Reply: Create a standalone payment token

```
req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_amount=100.00
req_payment_method=card
req_card_type=001
req_card_number=xxxxxxxxxxxx1111
req_card_expiry_date=12-2022
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_city=Mountain View
req_bill_to_address_postal_code=94043
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=3529893314302230706689
```

eCheck

![!] **Important**
Include the appropriate endpoint that supports the **create_payment_token** transaction type (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.

![pencil] **Note**
Include all request fields in the **signed_field_names** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

Example 3   Request: Create standalone payment token

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=create_payment_token
amount=100.00
locale=en
reference_number=1730560013735542024294683
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_postal_code=94043
bill_to_address_country=US
payment_method=echeck
driver_license_state=NY
driver_license_number=34-78239-396
date_of_birth=19901001
echeck_account_type=c
company_tax_id=123456789
echeck_sec_code=WEB
echeck_account_number=452894100
echeck_routing_number=672302882
```

Example 4   Reply: Create a standalone payment token

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_amount=100.00
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=create_payment_token
req_echeck_account_type=c
signature=NuxlJilx5YbvKoXlt0baB5hUj5gk4+OozqJnyVF390s=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-07-11T15:11:41Z
req_currency=USD
req_reference_number=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
req_payment_token=3529893314302130706689
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

Process a Payment Token Transaction

Credit Card

⚠️ **Important**   Include the appropriate endpoint that supports the **authorization** or **sale** transaction types (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.

📝 **Note**   The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information

Example 5   Request: Card Transaction

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=3427075830000181552556
consumer_id=1239874561
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Example 6   Reply: One-Click Transaction

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
```

```
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

eCheck

!	Include the appropriate endpoint that supports the **authorization** or **sale** transaction types (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.
Important	

	The **payment_token** field identifies the echeck account details and retrieves the associated billing, shipping, and payment information
Note	

Example 7   Request: Process eCheck Payment Token

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
transaction_type=sale
currency=USD
amount=100.00
locale=en
payment_token=3644783643210170561946
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Example 8   Reply: Process eCheck Payment Token

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=sale
req_echeck_account_type=c
signature=ZUk7d99c/yb+kidvVUbz10JtykmjOt8LMPgkllRaZR8=
req_locale=en
reason_code=100
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
signed_date_time=2013-06-12T09:59:50Z
req_currency=USD
req_reference_number=77353001371031080772693
req_echeck_routing_number=xxxxx2882
transaction_id=3710311877042130706689
req_amount=100.00
message=Request was processed successfully.
echeck_debit_ref_no=1
echeck_debit_submit_time=2013-03-25T104341Z
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=123456789
req_transaction_uuid=bdc596506c2677b79133c9705e5cf77c
req_bill_to_surname=Smith
req_bill_to_forename=Joe
req_bill_to_email=jsmith@example.com
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
```

Recurring Payments

You must specify the amount and frequency of each payment and the start date for processing recurring payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

![!] **Important**   Include the appropriate endpoint that supports the **authorization,create_payment_token** or **sale,create_payment_token** transaction types (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.

![!] **Important**   The **amount** field is an optional field that indicates the setup fee for processing recurring payments.

Example 9   Request: Create payment token for recurring payments

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
locale=en
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=1239874561
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_amount=25.00
payment_method=card
```

Example 10   Reply: Create payment token for recurring payments

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_tax_amount=2.50
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Installment Payments

You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

Include the appropriate endpoint that supports the **authorization,create_payment_token** or **sale,create_payment_token** transaction types (see "Endpoints and Transaction Types," page 36). For descriptions of all request and reply fields, see "API Fields," page 57.

The **amount** field is an optional field that indicates the setup fee for processing recurring payments. To charge this fee, include the **amount** field and ensure that the **transaction_type** field is set to **authorization,create_payment_token** or **sale,create_payment_token**.

Example 11   Request: Create payment token for installment payments

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
amount=5.00
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=1239874561
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
payment_method=card
```

Example 12 Reply: Create payment token for installment payments

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_number_of_installments=6
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Update a Payment Token

Credit Card

The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information.

<table>
<tr>
<td>

!

Important

</td>
<td>

Include the endpoint that supports **update_payment_token** or the endpoint that supports **authorization,update_payment_token** (updates the token and authorizes the transaction) or **sale,update_payment_token** (updates the token and processes the transaction). See You must include the **allow_ payment_token_update** field and set it to **true**.

</td>
</tr>
</table>

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=3427075830000181552556
amount=100.00
currency=USD
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
consumer_id=1239874561
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Example 13   Reply: Updating a Payment Token for a Card

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

eCheck

The **payment_token** field identifies the eCheck account and retrieves the associated billing, shipping, and payment information.

> ⚠️ **Important**   Include the endpoint that supports **update_payment_token** or the endpoint that supports **sale,update_payment_token** (updates the token and processes the transaction). See You must include the **allow_payment_token_update** field and set to **true**.

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1845864013783060468573616
currency=USD
amount=100.00
locale=en
payment_token=3644783643210170561946
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
unsigned_field_names=comma separated list of unsigned fields
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
payment_method=echeck
driver_license_state=NY
driver_license_number=34-78239-396
date_of_birth=19901001
echeck_account_type=c
company_tax_id=123456789
echeck_sec_code=WEB
echeck_account_number=452894100
echeck_routing_number=672302882
```

Example 14   Reply: Updating eCheck Payment Token

```
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=sale,update_payment_token
req_echeck_account_type=c
signature=NuxlJilx5YbvKoXlt0baB5hUj5gk4+OozqJnyVF390s=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-07-11T15:11:41Z
req_currency=USD
req_reference_number=1730560013735542024294683
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
payment_token=3529893314302130706689
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

Testing and Viewing Transactions

![Important] **Important**   You must create a profile in both the test and live versions of Secure Acceptance Silent Order POST. You cannot copy a profile from the test version to the live version. You must recreate the profile.

Testing Transactions

To test Secure Acceptance Silent Order POST transactions:

Step 1   Log in to the Test Business Center: https://ebctest.cybersource.com

Step 2   Create a Secure Acceptance Silent Order POST profile. See Chapter 2, "Creating a Silent Order POST Profile," on page 17.

Step 3   Integrate with Secure Acceptance Silent Order POST. See "Sample Scripting Languages," page 31.

![Important] **Important**   Include the test transactions endpoint in your HTML form. See "Sample Transaction Process Using JSP," page 31.

Step 4   You may use the following test credit card numbers for transactions:

Credit Card Type	Test Account Number
Visa	4111111111111111
Mastercard	5555555555554444
American Express	378282246310005
Discover	6011111111111117
JCB	3566111111111113
Diners Club	38000000000006
Maestro International (16 digits)	6000340000009859

Maestro Domestic (16 digits)	6759180000005546

To simulate processor-specific error messages, choose your payment processor here:

http://www.cybersource.com/developers/test_and_manage/testing/legacy_scmp_api/

Viewing Transactions in the Business Center

To view a transaction in the Business Center:

Step 1 Log in to the Business Center:

- Live transactions: https://ebc.cybersource.com
- Test transactions: https://ebctest.cybersource.com

Step 2 In the left navigation panel, choose **Transaction Search > Secure Acceptance Search**. The Secure Acceptance Search page appears. The search options are:

- Account suffix
- Cardholder's surname
- Merchant reference number
- Request ID

Step 3 Select the date range for your search. The dates can range from the current day to a maximum of 6 months past.

Step 4 Select the number of results to be displayed, from 10 to 100 transactions per page.

Step 5 Click **Search**. The Secure Acceptance Transaction Search Results page appears.

> ! **Important**
> If a transaction has missing or invalid data, it is displayed in the Secure Acceptance Transaction Search Results page without a request ID link.

Step 6   The additional search options for each transaction are:

- Click the **request ID** link of the transaction. The Transaction Search Details page appears.

- Click the magnifying glass icon in the Log column for each transaction. The Secure Acceptance Transaction Search Details page appears. The search results are:

  - Summary information—includes the merchant ID, request ID, profile ID, the transaction decision, and the message for the transaction.

  - Request log—includes all the request API fields for the transaction.

  - Reply log—includes all the reply API fields for the transaction.

API Fields

Data Type Definitions

> ⚠️ **Important** Unless otherwise noted, all fields are order and case sensitive. CyberSource recommends that you not include URL encoded characters in any request field prior to generating a signature.

Data Type	Permitted Characters and Formats
Alpha	Any letter from any language.
AlphaNumeric	Alpha with any numeric character in any script.
AlphaNumericPunctuation	AlphaNumeric including !"#$%&'()*+,-./:;=?@^_~
Amount	0123456789 including a decimal point (.)
ASCIIAlphaNumericPunctuation	Any ASCII alphanumeric character including !"#$%&'()*+,-.\\/:;=?@^_~
Date (a)	MM-YYYY
Date (b)	YYYYMMDD
Date (c)	yyyy-MM-dd HH:mm z yyyy-MM-dd hh:mm a z yyyy-MM-dd hh:mma z
Email	Valid email address.
Enumerated String	Comma-separated alphanumeric string.
IP	Valid IP address.
ISO 8601 Date	YYYY-MM-DDThh:mm:ssZ
Locale	[a-z] including a hyphen (-)
Numeric	0123456789
Phone	(),+-.*#xX1234567890
URL	Valid URL (http or https).

Request-Level Fields

![Important]	When generating the security signature, create a comma-separated *name*=*value* string of the POST fields that are included in the **signed_field_ names** field. The ordering of the fields in the string is critical to the signature generation process. For example:
Important	

- bill_to_forename=john

- bill_to_surname=doe

- bill_to_email=jdoe@example.com

- signed_field_names=bill_to_forename,bill_to_email,bill_to_surname

The string to sign is "bill_to_forename=john,bill_to_ email=jdoe@example.com,bill_to_surname =doe"

For information on the signature generation process, see the security script of the sample code for the scripting language you are using. See "Sample Scripting Languages," page 31.

![Note]	For data type definitions and permitted characters, see "Data Type Definitions," page 57.
Note	

Table 6   API Request Fields

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
access_key	Required for authentication with Secure Acceptance. See "Creating a Security Key," page 24.	Required by the Secure Acceptance application.	Alphanumeric String (32)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
aggregator_id	Value that identifies you as a payment aggregator. Obtain this value for the processor. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 95-105 ■ Field: Mastercard Payment Facilitator ID ***FDC Compass*** This value must consist of upper-case characters. ***Field Length*** American Express Direct: 20 CyberSource through VisaNet: 11 FDC Compass: 20 FDC Nashville Global: 15 ***Required/Optional*** American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: R for Mastercard aggregator authorizations; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	authorization (See description)	String (See description)
allow_payment_ token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: ■ true: customer can update details. ■ false: customer cannot update details.	update_payment_token (R)	Enumerated String String (5)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
amount	Total amount for the order. Must be greater than or equal to zero and must equal the total amount of each line item including the tax amount.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Amount String (15)
auth_indicator	Flag that specifies the purpose of the authorization. Possible values: ■ 0: Preauthorization ■ 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the default for this field, contact CyberSource Customer Support.	authorization (See description)	String (1)
bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: ■ true: bill payment or loan payment. ■ false (default): not a bill payment or loan payment.	This field is optional.	Enumerated String String (5)
bill_to_address_city	City in the billing address.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation Atos: String (32) All other processors: String (50)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_ country	Country code for the billing address. Use the two-character ISO country codes.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Alpha String (2)
bill_to_address_ line1	First line of the billing address. **Note** On JCN Gateway, this field is required when the authorization or sale request includes create_ payment_token or Decision Manager. This field is optional when requesting an authorization or a sale without create_payment_token or Decision Manager.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation Atos: String (29) CyberSource through VisaNet: String (40) Litle: String (35) Moneris: String (50) All other processors: String (60)
bill_to_address_ line2	Second line of the billing address.	This field is optional.	AlphaNumericPunctuation Atos: String (29) CyberSource through VisaNet: String (40) Litle: String (35) Moneris: String (50) All other processors: String (60)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_address_ postal_code	Postal code for the billing address. **Note** This field is required if **bill_ to_address_country** is US or CA. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] **Example** A1B 2C3 For the rest of the world countries, the maximum length is 10.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_ payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	AlphaNumericPunctuation See description.
bill_to_address_ state	State or province in the billing address. Use the two-character ISO state and province code. **Note** This field is required for U.S. and Canada.	See description.	AlphaNumericPunctuation String (2 for U.S. and Canada, otherwise 60)
bill_to_company_ name	Name of the customer's company.	This field is optional.	AlphaNumericPunctuation String (40)
bill_to_email	Customer email address, including the full domain name.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_ payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	Email String (255)
bill_to_forename	Customer first name. This name must be the same as the name on the card.	▪ create_payment_token (R) ▪ authorization or sale (R) ▪ authorization,create_ payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	AlphaNumericPunctuation String (60)

Table 6 API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
bill_to_phone	Customer phone number. CyberSource recommends that you include the country code if the order is from outside the U.S. **Note** This field is optional for card payments. For eCheck payments this field is required if your processor is CyberSource ACH Service or Telecheck.	See description.	Phone String (6 to 15) String (10) if using Telecheck for echeck payments.
bill_to_surname	Customer last name. This name must be the same as the name on the card.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	AlphaNumericPunctuation String (60)
card_cvn	Card verification number. **Important** For American Express card types, the cvn must be 4 digits. This field can be configured as required or optional. See "Configuring Payment Methods," page 18.	See description.	Numeric String (4)
card_expiry_date	Card expiration date. Format: MM-YYYY	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Date (a) String (7)
card_number	Card number. **Important** Use only numeric values. Make sure that you include valid and well formed data for this field.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric String (20)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_type	Type of card to authorize. Use one of these values: 001: Visa 002: Mastercard 003: American Express 004: Discover 005: Diners Club: cards starting with 54 or 55 are rejected. 006: Carte Blanche 007: JCB 014: EnRoute 021: JAL 024: Maestro UK Domestic 027: Nicos 031: Delta 033: Visa Electron 034: Dankort 036: Carte Bleue 037: Carta Si 042: Maestro International 043: GE Money UK card 050: Hipercard (sale only) 053: Orico 054: Elo 055: Private Label	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Enumerated String String (3)
company_tax_id	Company's tax identifier. **Note** Contact your TeleCheck representative to find out whether this field is required or optional.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	AlphaNumericPunctuation String (9)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
complete_route	Concatenation of individual travel legs in the format for example: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_ route** takes precedence over that of the **journey_leg#** fields.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	AlphaNumericPunctuation String (255)
conditions_ accepted	Indicates whether the customer accepted the service few amount. Possible values: ■ false: the customer did not accept. ■ true: the customer did accept.	This is a required field if service fee is enabled for the profile. See "Enabling the Service Fee," page 23.	Enumerated String String (5)
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	■ create_payment_token (O) ■ authorization,create_ payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O)	AlphaNumericPunctuation String (100)
currency	Currency used for the order. For the possible values, see the ISO currency codes.	■ create_payment_token (R) ■ authorization or sale (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Alpha String (3)
customer_ cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ■ true: customer browser accepts cookies. ■ false: customer browser does not accept cookies.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Enumerated String String (5)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_gift_ wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: ■ true: customer requested gift wrapping. ■ false: customer did not request gift wrapping.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Enumerated String String (5)
customer_ip_ address	Customer's IP address reported by your web server via socket information.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	IP String (15)
date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Date (b) String (8)
debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: ■ false (default): not a loan payment ■ true: loan payment	This field is optional.	Enumerated String String (5)
departure_time	Departure date and time of the first leg of the trip. Use one of the following formats: yyyy-MM-dd HH:mm z (2014-01-20 11:30 GMT) yyyy-MM-dd hh:mm a z (2014-01-20 11:30 PM GMT) yyyy-MM-dd hh:mma z (2014-01-20 11:30pm GMT) HH = 24-hour format hh = 12-hour format a = am or pm (case insensitive) z = time zone of the departing flight.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Date (c) DateTime (29)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
device_fingerprint_ id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_) However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID. **Important** The CyberSource generated device fingerprint ID overrides the merchant generated device fingerprint ID. See Chapter 4, "Using Decision Manager," on page 34.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	AlphaNumericPunctuation String (88)
driver_license_ number	Driver's license number of the customer. Contact your TeleCheck representative to find out whether this field is required or optional. If you include this field in your request then you must also include the **driver_license_state** field.	▪ sale (See description) ▪ create_payment_token (See description) ▪ sale,create_payment_token (See description) ▪ update_payment_token (See description)	AlphaNumeric String (30)
driver_license_ state	State or province from which the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*. Contact your TeleCheck representative to find out whether this field is required or optional.	▪ sale (See description) ▪ create_payment_token (See description) ▪ sale,create_payment_token (See description) ▪ update_payment_token (See description)	Alpha String (2)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
e_commerce_indicator	The commerce indicator for the transaction type. Value: install **Note** This field is required only for installment payments using the CyberSource Latin American Processing connection.	▪ authorization (See description)	String (20)
echeck_account_number	Account number.	▪ sale (R) ▪ create_payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	Numeric Non-negative integer (8 to 17)
echeck_account_type	Account type. Possible values: ▪ C: checking ▪ S: savings (USD only) ▪ X: corporate checking (USD only) ▪ G: General Ledger	▪ sale (R) ▪ create_payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	Enumerated String String (1)
echeck_check_number	Check number. **Note** If your payment processor is TeleCheck we recommend that you include this field.	▪ sale (See description) ▪ create_payment_token (See description) ▪ sale,create_payment_token (See description) ▪ update_payment_token (See description)	Numeric Integer (8)
echeck_effective_date	The postdate for the transaction. This date must be within 45 days of the current date. Use the format: MMDDYYYY	▪ sale (O) ▪ sale,create_payment_token (O)	Date (b) String (8)
echeck_routing_number	Bank routing number. If the currency being used is CAD, the maximum length of the routing number is 8 digits. If the currency being used is USD, the maximum length of the routing number is 9 digits.	▪ sale (R) ▪ create_payment_token (R) ▪ sale,create_payment_token (R) ▪ update_payment_token (O)	Numeric Non-negative integer (See description)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
echeck_sec_code	If you payment processor is TeleCheck then this field is required. Possible values: CCD: Corporate cash disbursement—charge or credit against a business checking account. You can use one-time or recurring CCD transactions to transfer funds to or from a corporate entity. A standing authorization is required for recurring transactions. PPD: Prearranged payment and deposit entry—charge or credit against a personal checking or savings account. You can originate a PPD entry only when the payment and deposit terms between you and the customer are prearranged. A written authorization from the customer is required for one-time transactions and a written standing authorization is required for recurring transactions. TEL: Telephone-initiated entry— one-time charge against a personal checking or savings account. You can originate a TEL entry only when there is a business relationship between you and the customer or when the customer initiates a telephone call to you. For a TEL entry, you must obtain an authorization from the customer over the telephone. WEB: Internet-initiated entry— charge against a personal checking or savings account. You can originate a one-time or recurring WEB entry when the customer initiates the transaction over the Internet. You must obtain an authorization from the customer over the Internet.	■ sale (See description) ■ create_payment_token (See description) ■ sale,create_payment_token (See description) ■ update_payment_token (See description)	Enumerated String String (3)

Table 6 API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends that you include this field within the **signed_field_ names** field when generating a signature.	This field is optional.	Enumerated String String (5)
ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends that you include this field within the **signed_field_ names** field when generating a signature.	This field is optional.	Enumerated String String (5)
installment_ amount	Amount for the current installment payment. **Note** This field is required only for installment payments using the CyberSource Latin American Processing or CyberSource through VisaNet connections.	authorization (See description)	Amount (12)
installment_ frequency	Frequency of the installment payments. Possible values: ■ B: Biweekly ■ M: Monthly ■ W: Weekly **Note** This field is supported only for the CyberSource through VisaNet connection.	authorization (See description)	AlphaNumeric (2)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_plan_ type	Flag that indicates the type of funding for the installment plan associated with the payment. Possible values: ■ 1: Merchant-funded installment plan ■ 2: Issuer-funded installment plan If you do not include this field in the request, CyberSource uses the value in your CyberSource account. To change this value contact CyberSource Customer Service. ***CyberSource through VisaNet*** American Express-defined code that indicates the type of installment plan for this transaction. Contact American Express for: ■ Information about the types of installment plans that American Express provides ■ Values for this field	authorization (See description)	CyberSource Latin American Processing: String (1) CyberSource through VisaNet: String (2)
installment_ sequence	Installment number when making payments in installments. Used along with **installment_total_ count** to keep track of which payment is being processed. For example, the second of 5 payments would be passed to CyberSource as **installment_sequence** = 2 and **installment_total_count** = 5. **Note** This field is required only for installment payments using the CyberSource through VisaNet connection.	authorization (See description)	Integer (2)
installment_total_ amount	Total amount of the loan that is being paid in installments. **Note** This field is required only for installment payments using CyberSource Latin American Processing or CyberSource through VisaNet connections.	authorization (see description)	Amount (12)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_total_ count	Total number of installment payments as part of an authorization. Possible values: 1 to 99 **Note** This field is required only for installment payments using the CyberSource Latin American Processing connection.	authorization (See description)	Numeric String (2)
issuer_additional_ data	Data defined by the issuer. See the "Formats for Discretionary Data" section in *Credit Card Services Using the SCMP API* or *Credit Card Services Using the Simple Order API*.	authorization (O)	Alphanumeric String (256)
item_#_code	Type of product. # can range from 0 to 199.	This field is optional. If you include this field, you must also include the **line_ item_count** field.	AlphaNumericPunctuation String (255)
item_#_name	Name of the item. # can range from 0 to 199. **Note** This field is required when the **item_#_code** value is not default or relating to shipping or handling.	See description. If you include this field, you must also include the **line_ item_count** field.	AlphaNumericPunctuation String (255)
item_#_ passenger_email	Passenger's email address.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (255)
item_#_ passenger_ forename	Passenger's first name.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (60)
item_#_ passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (32)
item_#_ passenger_phone	Passenger's phone number. If the order is from outside the U.S., CyberSource recommends that you include the country code.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (15)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_ passenger_status	Your company's passenger classification, such as with a frequent flyer classification. In this case, you might use values such as standard, gold, or platinum.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (32)
item_#_ passenger_ surname	Passenger's last name.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (60)
item_#_ passenger_type	Passenger classification associated with the price of the ticket. You can use one of the following values: ■ ADT: Adult ■ CNN: Child ■ INF: Infant ■ YTH: Youth ■ STU: Student ■ SCR: Senior Citizen ■ MIL: Military	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	String (32)
item_#_quantity	Quantity of line items. The default value is 1. Required field if one of the following product codes is used: ■ adult_content ■ coupon ■ electronic_good ■ electronic_software ■ gift_certificate ■ service ■ subscription # can range from 1 to 199. **Note** This field is required when the **item_#_code** value is not default or relating to shipping or handling.	See description. If you include this field, you must also include the **line_ item_count** field.	Numeric String (10)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_sku	Identification code for the product. Required field if one of the following product codes is used: ■ adult_content ■ coupon ■ electronic_good ■ electronic_software ■ gift_certificate ■ service ■ subscription # can range from 0 to 199.	See description. If you include this field, you must also include the **line_item_count** field.	AlphaNumericPunctuation String (255)
item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	This field is optional. If you include this field, you must also include the **line_item_count** field.	Amount String (15)
item_#_unit_price	Price of the line item. # can range from 0 to 199. This value cannot be negative. You must include either this field or the **amount** field in the request.	See description. If you include this field, you must also include the **line_item_count** field.	Amount String (15)
journey_leg#_dest	Airport code for the destination leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Alpha String (3)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_leg#_orig	Airport code for the origin leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Alpha String (3)
journey_type	Type of travel, such as: one way or round trip.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	AlphaNumericPunctuation String (32)
jpo_payment_ installments	Total number of Japanese installment payments. Possible values: ▪ 2 ▪ 3 ▪ 5 ▪ 6 ▪ 10 ▪ 12 ▪ 15 ▪ 18 ▪ 20 ▪ 24	This field is required when the **jpo_payment_method** value is 4 and the currency type is JPY.	Numeric String (2)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
jpo_payment_ method	Japanese payment method. Possible values: ■ 1: single payment ■ 2: bonus payment ■ 4: installment payment ■ 5: revolving repayment **Important** This field is only valid when the currency type is JPY.		Numeric String (1)
line_item_count	Total number of line items. Maximum number is 200.	This field is required when you include any item fields in the request.	Numeric String (2)
locale	Indicates the language to use for customer-facing content. Possible value: en-us. See "Activating a Profile," page 30.	Required by the Secure Acceptance application.	Locale String (5)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_defined_ data#	Optional fields that you can use to store information (see "Custom Email Receipt," page 28). # can range from 1 to 100. Merchant defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant-defined data fields 5 to 100 are passed trough to Decision Manager as part of the initial payment request and are not stored against the payment token. **Important** Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields and any Secure Acceptance field that is not specifically designed to capture personally identifying information. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	AlphaNumericPunctuation String (100)

Table 6 API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_ descriptor merchant_ descriptor_ alternate merchant_ descriptor_city merchant_ descriptor_contact merchant_ descriptor_country merchant_ descriptor_state merchant_ descriptor_postal_ code merchant_ descriptor_street	For the descriptions, used-by information, data types, and lengths for these fields, see the Merchant Descriptors section in either *Credit Card Services Using the SCMP API* or *Credit Card Services Using the Simple Order API*.	authorization (See description)	
merchant_secure_ data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	This field is optional.	AlphaNumericPunctuation String (2000)
merchant_secure_ data1 merchant_secure_ data2 merchant_secure_ data3	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	This field is optional.	AlphaNumericPunctuation String (100)
override_ backoffice_post_ url	Overrides the backoffice post URL profile setting with your own URL.	This field is optional.	URL String (255)
override_custom_ cancel_page	Overrides the custom cancel page profile setting with your own URL.	This field is optional.	URL String (255)
override_custom_ receipt_page	Overrides the custom receipt profile setting with your own URL. **Important** CyberSource recommends signing this field.	This field is optional.	URL String (255)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
override_paypal_ order_setup	Overrides the paypal order setup profile setting. Possible values: ■ include_authorization: the paypal order is created and authorized. ■ exclude_authorization: the paypal order is created but not authorized.	This field is optional. See "Enabling PayPal Express Checkout," page 22.	String (21)
payment_method	Method of payment. Possible values: ■ card ■ echeck ■ paypal	Required by the Secure Acceptance application.	Enumerated String String (30)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. When this field is included in the request, the card data, and billing and shipping information are optional. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID. **Note** This field is required for token-based transactions.	■ authorization or sale (R) ■ authorization,update_ payment_token (R) ■ sale,update_payment_token (R) ■ update_payment_token (R)	Numeric String (26)
payment_token_ comments	Optional comments you have for the customer subscription.	This field is optional.	AlphaNumericPunctuation String (255)
payment_token_ title	Name or title for the customer subscription.	This field is optional.	AlphaNumericPunctuation String (60)
profile_id	Identifies the profile to use with each transaction.	Assigned by the Secure Acceptance application.	ASCIIAlphaNumericPunct uation String (36)
recipient_account_ id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	authorization (R for recipient transactions, otherwise not used)	Numeric String (10)
recipient_date_of_ birth	Recipient's date of birth. Format: YYYYMMDD.	authorization (R for recipient transactions, otherwise not used)	Date (b) String (8)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recipient_postal_code	Partial postal code for the recipient's address. For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.	authorization (R for recipient transactions, otherwise not used)	Alphanumeric String (6)
recipient_surname	Recipient's last name.	authorization (R for recipient transactions, otherwise not used)	Alpha String (6)
recurring_amount	Payment amount for each installment or recurring subscription payment.	■ create_payment_token (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Amount String (15)
recurring_ automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: ■ true (default): automatically renew. ■ false: do not automatically renew.	■ create_payment_token (O) ■ authorization,create_ payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O)	Enumerated String String (5)
recurring_ frequency	Frequency of payments for an installment or recurring subscription. Possible values: ■ weekly: every 7 days. ■ bi-weekly: every 2 weeks. ■ quad-weekly: every 4 weeks. ■ monthly ■ semi-monthly: twice every month (1st and 15th). ■ quarterly ■ semi-annually: twice every year. ■ annually	■ create_payment_token (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Enumerated String String (20)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recurring_number_ of_installments	Total number of payments set up for an installment subscription. Maximum values: ■ 261: weekly ■ 130: bi-weekly ■ 65: quad-weekly ■ 60: monthly ■ 120: semi-monthly ■ 20: quarterly ■ 10: semi-annually ■ 5: annually	■ create_payment_token (R) ■ authorization,create_ payment_token (R) ■ sale,create_payment_token (R) ■ update_payment_token (O)	Numeric String (3)
recurring_start_ date	First payment date for an installment or recurring subscription payment. Date must use the format YYYYMMDD. If a date in the past is supplied, the start date defaults to the day after the date that was entered.	■ create_payment_token (O) ■ authorization,create_ payment_token (O) ■ sale,create_payment_token (O) ■ update_payment_token (O)	Date (b) String (8)
reference_number	Unique merchant-generated order reference or tracking number for each transaction.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Asia, Middle East, and Africa Gateway: String (40) Atos: String (32) All other processors: String (50)
returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: ■ true ■ false	This field is optional. See Chapter 4, "Using Decision Manager," on page 34.	Enumerated String String (5)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
sales_ organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 106-116 ■ Field: Mastercard Independent Sales Organization ID	authorization (Required for Mastercard aggregator transactions on CyberSource through VisaNet)	Nonnegative integer (11)
ship_to_address_ city	City of shipping address.	This field is optional.	AlphaNumericPunctuation String (50)
ship_to_address_ country	Country code for the shipping address. Use the two-character ISO country codes.	This field is optional.	Alpha String (2)
ship_to_address_ line1	First line of shipping address.	This field is optional.	AlphaNumericPunctuation String (60)
ship_to_address_ line2	Second line of shipping address.	This field is optional.	AlphaNumericPunctuation String (60)
ship_to_address_ postal_code	Postal code for the shipping address. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] **Example** A1B 2C3 For the rest of the world countries, the maximum length is 10.	This field is optional.	AlphaNumericPunctuation See description.

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_ state	State or province of shipping address. Use the two-character ISO state and province codes. **Note** This field is required if the shipping address value is U.S. and Canada.	This field is optional.	AlphaNumericPunctuation String (2)
ship_to_company_ name	Name of the company receiving the product.	This field is optional.	AlphaNumericPunctuation String (40)
ship_to_forename	First name of the person receiving the product.	This field is optional.	AlphaNumericPunctuation String (60)
ship_to_phone	Phone number of the shipping address.	This field is optional.	Phone String (6 to 15)
ship_to_surname	Last name of the person receiving the product.	This field is optional.	AlphaNumericPunctuation String (60)
shipping_method	Shipping method for the product. Possible values: ■ sameday：courier or same-day service ■ oneday：next day or overnight service ■ twoday：two-day service ■ threeday：three-day service ■ lowcost：lowest-cost service ■ pickup：store pick-up ■ other：other shipping method ■ none：no shipping method	This field is optional.	Enumerated String String (10)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the **access_ key** field supplied.	Required by the Secure Acceptance application.	AlphaNumericPunctuation

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
signed_date_time	The date and time that the signature was generated. Must be in UTC Date & Time format. This field is used to check for duplicate transaction attempts. Format: YYYY-MM-DDThh:mm:ssZ Example 2016-08-11T22:47:57Z equals August 11, 2016, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC. Your system time must be accurate to avoid payment processing errors related to the **signed_date_time** field.	Required by the Secure Acceptance application.	ISO 8601 Date String (20)
signed_field_ names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. All request fields should be signed to prevent data tampering, with the exception of the **card_number** field and the signature field.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable
skip_bin_lookup	Indicates whether to skip the BIN lookup service. See "Enabling eChecks," page 21. This field can contain one of the following values: ■ true ■ false	This field is optional.	Enumerated String String (5)
skip_decision_ manager	Indicates whether to skip Decision Manager. See Chapter 4, "Using Decision Manager," on page 34. This field can contain one of the following values: ■ true (decision manager is not enabled for this transaction and the device fingerprint id will not be displayed) ■ false	This field is optional.	Enumerated String String (5)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_city	Sub-merchant's city. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (15) FDC Compass: String (21) FDC Nashville Global: String (11)
submerchant_ country	Sub-merchant's country. Use the two-character *ISO Standard Country Codes*. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (3)
submerchant_ email	Sub-merchant's email address. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 25-64 ■ Field: American Express Seller E-mail Address	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: O for all aggregator transactions with American Express; otherwise, not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (40) CyberSource through VisaNet: String (40) FDC Compass: String (40) FDC Nashville Global: String (19)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_id	The ID you assigned to your sub-merchant. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 65-84 ■ Field: American Express Seller ID With Mastercard, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 117-131 ■ Field: Mastercard Sub-Merchant ID ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: ■ O for all American Express aggregator transactions; ■ R for all Mastercard aggregator authorizations; ■ otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (20) CyberSource through VisaNet with American Express: String (20) CyberSource through VisaNet with Mastercard: String (15) FDC Compass: String (20) FDC Nashville Global: String (14)
submerchant_ name	Sub-merchant's business name. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (37) FDC Compass with American Express: String (19) FDC Compass with Mastercard: String (37) FDC Nashville Global: String (12)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_ phone	Sub-merchant's telephone number. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 5-24 ■ Field: American Express Seller Telephone Number ***FDC Compass*** This value must consist of upper-case characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: O for all aggregator transactions with American Express; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (20) CyberSource through VisaNet: String (20) FDC Compass: String (13) FDC Nashville Global: String (10)
submerchant_ postal_code	Partial postal code for the sub-merchant's address. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (9) FDC Compass: String (15) FDC Nashville Global: String (9)
submerchant_state	Sub-merchant's state or province. Use the *State, Province, and Territory Codes for the United States and Canada*. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (3)

Table 6   API Request Fields (Continued)

Field Name	Description	Used By: Required (R) or Optional (O)	Data Type & Length
submerchant_ street	First line of the sub-merchant's street address. ***FDC Compass*** This value must consist of upper-case characters.	authorization American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: not used. FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	American Express Direct: String (30) FDC Compass: String (38) FDC Nashville Global: String (25)
tax_amount	Total tax amount to apply to the order. This value cannot be negative. **Important** To prevent data tampering CyberSource recommends that you include this field within the **signed_field_ names** field for generating a signature.	This field is optional.	Amount String (15)
transaction_type	The type of transactions: ■ authorization ■ authorization,create_payment_ token ■ authorization,update_payment_ token ■ sale ■ sale,create_payment_token ■ sale,update_payment_token ■ create_payment_token ■ update_payment_token	Required by the Secure Acceptance application.	Enumerated String String (60)
transaction_uuid	Unique merchant-generated identifier. Include with the **access_ key** field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts.	Required by the Secure Acceptance application.	ASCIIAlphaNumericPunct uation String (50)
unsigned_field_ names	A comma-separated list of request fields that are not signed.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable

API Reply Fields

Reply fields are sent using the following notification methods:

■ Merchant POST URL (see "Receiving Merchant Notifications," page 26)

■ Merchant POST Email (see "Receiving Merchant Notifications," page 26)

■ POSTed to the URL specified in the Transaction or Custom Cancel Response page (see "Transaction Response Page," page 29)

Notification methods are enabled on the Notifications and Customer Response pages of your Secure Acceptance profile.

To ensure the integrity of the reply fields, a signature is included in the response. This signature is generated using the same **secret_key** value that was used to generate the request signature.

To verify that the reply fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** reply field. This signature must be the same value that is included in the signature response field. Refer to the receipt page that is included in the sample scripts (see "Sample Scripting Languages," page 31).

![Important]	Because CyberSource may add reply fields and reason codes at any time, proceed as follows:
Important	■ Parse the reply data according to the names of the fields instead of their order in the reply. For more information on parsing reply fields, see the documentation for your scripting language.
	■ The signature that you generate must be the same value that is included in the signature response field.
	■ Your error handler should use the decision field to determine the transaction result if it receives a reason code that it does not recognize.

![Note]	If configured, these API reply fields are sent back to your Merchant POST URL or email. See "Receiving Merchant Notifications," page 26. Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.
Note	

Table 7   API Reply Fields

Field Name	Description	Data Type and Length
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes," page 124.	String (1)
auth_avs_code_raw	AVS result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_card_payroll	Indicates whether the card is a payroll card. Possible values: ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown **Note** This field is supported for Visa, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)
auth_card_pinless_debit	Indicates whether the card is a PINless debit card. Possible values: ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown **Note** This field is supported for Visa and Mastercard on Chase Paymentech Solutions.	String (1)
auth_card_prepaid	Indicates whether the card is a prepaid card. This information enables you to determine when a gift card or prepaid card is presented for use when establishing a new recurring or installment billing relationship. Possible values: ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown **Note** This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
auth_card_regulated	Indicates whether the card is regulated according to the Durbin Amendment. If the card is regulated, the card issuer is subject to price caps and interchange rules. Possible values: ■ Y: Yes (assets greater than $10B) ■ N: No (assets less than $10B) ■ X: Not applicable / Unknown **Note** This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.	String (1)
auth_card_signature_debit	Indicates whether the card is a signature debit card. This information enables you to alter the way an order is processed. Possible values: ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown **Note** This field is supported for Visa, Mastercard, and Maestro (International) on Chase Paymentech Solutions.	String (1)
auth_code	Authorization code. Returned only if a value is returned by the processor.	String (7)
auth_cv_result	CVN result code. See "CVN Codes," page 126.	String (1)
auth_cv_result_raw	CVN result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_response	For most processors, this is the error message sent directly from the bank. Returned only if a value is returned by the processor.	String (10)
auth_time	Time of authorization in UTC.	String (20)
auth_trans_ref_no	Reference number that you use to reconcile your CyberSource reports with your processor reports.	String (60)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
decision	The result of your request. Possible values: ■ ACCEPT ■ DECLINE ■ REVIEW ■ ERROR ■ CANCEL	String (7)
echeck_debit_ref_no	Reference number for the transaction.	String (60)
echeck_debit_submit_time	Time when the debit was requested in UTC.	Date and Time (20)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Reply message from the payment gateway.	String (255)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank. This field is used by the payer authentication validation service.	String (50)
payer_authentication_eci	Electronic commerce indicator (ECI). This field is used by payer authentication validation and enrollment services. Possible values for Visa, American Express, and JCB: ■ 05: Successful authentication. ■ 06: Authentication attempted. ■ 07: Failed authentication. Possible values for Mastercard: ■ 01: Merchant is liable. ■ 02: Card issuer is liable.	String (3)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_enroll_e_commerce_indicator	Commerce indicator for cards not enrolled. This field contains one of these values: ■ internet: Card not enrolled or card type not supported by payer authentication. No liability shift. ■ js_attempted: JCB card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ js_failure: J/Secure directory service is not available. No liability shift. ■ spa: Mastercard card not enrolled in the SecureCode program. No liability shift. ■ vbv_attempted: Visa card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ vbv_failure: For payment processor Barclays, Streamline, AIBMS, or FDC Germany, you receive this result if Visa's directory service is not available. No liability shift.	String (255)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_enroll_veres_ enrolled	Result of the enrollment check. This field can contain one of these values:	String (255)
	■ Y: Card enrolled or can be enrolled; you must authenticate. Liability shift.	
	■ N: Card not enrolled; proceed with authorization. Liability shift.	
	■ U: Unable to authenticate regardless of the reason. No liability shift.	
	Note This field applies only to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request.	
	The following value can be returned if you are using rules-based Payer Authentication:	
	■ B: Indicates that authentication was bypassed.	
	For Rules-Based Payer Authentication information see the *Payer Authentication Using the SCMP API* (PDF | HTML) or *Payer Authentication Using the Simple Order API* (PDF | HTML).	

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_enroll_veres_enrolled	Result of the enrollment check. This field can contain one of these values: ■ Y: Card enrolled or can be enrolled; you must authenticate. Liability shift. ■ N: Card not enrolled; proceed with authorization. Liability shift. ■ U: Unable to authenticate regardless of the reason. No liability shift. **Note** This field applies only to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request. The following value can be returned if you are using rules-based Payer Authentication: ■ B: Indicates that authentication was bypassed. For "Rules-Based Payer Authentication" information see the *Payer Authentication Using the SCMP API* (PDF | HTML) or *Payer Authentication Using the Simple Order API* (PDF | HTML).	String (255)
payer_authentication_pares_status	Raw result of the authentication check. This field can contain one of these values: ■ A: Proof of authentication attempt was generated. ■ N: Customer failed or cancelled authentication. Transaction denied. ■ U: Authentication not completed regardless of the reason. ■ Y: Customer was successfully authenticated.	String (255)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_proof_xml	XML element containing proof of enrollment verification. For cards not issued in the U.S. or Canada, your bank may require this data as proof of enrollment verification for any payer authentication transaction that you re-submit because of a chargeback. For cards issued in the U.S. or Canada, Visa may require this data for specific merchant category codes. This field is HTML encoded.	String (1024)
payer_authentication_reason_code	Numeric value corresponding to the result of the payer authentication request. See "Reason Codes," page 120.	String (5)
payer_authentication_uad	Mastercard SecureCode UCAF authentication data. Returned only for Mastercard SecureCode transactions.	String (32)
payer_authentication_uci	Mastercard SecureCode UCAF collection indicator. This field indicates if authentication data is collected at your web site. Possible values: ■ 0: Authentication data not collected and customer authentication was not completed. ■ 1: Authentication data not collected because customer authentication was not completed. ■ 2: Authentication data collected. customer completed authentication.	String (1)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_validate_e_commerce_indicator	Indicator that distinguishes Internet transactions from other types. The authentication failed if this field is not returned. For Visa, if your payment processor is Streamline, Barclays, AIBMS, or FDC Germany, you receive the value vbv_failure instead of internet when **payer_authentication_eci** is not present. The value of this field is passed automatically to the authorization service if you request the services together. This field contains one of these values: ■ aesk: American Express SafeKey authentication verified successfully. ■ aesk_attempted: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. ■ internet: Authentication was not verified successfully. ■ js: J/Secure authentication verified successfully. ■ js_attempted: JCB card not enrolled in J/Secure, but the attempt to authenticate was recorded. ■ spa: Mastercard SecureCode authentication verified successfully. ■ spa_failure: Mastercard SecureCode failed authentication. ■ vbv: Verified by Visa authentication verified successfully. ■ vbv_attempted: Card not enrolled in Verified by Visa, but the attempt to authenticate was recorded. ■ vbv_failure: Verified by Visa authentication unavailable.	String (255)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_validate_result	Raw authentication data that comes from the card issuing bank that indicates whether authentication was successful and whether liability shift occurred. This field contains one of these values: ■ -1: Invalid PARes. ■ 0: Successful validation. ■ 1: Cardholder is not participating, but the attempt to authenticate was recorded. ■ 6: Issuer unable to perform authentication. ■ 9: Cardholder did not complete authentication.	String (255)
payer_authentication_xid	Transaction identifier generated by CyberSource Payer Authentication. Used to match an outgoing PA request with an incoming PA response.	String (28)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. This payment token supercedes the previous payment token and is returned if: ■ The merchant is configured for a 16 digit payment token which displays the last four-digits of the primary account number (PAN) and passes Luhn mod-10 check. See "Payment Tokens," page 14. ■ The customer has updated the card number on their payment token. This payment token supercedes the previous payment token and should be used for subsequent transactions. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_address_status	Status of the street address on file with PayPal. Possible values: ■ None ■ Confirmed ■ Unconfirmed	String (12)
paypal_authorization_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_authorization_transaction_id	Unique identifier for the transaction.	String (17)
paypal_customer_email	Email address of the customer as entered during checkout. PayPal uses this value to pre-fill the PayPal membership sign-up portion of the PayPal login page.	String (127)
paypal_do_capture_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_do_capture_transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_get_details_correlation_ id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_ec_get_details_request_id	Value of the request ID returned from a PayPal get details service request.	String (26)
paypal_ec_get_details_transaction_ id	Unique identifier for the transaction.	String (17)
paypal_ec_order_setup_ correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_ec_order_setup_ transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_set_request_id	Value of the request ID returned from a PayPal set service request.	String (26)
paypal_fee_amount	PayPal fee charged for the transaction. This value does not exceed the equivalent of 10,000 USD in any currency and does not include a currency symbol. The decimal separator is a period (.), and the optional thousands separator is a comma (,).	String (9)
paypal_order_request_id	Value of the request ID returned from a PayPal order setup service request.	String (26)
paypal_payer_id	Customer's PayPal account identification number.	Alphanumeric String (13)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_payer_status	Customer's status. Possible values: ▪ verified ▪ unverified	String (10)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_pending_reason	Indicates the reason that payment is pending. Possible values:	String (14)
	■ address: Your customer did not include a confirmed shipping address, and your Payment Receiving preferences are set to manually accept or deny such payments. To change your preferences, go to the Preferences section of your PayPal profile.	
	■ authorization: The payment has been authorized but not settled. You need to capture the authorized amount.	
	■ echeck: Payment was made by an eCheck that has not yet cleared.	
	■ intl: You have a non-U.S. account and do not have a withdrawal mechanism. You must manually accept or deny this payment in your PayPal Account Overview.	
	■ multi-currency: You do not have a balance in the currency sent, and your Payment Receiving preferences are not set to automatically convert and accept this payment. You must manually accept or deny this payment in your PayPal Account Overview.	
	■ none: No pending reason.	
	■ order: The payment is part of an order that has been authorized but not settled.	
	■ paymentreview: The payment is being reviewed by PayPal for possible fraud.	
	■ unilateral: The payment was made to an email address that is not registered or confirmed.	
	■ verify: Your account is not yet verified. You must verify your account before you can accept this payment.	

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_pending_status	Status of the transaction. Possible values: ■ Canceled-Reversal: PayPal canceled the reversal, which happens when you win a dispute and the funds for the reversal are returned to you. ■ Completed: PayPal completed the payment and added the funds to your account. ■ Denied: You denied a payment, which happens only if the payment was pending for the reason indicated in the **reason_code** field. ■ Expired: The authorization expired. ■ Failed: The payment failed. This event can happen only when the payment is made from your customer's bank account. ■ In-Progress: The transaction has not been completed yet. ■ None: No status. ■ Partially-Refunded: The payment was partially refunded. ■ Pending: The payment is pending for the reason indicated in the **paypal_pending_reason** field. ■ Processed: PayPal accepted the payment. ■ ReasonCode ■ Refunded: You refunded the payment. ■ Reversed: PayPal reversed the payment for the reason specified in the **reason_code** field. The funds were transferred from your account to the customer's account. ■ Voided: The authorization was voided	String (20)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_protection_eligibility	Seller protection in force for the transaction. Possible values: ■ Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. ■ PartiallyEligible: You are protected by the PayPal Seller Protection Policy for item not received. ■ Ineligible: You are not protected under the PayPal Seller Protection Policy.	String (17)
paypal_protection_eligibility_type	Seller protection in force for the transaction. Possible values: ■ Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. ■ ItemNotReceivedEligible: You are protected by the PayPal Seller Protection Policy for item not received. ■ UnauthorizedPaymentEligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment. ■ Ineligible: You are not protected under the PayPal Seller Protection Policy. **Note** To enable the **paypal_protection_eligibility_type** field, contact CyberSource Customer Support to have your account configured for this feature.	String (32)
paypal_request_id	Identifier for the request generated by the client.	String (26)
paypal_token	Timestamped paypal token which identifies that PayPal Express Checkout is processing the transaction. You need to save this value to send in future request messages.	String (20)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
paypal_transaction_type	Indicates the paypal transaction type. Possible value: expresscheckout	String (16)
reason_code	Numeric value corresponding to the result of the credit card authorization request. See "Reason Codes," page 120.	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)
req_aggregator_id	Value that identifies you as a payment aggregator. Obtain this value for the processor. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 95-105 ■ Field: Mastercard Payment Facilitator ID ***FDC Compass*** This value must consist of upper-case characters. ***Field Length*** American Express Direct: 20 CyberSource through VisaNet: 11 FDC Compass: 20 FDC Nashville Global: 15 ***Required/Optional*** American Express Direct: R for all aggregator transactions. CyberSource through VisaNet: R for Mastercard aggregator authorizations; otherwise, not used. FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (See description)
req_amount	Total amount for the order. Must be greater than or equal to zero.	String (15)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_auth_indicator	Flag that specifies the purpose of the authorization. Possible values: ■ 0: Preauthorization ■ 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the default for this field, contact CyberSource Customer Support.	String (1)
req_bill_payment	Flag that indicates that this payment is for a bill or for an existing contractual loan. Possible values: ■ Y: bill payment or loan payment. ■ N (default): not a bill payment or loan payment.	String (1)
req_bill_to_address_city	City in the billing address.	String (50)
req_bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes.	String (2)
req_bill_to_address_line1	First line of the street address in the billing address.	String (60)
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60)
req_bill_to_address_postal_code	Postal code for the billing address. **Note** This field is required if **bill_to_address_country** is US or CA. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] **Example** A1B 2C3 For the rest of the world countries, the maximum length is 10.	String (10)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_bill_to_address_state	The two-character ISO state and province code. See *State, Province, and Territory Codes for the United States and Canada*. **Note** This field is required for the U.S and Canada.	String (2 for U.S. and Canada, otherwise 60)
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer email address.	String (255)
req_bill_to_forename	Customer first name.	String (60)
req_bill_to_phone	Customer phone number.	String (15)
req_bill_to_surname	Customer last name.	String (60)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number. See "Receiving Merchant Notifications," page 26.	String (20)
req_card_type	Type of card.	String (3)
req_company_tax_id	Company's tax identifier. The the last four digits are not masked.	String (9)
req_complete_route	Concatenation of individual travel legs in the format: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_route** takes precedence over that of the **journey_leg#** fields.	String (255)
req_consumer_id	Identifier for the customer account. This value is defined when creating a customer subscription.	String (100)
req_currency	Currency used for the order.	String (3)

Table 7 **API Reply Fields (Continued)**

Field Name	Description	Data Type and Length
req_customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ■ true: customer's browser accepts cookies. ■ false: customer's browser does not accept cookies.	String (5)
req_customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: ■ true: customer requested gift wrapping. ■ false: customer did not request gift wrapping.	String (5)
req_customer_ip_address	Customer IP address reported by your web server using socket information.	
req_date_of_birth	Date of birth of the customer in the format: YYYYMMDD.	String (8)
req_debt_indicator	Flag that indicates a payment for an existing contractual loan. Possible values: ■ true: Loan payment. ■ false (default): Not a loan payment.	String (5)
req_departure_time	Departure date and time of the first leg of the trip. Use one of the following formats: yyyy-MM-dd HH:mm z yyyy-MM-dd hh:mm a z yyyy-MM-dd hh:mma z HH = 24-hour format hh = 12-hour format a = am or pm (case insensitive) z = time zone of the departing flight.	String (29)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different sessions IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	String (88)
req_driver_license_number	Driver's license number of the customer. The the last four-digits are not masked.	String (30)
req_driver_license_state	State or province from which the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada.*	String (2)
req_e_commerce_indicator	The commerce indicator for the transaction type. Value: install **Note** This field is required only for installment payments using the CyberSource Latin American Processing connection.	String (13)
req_echeck_account_number	Account number. This number is masked.	Non-negative integer (17)
req_echeck_account_type	Account type. Possible values: ■ C: checking ■ S: savings (USD only) ■ X: corporate checking (USD only)	String (1)
req_echeck_check_number	Check number.	Integer (8)
req_echeck_routing_number	Bank routing number. It is also called the transit number.	Non-negative integer (9)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_echeck_sec_code	The authorization method for the transaction. Possible values: ■ CCD ■ PPD ■ TEL ■ WEB	String (3)
req_ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false	String (5)
req_ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false	String (5)
req_installment_total_amount	Total amount of the loan that is being paid in installments. **Note** This field is required only for installment payments using the CyberSource Latin American Processing or CyberSource through VisaNet connections.	Amount (12)
req_installment_total_count	Total number of installment payments as part of an authorization. Possible values: 1 to 99 **Note** This field is required only for installment payments using the CyberSource Latin American Processing connection.	Numeric String (2)
req_issuer_additional_data	Data defined by the issuer. See the "Formats for Discretionary Data" section in *Credit Card Services Using the SCMP API* or *Credit Card Services Using the Simple Order API*.	Alphanumeric String (256)
req_item_#_code	Type of product. # can range from 0 to 199.	String (255)
req_item_#_description	Description of the item. # can range from 0 to 199.	String (255)
req_item_#_name	Name of the item. # can range from 0 to 199.	String (255)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_item_#_passenger_email	Passenger's email address.	String (255)
req_item_#_passenger_forename	Passenger's first name.	String (60)
req_item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	String (32)
req_item_#_passenger_phone	Passenger's phone number. If the order is from outside the U.S., CyberSource recommends that you include the country code.	String (15)
req_item_#_passenger_status	Your company's passenger classification, such as with a frequent flyer classification. In this case, you might use values such as standard, gold, or platinum.	String (32)
req_item_#_passenger_surname	Passenger's last name.	String (60)
req_item_#_passenger_type	Passenger classification associated with the price of the ticket. You can use one of the following values: ■ ADT: Adult ■ CNN: Child ■ INF: Infant ■ YTH: Youth ■ STU: Student ■ SCR: Senior Citizen ■ MIL: Military	String (32)
req_item_#_quantity	Quantity of line items. # can range from 0 to 199.	String (10)
req_item_#_sku	Identification code for the product. # can range from 0 to 199.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	String (15)
req_item_#_unit_price	Price of the line item. # can range from 0 to 199. This value cannot be negative.	String (15)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_journey_leg#_dest	Airport code for the destination leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long; for example: SFO = San Francisco. Do not use the colon (:) or the dash (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_journey_leg#_orig	Airport code for the origin leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long; for example: SFO = San Francisco. Do not use the colon (:) or the dash (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_journey_type	Type of travel, such as one way or round trip.	String (32)
req_jpo_payment_installments	Total number of Japanese installment payments.	String (2)
req_jpo_payment_method	Japanese payment method.	String (1)
req_line_item_count	Total number of line items. Maximum number is 200.	String (2)
req_locale	Indicates the language used for the customer-facing content.	String (5)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from 1 to 100.	String (100)
	Merchant-defined data fields 1 to 4 are associated with the payment token and are used for subsequent token-based transactions. Merchant-defined data fields 5 to 100 are passed through to Decision Manager as part of the initial payment request and are not associated with the payment token.	
	Important Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields and any Secure Acceptance field that is not specifically designed to capture personally identifying information. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_descriptor req_merchant_descriptor_alternate req_merchant_descriptor_city req_merchant_descriptor_contact req_merchant_descriptor_country req_merchant_descriptor_state req_merchant_descriptor_postal_code req_merchant_descriptor_street	For the descriptions, used-by information, data types, and lengths for these fields, see the Merchant Descriptors section in either *Credit Card Services Using the SCMP API* or *Credit Card Services Using the Simple Order API*.	
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (100)
req_merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (2000)
req_override_backoffice_post_url	Overrides the backoffice post URL profile setting with your own URL.	URL (255)
req_override_custom_cancel_page	Overrides the custom cancel page profile setting with your own URL.	URL (255)
req_override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL.	URL (255)
req_payment_method	Method of payment. Possible values: ▪ card ▪ echeck ▪ paypal	String (30)
req_payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. When this field is included in the request, the card data and billing and shipping information are optional. You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_payment_token_comments	Optional comments about the customer subscription.	String (255)
req_payment_token_title	Name of the customer subscription.	String (60)
req_profile_id	Identifies the profile to use with each transaction.	String (36)
req_recipient_account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	Numeric String (10)
req_recipient_date_of_birth	Recipient's date of birth. Format: YYYYMMDD.	Date (b) String (8)
req_recipient_postal_code	Partial postal code for the recipient's address. For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.	Alphanumeric String (6)
req_recipient_surname	Recipient's last name.	Alpha String (6)
req_recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
req_recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: ■ true (default): automatically renew. ■ false: do not automatically renew.	Enumerated String String (5)
req_recurring_frequency	Frequency of payments for an installment or recurring subscription.	String (20)
req_recurring_number_of_ installments	Total number of payments set up for an installment subscription.	String (3)
req_recurring_start_date	First payment date for an installment or recurring subscription payment.	String (8)
req_reference_number	Unique merchant-generated order reference or tracking number for each transaction.	String (50)
req_returns_accepted	Indicates whether product returns are accepted. Possible values: ■ true ■ false	String (5)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_sales_organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 106-116 ■ Field: Mastercard Independent Sales Organization ID	Nonnegative integer (11)
req_ship_to_address_city	City of shipping address.	String (50)
req_ship_to_address_country	The two-character ISO country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60)
req_ship_to_address_line2	Second line of shipping address.	String (60)
req_ship_to_address_postal_code	Postal code of shipping address.	String (10)
req_ship_to_address_state	The two-character ISO state and province code.	String (2)
req_ship_to_company_name	Name of the company receiving the product.	String (40)
req_ship_to_forename	First name of person receiving the product.	String (60)
req_ship_to_phone	Phone number for the shipping address.	String (15)
req_ship_to_surname	Second name of person receiving the product.	String (60)
req_shipping_method	Shipping method for the product. Possible values: ■ sameday: Courier or same-day service ■ oneday: Next day or overnight service ■ twoday: Two-day service ■ threeday: Three-day service ■ lowcost: Lowest-cost service ■ pickup: Store pick-up ■ other: Other shipping method ■ none: No shipping method because	String (10)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_skip_bin_lookup	Indicates whether the BIN lookup service was skipped. See "Enabling eChecks," page 21.	Enumerated String String (5)
req_skip_decision_manager	Indicates whether to skip Decision Manager. See Chapter 4, "Using Decision Manager," on page 34. This field can contain one of the following values: ■ true ■ false	String (5)
req_submerchant_city	Sub-merchant's city. ***FDC Compass*** This value must consist of upper-case characters.	American Express Direct: String (15) FDC Compass: String (21) FDC Nashville Global: String (11)
req_submerchant_country	Sub-merchant's country. Use the two-character *ISO Standard Country Codes*. ***FDC Compass*** This value must consist of upper-case characters.	String (3)
req_submerchant_email	Sub-merchant's email address. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 25-64 ■ Field: American Express Seller E-mail Address	American Express Direct: String (40) CyberSource through VisaNet: String (40) FDC Compass: String (40) FDC Nashville Global: String (19)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_submerchant_id	The ID you assigned to your sub-merchant. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 65-84 ■ Field: American Express Seller ID With Mastercard, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCR6 ■ Position: 117-131 ■ Field: Mastercard Sub-Merchant ID ***FDC Compass*** This value must consist of upper-case characters.	American Express Direct: String (20) CyberSource through VisaNet with American Express: String (20) CyberSource through VisaNet with Mastercard: String (15) FDC Compass: String (20) FDC Nashville Global: String (14)
req_submerchant_name	Sub-merchant's business name. ***FDC Compass*** This value must consist of upper-case characters.	American Express Direct: String (37) FDC Compass with American Express: String (19) FDC Compass with Mastercard: String (37) FDC Nashville Global: String (12)

Table 7   API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_submerchant_phone	Sub-merchant's telephone number. ***CyberSource through VisaNet*** With American Express, the value for this field corresponds to the following data in the TC 33 capture file[5]: ■ Record: CP01 TCRB ■ Position: 5-24 ■ Field: American Express Seller Telephone Number ***FDC Compass*** This value must consist of upper-case characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA	American Express Direct: String (20) CyberSource through VisaNet: String (20) FDC Compass: String (13) FDC Nashville Global: String (10)
req_submerchant_postal_code	Partial postal code for the sub-merchant's address. ***FDC Compass*** This value must consist of upper-case characters.	American Express Direct: String (9) FDC Compass: String (15) FDC Nashville Global: String (9)
req_submerchant_state	Sub-merchant's state or province. Use the *State, Province, and Territory Codes for the United States and Canada*. ***FDC Compass*** This value must consist of upper-case characters.	String (3)
req_submerchant_street	First line of the sub-merchant's street address. ***FDC Compass*** This value must consist of upper-case characters.	American Express Direct: String (30) FDC Compass: String (38) FDC Nashville Global: String (25)
req_tax_amount	Total tax to apply to the product.	String (15)
req_transaction_type	The type of transaction requested.	String (60)

Table 7 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_transaction_uuid	Unique merchant-generated identifier. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts.	String (50)
required_fields	Indicates which of the request parameters were required but not provided.	Variable
service_fee_amount	The service fee amount for the order.	String (15)
service_fee_return_url	URL to POST the **conditions_ accepted** field value to. See "Enabling the Service Fee," page 23.	
signature	The Base64 signature returned by the server.	String (44)
signed_date_time	The date and time of when the signature was generated by the server. Format: YYYY-MM-DDThh:mm:ssZ Example 2016-08-11T22:47:57Z equals August 11, 2016, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	String (20)
signed_field_names	A comma-separated list of response data that was signed by the server. All fields within this list should be used to generate a signature that can then be compared to the response signature to verify the response.	Variable
transaction_id	The transaction identifier from the payment gateway.	String (26)
utf8	Indicates whether the unicode characters are encoded. Possible value: ✓	String (3)

Reason Codes

The **reasonCode** field contains additional data regarding the decision response of the transaction. Depending on the decision of a transaction request, CyberSource's default receipt page or your receipt page is displayed to the customer. Both you and your customer may also receive an email receipt. See "Receiving Merchant Notifications," page 26.

Table 8   Reason Codes

Reason Code	Description
100	Successful transaction.
102	One or more fields in the request contain invalid data.
	Possible action: see the reply field **invalid_fields** to ascertain which fields are invalid. Resend the request with the correct information.
104	The **access_key** and **transaction_uuid** fields for this authorization request match the **access_key** and **transaction_uuid** fields of another authorization request that you sent within the past 15 minutes.
	Possible action: resend the request with a unique **access_key** field and **transaction_uuid** field.
110	Only a partial amount was approved.
150	General system failure.
	Possible action: wait a few minutes and resend the request.
151	The request was received but there was a server timeout. This error does not include timeouts between the client and the server.
	Possible action: wait a few minutes and resend the request.
152	The request was received, but a service timeout occurred.
	Possible action: wait a few minutes and resend the request.
200	The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the Address Verification System (AVS) check.
	Possible action: you can capture the authorization, but consider reviewing the order for fraud.
201	The issuing bank has questions about the request. You do not receive an authorization code programmatically, but you might receive one verbally by calling the processor.
	Possible action: call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.
202	Expired card. You might also receive this value if the expiration date you provided does not match the date the issuing bank has on file.
	Possible action: request a different card or other form of payment.

Table 8   Reason Codes (Continued)

Reason Code	Description
203	General decline of the card. No other information was provided by the issuing bank.
	Possible action: request a different card or other form of payment.
204	Insufficient funds in the account.
	Possible action: request a different card or other form of payment.
205	Stolen or lost card.
	Possible action: review this transaction manually to ensure that you submitted the correct information.
207	Issuing bank unavailable.
	Possible action: wait a few minutes and resend the request.
208	Inactive card or card not authorized for card-not-present transactions.
	Possible action: request a different card or other form of payment.
210	The card has reached the credit limit.
	Possible action: request a different card or other form of payment.
211	Invalid CVN.
	Possible action: request a different card or other form of payment.
221	The customer matched an entry on the processor's negative file.
	Possible action: review the order and contact the payment processor.
222	Account frozen.
230	The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the CVN check.
	Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.
231	Invalid account number.
	Possible action: request a different card or other form of payment.
232	The card type is not accepted by the payment processor.
	Possible action: contact your merchant bank to confirm that your account is set up to receive the card in question.
233	General decline by the processor.
	Possible action: request a different card or other form of payment.
234	There is a problem with the information in your CyberSource account.
	Possible action: do not resend the request. Contact CyberSource Customer Support to correct the information in your account.
236	Processor failure.
	Possible action: wait a few minutes and resend the request.

Table 8 Reason Codes (Continued)

Reason Code	Description
240	The card type sent is invalid or does not correlate with the credit card number.
	Possible action: confirm that the card type correlates with the credit card number specified in the request; then resend the request.
475	The cardholder is enrolled for payer authentication.
	Possible action: authenticate cardholder before proceeding.
476	Payer authentication could not be authenticated.
520	The authorization request was approved by the issuing bank but declined by CyberSource based on your Decision Manager settings.
	Possible action: review the authorization request.

Types of Notifications

Table 9   Types of Notifications

Decision	Description	Type of Notification
ACCEPT	Successful transaction. **Note** See reason codes 100 and 110.	■ Custom receipt page ■ Customer receipt email ■ Merchant POST URL ■ Merchant receipt email
REVIEW	Authorization was declined; however, the capture may still be possible. Review payment details. **Note** See reason codes 200, 201, 230, and 520.	■ Custom receipt page ■ Customer receipt email ■ Merchant POST URL ■ Merchant receipt email
DECLINE	Transaction was declined. **Note** See reason codes 102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, and 476.	■ Custom receipt page [1] ■ Merchant POST URL [1] ■ Merchant receipt email [1]
ERROR	Access denied, page not found, or internal server error. **Note** See reason codes 102, 104, 150, 151, and 152.	■ Custom receipt page ■ Merchant POST URL
CANCEL	The customer did not accept the service fee conditions. The customer cancelled the transaction.	■ Custom receipt page ■ Custom cancel page ■ Merchant POST URL

1 If the retry limit is set to 0, the customer receives the decline message, *Your order was declined. Please verify your information.* before the merchant receives it. The decline message relates to either the processor declining the transaction or a payment processing error, or the customer entered their 3D Secure credentials incorrectly.

AVS Codes

An issuing bank uses the AVS code to confirm that your customer is providing the correct billing address. If the customer provides incorrect information, the transaction might be fraudulent. The international and U.S. domestic Address Verification Service (AVS) codes are the Visa standard AVS codes, except for codes 1 and 2, which are CyberSource AVS codes. The standard AVS return codes for other types of credit cards (including American Express cards) are mapped to the Visa standard codes. You receive the code in the **auth_avs_code** reply field. See "API Reply Fields," page 89.

⚠ **Important**	When you populate billing street address 1 and billing street address 2, CyberSource through VisaNet concatenates the two values. If the concatenated value exceeds 40 characters, CyberSource through VisaNet truncates the value at 40 characters before sending it to Visa and the issuing bank. Truncating this value affects AVS results and therefore might impact risk decisions and chargebacks.

International AVS Codes

These codes are returned only for Visa cards issued outside the U.S.

Table 10   International AVS Codes

Code	Response	Description
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
I	No match	Address not verified.
P	Partial match	Postal code matches, but street address not verified.

U.S. Domestic AVS Codes

Table 11   Domestic AVS Codes

Code	Response	Description
A	Partial match	Street address matches, but five-digit and nine-digit postal codes do not match.
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
E	Invalid	AVS data is invalid or AVS is not allowed for this card type.

Table 11   Domestic AVS Codes (Continued)

Code	Response	Description
F	Partial match	Card member's name does not match, but billing postal code matches. Returned only for the American Express card type.
G		Not supported.
H	Partial match	Card member's name does not match, but street address and postal code match. Returned only for the American Express card type.
I	No match	Address not verified.
J	Match	Card member's name, billing address, and postal code match. Shipping information verified and chargeback protection guaranteed through the Fraud Protection Program. Returned only if you are signed up to use AAV+ with the American Express Phoenix processor.
K	Partial match	Card member's name matches, but billing address and billing postal code do not match. Returned only for the American Express card type.
L	Partial match	Card member's name and billing postal code match, but billing address does not match. Returned only for the American Express card type.
M	Match	Street address and postal code match.
N	No match	One of the following: ■ Street address and postal code do not match. ■ Card member's name, street address, and postal code do not match. Returned only for the American Express card type.
O	Partial match	Card member's name and billing address match, but billing postal code does not match. Returned only for the American Express card type.
P	Partial match	Postal code matches, but street address is not verified.
Q	Match	Card member's name, billing address, and postal code match. Shipping information verified but chargeback protection not guaranteed (Standard program). Returned only if you are registered to use AAV+ with the American Express Phoenix processor.
R	System unavailable	System unavailable.
S	Not supported	U.S.-issuing bank does not support AVS.
T	Partial match	Card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable	Address information unavailable for one of these reasons: ■ The U.S. bank does not support non-U.S. AVS. ■ The AVS in a U.S. bank is not functioning properly.
V	Match	Card member's name, billing address, and billing postal code match. Returned only for the American Express card type.

Table 11   Domestic AVS Codes (Continued)

Code	Response	Description
W	Partial match	Street address does not match, but nine-digit postal code matches.
X	Match	Street address and nine-digit postal code match.
Y	Match	Street address and five-digit postal code match.
Z	Partial match	Street address does not match, but 5-digit postal code matches.
1	Not supported	AVS is not supported for this processor or card type.
2	Unrecognized	The processor returned an unrecognized value for the AVS response.
3	Match	Address is confirmed. Returned only for PayPal Express Checkout.
4	No match	Address is not confirmed. Returned only for PayPal Express Checkout.

CVN Codes

Table 12   CVN Codes

Code	Description
D	The transaction was considered to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation.
M	The CVN matched.
N	The CVN did not match.
P	The CVN was not processed by the processor for an unspecified reason.
S	The CVN is on the card but was not included in the request.
U	Card verification is not supported by the issuing bank.
X	Card verification is not supported by the card association.
1	Card verification is not supported for this processor or card type.
2	An unrecognized result code was returned by the processor for the card verification response.
3	No result code was returned by the processor.

iFrame Implementation

! **Important**	Internet Explorer and Safari handle third-party content differently. Therefore, you must consider these differences when implementing a standard Secure Acceptance Silent Order POST implementation or an iFrame implementation. Otherwise, payments may fail for customers using these browsers.
	PayPal Express Checkout is not supported on a Secure Acceptance iFrame integration.

Clickjacking Prevention

Clickjacking (also known as *user-interface redress attack* and *iframe overlay*) is used by attackers to trick users into clicking on a transparent layer (with malicious code) above legitimate buttons or clickable content for a site. To prevent clickjacking, you must prevent third-party sites from including your web site within an iFrame.

While no security remediation can prevent every clickjacking, these are the minimum measures you must use for modern web browsers:

■   Set HTTP response header X-FRAME_OPTIONS to either "DENY" or "SAMEORIGIN".

■   Provide frame-busting scripts to ensure that your page is always the top level window or disabling code for older browsers that do not support X-FRAME_OPTIONS.

You are required to implement the recommended prevention techniques in your web site. See the OWASP clickjacking page and the Cross-Site scripting page for current information.

Web application protections for Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF), etc. must also be incorporated.

- For XSS protection, you must implement comprehensive input validation and the OWASP-recommended security encoding library to do output encoding on your web site.

- For CSRF protection, you are strongly encouraged to use a synchronized token pattern. This measure requires generating a randomized token associated with the user session. The token will be inserted whenever an HTTP request is sent to the server. Your server application will verify that the token from the request is the same as the one associated with the user session.

iFrame Transaction Endpoints

For iFrame transaction endpoints and supported transaction types for each endpoint, see "Endpoints and Transaction Types," page 36.