

Credit Card Services

User Guide

March 2017



CyberSource Contact Information

For technical support questions, go to the Home page in the Business Center to see the contact information appropriate for your account.

Visit the Business Center, your central location for managing your online payment transactions, at <https://businesscenter.cybersource.com>.

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).

Copyright

© 2017 CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

Restricted Rights Legends

For Government or defense agencies. Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies. Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in CyberSource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of CyberSource Corporation.

CyberSource, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, and CyberSource Connect are trademarks and/or service marks of CyberSource Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Contents

Recent Revisions to This Document 9

About This Guide 11

Audience 11

Purpose 11

Conventions 11

Related Documentation 12

Chapter 1 Introduction to the Credit Card Services 13

Cards and Payment Methods 13

 Discover Acquisitions and Alliances 13

 Mastercard New 2-Series Bank Identification Numbers 15

Types of Transactions 15

 Card-Present Transactions 15

 Card-Not-Present Transactions 15

 Transactions with Special Data 16

Banks and Associations 16

 Acquiring (Merchant) Banks 16

 Issuing (Consumer) Banks 17

 Payment Card Companies 17

Services 18

Order Tracking 18

 Request IDs 18

 Reconciliation IDs 19

Payment Processors 19

Chapter 2	Credit Card Processing	21
	Authorizing a Payment	21
	Online Authorizations	21
	Offline Authorizations	23
	Creating an Authorization Request	23
	Authorization Information for Specific Processors	25
	Reversing an Authorization	25
	Supported Processors and Card Types	26
	Creating a Full Authorization Reversal Request	27
	Authorization Reversal after Void (ARAV)	28
	Capturing an Authorization	29
	Captures	30
	Creating a Capture Request	31
	Capture Information for Specific Processors	32
	Capture Features	33
	Automatic Partial Authorization Reversals	33
	Interchange Optimization	34
	Multiple Partial Captures	35
	Performing a Sale	37
	Crediting a Payment	38
	Types of Credits	38
	Creating a Credit Request	39
	Credit Information for Specific Processors	41
	Voiding a Capture or Credit	41
	Capture after Void	42
	Creating a Void Request	42

Chapter 3	Authorization Features	44
	Address Verification System (AVS)	44
	Relaxed Requirements for Address Data and Expiration Date	45
	Processing AVS Codes	46
	Electronic Verification (EV)	47
	Request Fields	48
	Reply Fields	49
	Card Verification Numbers (CVNs)	50
	CVN Locations and Terminology	51
	CVN Codes	51
	Verbal Authorizations	52

Chapter 4	Debit Cards and Prepaid Cards	55
	Partial Authorizations	55
	Supported Processors and Card Types	55
	Opting In	56
	How a Partial Authorization Works	57
	Special Processing for American Express Cards on Chase Paymentech Solutions	58
	Real-Time Reversals	59
	Balance Responses	60
	Unsupported Processors and Card Types	62

Chapter 5	Optional Features	63
	\$0 Authorizations	63
	Aggregator Support	63
	Terminology	64
	FDC Compass Aggregators	64
	FDC Nashville Global Aggregators	66
	AVS Only	66
	Bill Payments with Visa	67
	Card-Present Data	67
	Card Type Indicators (CTIs)	67
	Customer Profiles	68
	Final Authorization Indicator	68
	Final Authorizations	69
	Preauthorizations	69
	Undefined Authorizations	70
	Unmarked Authorizations	71
	Forced Captures	72
	Installment Payments	73
	Installment Payments on Chase Paymentech Solutions and FDC Compass	74
	Installment Payments on FDC Nashville Global	74
	Installment Payments on Other Processors	75
	JCB J/Secure	75
	Level II Data	75
	Level III Data	75
	Mastercard SecureCode	75
	Merchant Descriptors	76
	Chase Paymentech Solutions Merchant Descriptors	76
	Merchant Descriptor Logic	77
	Characters	78
	API Fields	78

FDC Compass Merchant Descriptors	81
Characters	81
API Fields	82
FDC Nashville Global Merchant Descriptors	84
Merchant Descriptor Logic	84
API Fields	86
FDMS South Merchant Descriptors	89
GPN Merchant Descriptors	90
TSYS Acquiring Solutions Merchant Descriptors	92
Merchant-Initiated Reversals and Voids	93
Micropayments	94
Payer Authentication	95
Verified by Visa	95
JCB J/Secure	97
Mastercard SecureCode	98
American Express SafeKey	100
Payment Tokenization	102
POS Transactions	102
Quasi-Cash	103
Recurring Billing	104
Recurring Payments	105
AVS and Recurring Payments	107
CVN and Recurring Payments	107
Replacement Expiration Dates for Recurring Payments	108
Recurring Profiles	108
Retail POS Data	109
Secure Data	109
Soft Descriptors	109
Split Dial/Route	109
Subscriptions	109
Type II Cards	109
Verbal Authorizations	109
Verified by Visa	109
Visa Bill Payments	110
Visa Debt Repayments	111
Zero Amount Authorizations	112

Chapter 6 Testing the Credit Card Services 114

- Requirements for Testing 114
 - Testing the Services 115
 - Using Amounts to Simulate Errors 115
 - Testing American Express Card Verification 116
-

Appendix A API Fields 117

- Formatting Restrictions 117
 - Data Type Definitions 117
 - Numbered Elements 118
 - Request Fields 119
 - Reply Fields 148
-

Appendix B Examples 159

- Name-Value Pair Examples 159
 - Basic Credit Card Examples 159
 - Partial Authorization Examples 161
 - Fully Approved Request 161
 - Partially Approved Request 162
 - XML Examples 164
 - Basic Credit Card Examples 164
 - Partial Authorization Examples 167
 - Fully Approved Request 167
 - Partially Approved Request 169
-

Appendix C American Express SafeKey Response Codes 171

Appendix D AVS Codes 172

Appendix E Commerce Indicators 175

Appendix F CVN Codes 176

Appendix G Electronic Verification Response Codes 177

Appendix H [Frequently Asked Questions](#) 178

Appendix I [Network Transaction Identifiers](#) 181

Appendix J [Product Codes](#) 182

Appendix K [Product IDs](#) 183
 [Visa Product IDs](#) 183
 [Mastercard Product IDs](#) 184

Appendix L [Reason Codes](#) 187

Appendix M [Smart Authorization Factor Codes](#) 191

Appendix N [Verified by Visa Response Codes](#) 192

[Index](#) 193

Recent Revisions to This Document

Release	Changes
March 2017	<p>All processors that support replacement expiration dates for recurring payments: 12/2021 is no longer a valid replacement expiration date. See "Replacement Expiration Dates for Recurring Payments," page 108.</p> <p>FDC Compass: added support for the final authorization indicator. See "Final Authorization Indicator," page 68.</p> <p>FDMS Nashville:</p> <ul style="list-style-type: none"> ■ Added support for multiple partial captures. See "Multiple Partial Captures," page 35. ■ Added support for the final authorization indicator. See "Final Authorization Indicator," page 68.
February 2017	<p>Chase Paymentech Solutions: updated the kind of support provided for the final authorization indicator:</p> <ul style="list-style-type: none"> ■ Added support for the authIndicator reply field. See "Reply Fields," page 148. ■ Removed support for undefined authorizations and added support for unmarked authorizations. See "Final Authorization Indicator," page 68. <p>FDC Nashville Global:</p> <ul style="list-style-type: none"> ■ Added support for the final authorization indicator. See "Final Authorization Indicator," page 68. ■ Added support for multiple captures. See "Multiple Partial Captures," page 35. <p>TSYS Acquiring Solutions: added support for the final authorization indicator. See "Final Authorization Indicator," page 68.</p>
January 2017	<p>All processors: added "Numbered Elements," page 118.</p> <p>All processors that support merchant-initiated reversals and voids: updated step 3 in "Merchant-Initiated Reversals and Voids," page 93.</p>
September 2016	<p>All processors that support multiple captures: created new section: "Multiple Partial Captures," page 35.</p> <p>FDC Nashville Global: updated the maximum length for the invoiceHeader_submerchantName field. See Table 43, "Request Fields," on page 119.</p>
August 2016	<p>FDC Compass: added support for American Express and JCB for full authorization reversals. See Table 10, "Processors That Support Full Authorization Reversals," on page 26.</p>

Release	Changes
July 2016	<p data-bbox="602 296 1409 352">Removed all mentions of Bill Me Later because this product is no longer supported.</p> <p data-bbox="602 373 662 405">GPN:</p> <ul data-bbox="602 422 1409 688" style="list-style-type: none"><li data-bbox="602 422 1409 506">■ Added Mastercard support for automatic partial authorization reversals. See Table 14, "Processors That Support Automatic Partial Authorization Reversals," on page 33.<li data-bbox="602 527 1409 590">■ Added Mastercard support for interchange optimization. See "Interchange Optimization," page 34.<li data-bbox="602 611 1409 688">■ For interchange optimization, the fresh authorization uses the same authorization indicator as the original authorization. See "Interchange Optimization," page 34 and "Final Authorization Indicator," page 68.

About This Guide

Audience

This guide is written for application developers who want to use the CyberSource Simple Order API to integrate credit card processing into their order management system.

Implementing the CyberSource credit card services requires software development skills. You must write code that uses the API request and reply fields to integrate the credit card services into your existing order management system.

Purpose

This guide describes tasks you must complete to integrate the credit card services into your existing order management system.

Conventions

The following special statements are used in this document:



Note

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

The following text conventions are used in this document:

Table 1 Text Conventions

Convention	Meaning
bold	Field and service names in text; for example: Include the ccAuthService_run field.
<i>italic</i>	Titles of documents
monospace	<ul style="list-style-type: none"> ■ XML elements ■ Code examples ■ Values for API fields; for example: Set the ccAuthService_run field to <code>true</code>.

Related Documentation

- *Getting Started with CyberSource Essentials* describes how to get started using the Simple Order API. ([PDF](#) | [HTML](#))
- The *Reporting User Guide* describes how to download reports. ([PDF](#) | [HTML](#))
- The *Secure Acceptance Silent Order POST Development Guide* describes how to create a Secure Acceptance Silent Order POST profile. ([PDF](#) | [HTML](#))
- The *Secure Acceptance Web/Mobile Configuration Guide* describes how to create a Secure Acceptance Web/Mobile profile. ([PDF](#) | [HTML](#))

Introduction to the Credit Card Services

Cards and Payment Methods

The credit card services can be used to process the types of cards and payment methods in the following table.

Table 2 Cards and Payment Methods Processed with Credit Card Services

Card or Payment Method	Description
Credit cards	CyberSource can accept payments made with numerous types of credit cards, including Visa [®] , Mastercard [®] , American Express [®] , Discover [®] , Diners Club [®] , and JCB [®] .
Debit cards and prepaid cards	Prepaid cards, Visa-branded debit cards, and Mastercard-branded debit cards can be processed with the credit card services. See Chapter 4, "Debit Cards and Prepaid Cards," on page 55.
Quasi-cash	A quasi-cash transaction is a cash-like transaction for the sale of items that are directly convertible to cash. See "Quasi-Cash," page 103.

Discover Acquisitions and Alliances

Discover has acquired or entered into alliances with the payment card companies shown in the following table.

Table 3 Discover Acquisitions and Alliances

Card Type	Description
China UnionPay Alliance	<p>In 2005, China UnionPay and Discover announced a strategic alliance whereby China UnionPay cards would be routed to the Discover Network. As a result of this alliance:</p> <ul style="list-style-type: none"> ■ If you have been accepting Discover but not China UnionPay, you are now able to accept and process China UnionPay cards that have been reissued with Discover bank identification numbers (BINs). ■ If you have been accepting China UnionPay but not Discover, you are now able to accept Discover cards.

Table 3 Discover Acquisitions and Alliances (Continued)

Card Type	Description
Diners Club Acquisition	<p>In July 2008, Discover acquired Diners Club International whereby Diners Club cards would be routed to the Discover Network starting October 16, 2009. As a result of this acquisition:</p> <ul style="list-style-type: none"> ■ If you have been accepting Discover but not Diners Club, you are now able to accept Diners Club cards. ■ If you have been accepting Diners Club but not Discover, you are now able to accept Discover cards.
JCB (US Domestic) Alliance	<p>In December 2006, JCB and Discover announced a strategic alliance whereby JCB cards would be routed to the Discover Network in the U.S. and select U.S. Territories (Puerto Rico, Guam, U.S. Virgin Islands, Northern Mariana Islands) that authorize, process, and fund in USD. As a result of this alliance:</p> <ul style="list-style-type: none"> ■ If you have been accepting Discover but not JCB, you are now able to accept JCB cards. ■ If you have been accepting JCB but not Discover, you are now able to accept Discover cards.

For some card types on some processors, the information in your CyberSource account must include processor-issued IDs for these transactions to be processed successfully. Call CyberSource Customer Support to update your account information.

As a result of these acquisitions and alliances, the following card types are processed on the Discover Network:

- China UnionPay
- Diners Club
- Discover
- JCB (US Domestic): For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.

**Note**

Non-U.S. JCB transactions are still routed through JCB.

**Note**

Your processor takes care of routing your transactions; you do not need to do any additional processing to route these card types to the Discover Network.

Mastercard New 2-Series Bank Identification Numbers

Mastercard is expanding the bank identification number (BIN) range by introducing BINs in the 222100-272099 range. Cards containing the 2-series BINs will be issued in 2017.

Effective October 2016, Mastercard requires processors, acquirers, issuers, and merchants to support the new 2-series BINs. Mastercard transactions on the 2-series primary account numbers (PANs) must be accepted, routed, and processed, and they must operate with the same rules that apply to the existing 5-series BINs.

Types of Transactions

Card-Present Transactions

When a customer uses a card that is physically present to make a purchase, the purchase is known as a *card-present transaction*. This type of transaction typically occurs in a retail environment. To process card-present transactions:

- Use the credit card services described in this guide.
- Provide card-present data as described in the [Card-Present Transactions Supplement](#).

Card-Not-Present Transactions

When a customer provides a card number but you do not have access to the physical card, the purchase is known as a *card-not-present transaction*. This type of transaction typically occurs over the Internet or through a call center. To process card-not-present transactions, use the credit card services described in this guide.

Card-not-present transactions pose an additional level of risk to your business because you cannot directly verify the customer's identification. CyberSource offers features, such as Address Verification System (AVS) and Card Verification Numbers (CVN), in the credit card services that can reduce that risk by checking the validity of the customer's information and notifying you when discrepancies occur. For descriptions of AVS and CVN, see [Chapter 3, "Authorization Features,"](#) on page 44.

Transactions with Special Data

The credit card services can process these types of special data:

- Level II and Level III data: see the [Level II and Level III Transactions Supplement](#).
- Card-present data: see [Card-Present Transactions Supplement](#).

Banks and Associations



Note

In this document, the word *processor* can refer to a processor, acquirer, or acquiring processor depending on your location.

Acquiring (Merchant) Banks

An acquiring, or merchant, bank offers accounts to businesses that accept credit card payments. Before you can accept payments, you must have a merchant bank account from an acquiring bank. Your merchant bank account must be configured to process card-not-present or mail order/telephone order (MOTO) transactions.



Note

Each acquiring bank has connections to a limited number of payment processors. You must choose a payment processor that your acquiring bank supports. See "[Payment Processors](#)," [page 19](#).

Expect to be charged the fees shown in the following table.

Table 4 Fees

Fee	Description
Discount rates	Your acquiring bank charges a fee and collects a percentage of every transaction. The combination of the fee and the percentage is called the discount rate. These charges can be <i>bundled</i> (combined into a single charge) or <i>unbundled</i> (charged separately) depending on your acquiring bank and other factors.
Interchange fees	Visa and Mastercard each have a base fee, called the interchange fee, for each type of transaction. Your acquiring bank and processor can explain how to minimize this fee.
Chargebacks	When customers dispute charges to their accounts, you can incur chargebacks. A chargeback occurs when a charge on a customer's account is reversed. Your merchant bank removes the money from your account and could charge you a fee for the chargeback.

You are responsible for maintaining:

- Good customer support
- Rapid problem resolution
- A high level of customer satisfaction
- Transaction management processes that minimize fraudulent transactions

The items in the preceding list are required to prevent an excessive number of credit card chargebacks. In the event that credit card chargebacks become excessive, CyberSource can require you to undertake business process changes to reduce chargebacks. If the chargebacks are not reduced to a satisfactory level, CyberSource can terminate your account.

If you receive a large number of chargebacks or if a large number of your transactions involve fraud, your acquiring bank might increase your discount rate or revoke your merchant bank account. Contact CyberSource for information about CyberSource products that can help prevent fraud.

Issuing (Consumer) Banks

An issuing, or consumer, bank provides credit cards to and underwrites lines of credit for consumers. The issuing bank provides monthly statements and collects payments. Issuing banks must follow the rules of the payment card companies to which they belong.

Payment Card Companies

Payment card companies manage communications between acquiring banks and issuing banks. They also develop industry standards, support their brands, and establish fees for acquiring banks.

Some payment card companies, such as Visa and Mastercard, are trade associations that do not issue cards. Instead, issuing banks are members of these associations and they issue cards under license from the associations.

Other card companies, such as Discover and American Express, act as the issuing banks for their own cards. Before you use CyberSource to process cards from these companies, you must sign agreements with the companies.

Services

The credit card services are:

- Authorization: see ["Authorizing a Payment," page 21](#).
- Full authorization reversal: see ["Reversing an Authorization," page 25](#).
- Capture: see ["Capturing an Authorization," page 29](#).
- Credit: see ["Crediting a Payment," page 38](#).
- Void: see ["Voiding a Capture or Credit," page 41](#). This service is not restricted to the credit card services; it can also be used for other payment methods.

You can also request an authorization and capture together. See ["Performing a Sale," page 37](#).

Order Tracking

See [Getting Started with CyberSource Essentials](#) for information about order tracking. This section provides the names of the API fields that are used for order tracking for the credit card services.

Request IDs

For all CyberSource services, the request ID is returned in the reply messages in **requestID**. The following table lists the fields for the request IDs in request messages.

Table 5 Fields for Request IDs in Request Messages

Service	Request ID Field
Authorization reversal	ccAuthReversalService_authRequestID
Capture	ccCaptureService_authRequestID
Credit	ccCreditService_captureRequestID
Void	voidService_voidRequestID

Reconciliation IDs

The following table lists the fields for the reconciliation IDs, which are returned in the reply messages.

Table 6 Fields for Reconciliation IDs

Service	Reconciliation ID Field	Notes
Authorization	ccAuthReply_reconciliationID	For authorization requests, the reconciliation ID is returned only for these processors: <ul style="list-style-type: none"> ■ Chase Paymentech Solutions ■ FDC Compass ■ FDC Nashville Global
Capture	ccCaptureReply_reconciliationID	The reconciliation ID is returned for all capture requests for all processors except RBS WorldPay Atlanta. When you perform multiple partial captures for an authorization, each reply includes a different reconciliation ID for each capture request. To find out whether your processor supports multiple partial captures, see Table 13, "Capture Information for Specific Processors," on page 32.
Credit	ccCreditReply_reconciliationID	The reconciliation ID is returned for all credit requests for all processors.

Payment Processors



Note

In this document, the word *processor* can refer to processors, acquirers, or acquiring processors depending on your location.

Payment processors connect CyberSource servers with acquiring banks. Before you can accept payments, you must register with a payment processor. Your acquiring bank might require you to use a payment processor with which the bank has a business relationship.

CyberSource does not necessarily support all the features that are offered by each processor. This guide describes the payment processing features supported by CyberSource. The beginning of each feature description specifies which payment processors support the feature.

Your processor provides you with unique identification numbers for your account. You must provide these identification numbers to CyberSource Customer Support.

The following table lists the processors and corresponding card types that CyberSource supports for the credit card services.



Only the card types explicitly listed here are supported.

Table 7 Payment Processors and Card Types

Payment Processor	Supported Card Types & Notes
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover, Diners Club, JCB, Carte Blanche
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club, JCB
FDC Nashville Global	Visa, Mastercard, American Express, Discover, Diners Club, JCB
FDMS Nashville	Visa, Mastercard, American Express, Discover, Diners Club, Carte Blanche, JCB
FDMS South	Visa, Mastercard, American Express, Discover, Diners Club, Carte Blanche, JCB <p>Important In 2017, FDMS South will quit accepting authorization requests. If FDMS South is your processor, you need to either update or migrate your account depending on your settlement currency.</p> <p>If you settle transactions in CAD, you must do the following:</p> <ul style="list-style-type: none"> ■ Contact CyberSource Customer Support to have your CyberSource account configured to send authorization requests to a third party who will forward the requests to FDMS South on your behalf. ■ Contact First Data to have your First Data account updated. <p>If you settle transactions in USD, CyberSource recommends that you change your processor to FDC Nashville Global, FDMS Nashville, or FDC Compass.</p>
GPN GPN is the CyberSource name for Global Payments, Inc.'s East processing platform.	Visa, Mastercard, American Express, Discover, Diners Club, JCB
RBS WorldPay Atlanta	Visa, Mastercard, American Express, Discover, Diners Club, JCB
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover, Diners Club, Carte Blanche, JCB

Credit Card Processing

Authorizing a Payment

CyberSource supports authorizations for all processors.

Online Authorizations

Online authorization means that when you submit an order using a credit card, you receive an immediate confirmation about the availability of the funds. If the funds are available, the issuing bank reduces your customer's open to buy, which is the amount of credit available on the card. Most of the common credit cards are processed online. For online authorizations, you typically start the process of order fulfillment soon after you receive confirmation of the order.

Online authorizations expire with the issuing bank after a specific length of time if they have not been captured and settled. Most authorizations expire within five to seven days. The issuing bank sets the length of time.

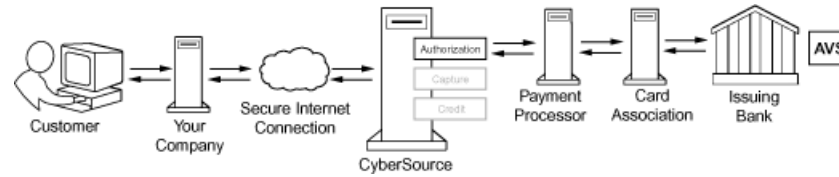
**Note**

CyberSource is not informed by the issuing bank when an authorization expires. By default, the authorization remains in the CyberSource system for 60 days after the authorization date, even after it expires with the issuing bank.

When an authorization expires with the issuing bank, your bank or processor might require you to resubmit an authorization request and include a request for capture in the same message.

The following figure shows the steps that occur when you request an online credit card authorization.

Figure 1 Processing an Online Authorization



- 1 The customer places an order and provides the credit card number, the card expiration date, and additional information about the card.
- 2 You send a request for authorization over a secure Internet connection. When the customer buys a digitally delivered product or service, you can request both the authorization and the capture at the same time. When the customer buys a physically fulfilled product, do not request the capture until you ship the product.
- 3 CyberSource validates the order information then contacts your payment processor and requests authorization.
- 4 The processor sends the transaction to the payment card company, which routes it to the issuing bank for the customer's credit card. Some card companies, including Discover and American Express, act as their own issuing banks.
- 5 The issuing bank approves or declines the request.

Depending on the processor and card type, the issuing bank can use AVS to confirm the billing address and CVN to verify that the customer has possession of the card. See [Chapter 3, "Authorization Features," on page 44](#).

For debit cards and prepaid cards, the issuing bank can approve a partial amount if the balance on the card is less than the requested authorization amount and if the transaction is enabled for partial authorization. For details about partial authorizations and for a list of the processors and card types supported for partial authorizations, see ["Partial Authorizations," page 55](#).



Note

For a limited number of processors and card types, partial authorizations and balance responses are supported for credit cards in addition to debit cards and prepaid cards. See ["Partial Authorizations," page 55](#), and ["Balance Responses," page 60](#).

- 6 CyberSource runs its own tests then tells you whether the authorization succeeded.

Offline Authorizations

Offline authorization means that when you submit an order using a credit card, you do not know whether the funds are available until you capture the order and receive confirmation of payment. You typically do not ship the goods until you receive this payment confirmation. For offline credit cards, it usually takes five days longer to receive payment confirmation than for online cards.

Creating an Authorization Request

Step 1 Do not include any of these services in the request:

- Full authorization reversal (**ccAuthReversalService**)
- Credit (**ccCreditService**)
- Services for other payment methods, such as electronic checks, PayPal, bank transfers, and direct debits

Step 2 Include the required fields in the request:

Table 8 Required Fields for Authorizations

Field	Notes
billTo_city ¹	
billTo_country ¹	
billTo_email ¹	
billTo_firstName ¹	
billTo_lastName ¹	
billTo_postalCode ¹	Required only for transactions in the U.S. and Canada.
billTo_state ¹	Required only for transactions in the U.S. and Canada.
billTo_street1 ¹	
card_accountNumber	
card_cardType	Required for certain card types. CyberSource strongly recommends that you send the card type even if it is optional for your processor. Omitting the card type can cause the transaction to be processed with the wrong card type.
card_expirationMonth ¹	
card_expirationYear ¹	

¹ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45.
Important It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 8 Required Fields for Authorizations (Continued)

Field	Notes
ccAuthService_run	Set to true.
merchantID	
merchantReferenceCode	
purchaseTotals_currency	
purchaseTotals_grandTotalAmount	Either purchaseTotals_grandTotalAmount or item_#_unitPrice must be included in the request.
<p>¹ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p>	

See [Appendix A, "API Fields,"](#) on page 117 for:

- Detailed descriptions of these required request fields
- Optional request fields
- Reply fields

Step 3 If needed, modify the request to accommodate additional information for your processor. See "[Authorization Information for Specific Processors,](#)" page 25.

Step 4 Include authorization features in the request.

There are several authorization features that can be performed automatically depending on the information included in your request. These features are described in [Chapter 3, "Authorization Features,"](#) on page 44.

Step 5 Include optional features in the request.

There are several optional features that you can include in your request. These features are described in [Chapter 5, "Optional Features,"](#) on page 63.

Authorization Information for Specific Processors

The following table provides additional information about authorizations for specific processors.

Table 9 Authorization Information for Specific Processors

Payment Processor	Authorization Information
FDMS South	FDMS South no longer requires you to include all AVS data fields in your requests. The only required AVS data fields are the country code and postal code. All other AVS data fields are optional even though they are marked as required in Table 43, "Request Fields," on page 119 . However, if you omit AVS data fields that were previously required, you might experience an increase in the number of declined transactions and chargebacks. For additional information, contact your processor.
GPN	GPN limits the authorization, capture, and credit amounts to 10 digits.
RBS WorldPay Atlanta	RBS WorldPay Atlanta limits the authorization, capture, and credit amounts to the equivalent of 999,999.99 USD. Depending on the value you send, the decimal is either truncated or appended. For example, if you send 1.123 the decimal is truncated to 1.12. If you send 123 it is converted to 123.00.
TSYS Acquiring Solutions	TSYS Acquiring Solutions limits authorization and capture amounts to the equivalent of 99,999.99 USD. To process an amount greater than this, contact TSYS Acquiring Solutions.

Reversing an Authorization

The full authorization reversal service releases the hold that the authorization placed on the customer's credit card funds. Use this service to reverse an unnecessary or undesired authorization.



Note

Each issuing bank has its own rules for deciding whether a full authorization reversal succeeds or fails. If your reversal fails, contact the issuing bank to find out whether it is possible to reverse the authorization by alternate means.

If your processor supports authorization reversal after void (ARAV), you can reverse an authorization after you void the associated capture. See "[Authorization Reversal after Void \(ARAV\)](#)," [page 28](#). If your processor does not support ARAV, you can use the full authorization reversal service only for an authorization that has not been captured and settled.

Supported Processors and Card Types

The following table lists the processors that are supported for full authorization reversals. For processors that support debit cards and prepaid cards, the full authorization reversal service works for debit cards and prepaid cards in addition to credit cards.

Table 10 Processors That Support Full Authorization Reversals

Processor	Card Types and Notes
Chase Paymentech Solutions	<p>Card types supported for full authorization reversals: Visa, Mastercard, Discover, and Diners Club.</p> <p>Time limit: a full authorization reversal must occur within three days of the authorization.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>
FDC Compass	<p>Card types supported for full authorization reversals: Visa, Mastercard, American Express, Discover, Diners Club, and JCB.</p> <p>Time limit: a full authorization reversal must occur within three days of the authorization.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>
FDC Nashville Global	<p>Card types supported for full authorization reversals: Visa, Mastercard, American Express, Discover, Diners Club, and JCB (US Domestic).</p> <p>For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.</p> <p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>
FDMS Nashville	<p>Card types supported for full authorization reversals: Visa, Mastercard, Discover, Diners Club, and JCB (US Domestic).</p> <p>For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.</p> <p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>

Table 10 Processors That Support Full Authorization Reversals (Continued)

Processor	Card Types and Notes
FDMS South	<p>Card types supported for full authorization reversals: Visa, Mastercard, Discover, and JCB (US Domestic).</p> <p>For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.</p> <p>Full authorization reversals:</p> <ul style="list-style-type: none"> ■ Are supported only for transactions that do not go through a currency conversion. ■ Are supported for the following types of merchants and currencies: <ul style="list-style-type: none"> ● Merchants located in the U.S. who authorize, settle, and fund in U.S. dollars. ● Merchants located in Canada who authorize, settle, and fund in Canadian dollars. <p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>
GPN	<p>Card types supported for full authorization reversals: Visa, Mastercard, Discover, Diners Club, and JCB.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>
RBS WorldPay Atlanta	<p>Card types supported for full authorization reversals: Visa, Mastercard, American Express, and Discover.</p>
TSYS Acquiring Solutions	<p>Card types supported for full authorization reversals: Visa, Mastercard, American Express, Discover, Diners Club, and JCB.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>

Creating a Full Authorization Reversal Request

A full authorization reversal is a follow-on transaction that uses the request ID returned from a previous authorization. The request ID links the full authorization reversal to the authorization. CyberSource uses the request ID to look up the customer's billing and account information from the original authorization, so you are not required to include those fields in your full authorization reversal request.

For information about requesting a follow-on service, see [Getting Started with CyberSource Essentials](#).

To create a full authorization reversal request:

Step 1 Do not include any other CyberSource services in the request.

Step 2 Include the required fields in the request:

Table 11 Required Fields for Full Authorization Reversals

Field	Notes
ccAuthReversalService_authRequestID	Set to the request ID that was included in the authorization reply message.
ccAuthReversalService_run	Set to <code>true</code> .
merchantID	
merchantReferenceCode	
purchaseTotals_currency	
purchaseTotals_grandTotalAmount	Either purchaseTotals_grandTotalAmount or item_#_unitPrice must be included in the request.

See [Appendix A, "API Fields,"](#) on page 117 for:

- Detailed descriptions of these required request fields
- Optional request fields
- Reply fields

Step 3 Make sure the amount of the reversal is the same as the amount that was authorized:

- You cannot partially reverse an authorization; you can reverse an authorization only for its full amount.
 - When you use a debit card or prepaid card and only a partial amount was approved, the amount of the reversal must be the amount that was authorized, not the amount that was requested.
-

Authorization Reversal after Void (ARAV)

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- FDMS South

- GPN
- TSYS Acquiring Solutions

This feature enables you to reverse an authorization after you void the associated capture.



Important

This functionality enables you to meet the Visa mandate requirements to reverse unused authorizations, and it benefits the cardholder by releasing the hold on unused credit card funds.

To reverse an authorization after a void:

Step 1 Void a capture. See "[Voiding a Capture or Credit](#)," page 41.

Step 2 Reverse the authorization associated with the capture. See "[Reversing an Authorization](#)," page 25.



Note

You might need to perform additional steps if you performed multiple partial captures for the authorization. To find out whether your processor supports multiple partial captures, see "[Multiple Partial Captures](#)," page 35. For information about multiple captures and ARAV, see "[Multiple Partial Captures and Authorization Reversal after Void](#)," page 36.

Capturing an Authorization

CyberSource supports captures for all processors.

When you are ready to fulfill a customer's order and transfer funds from the customer's bank to your bank, capture the authorization for that order.

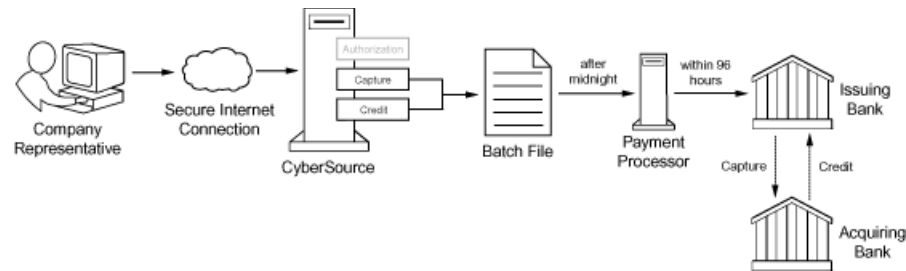
If you can fulfill only part of a customer's order, do not capture the full amount of the authorization. Capture only the cost of the items that you ship. When you ship the remaining items, request a new authorization, and then capture the new authorization.

Captures

Unlike authorizations, a capture does not happen in real time. All of the capture requests for a day are placed in a batch file and sent to the processor. In most cases, the batch is settled at night. It usually takes two to four days for your acquiring bank to deposit funds in your merchant bank account.

The following figure shows the steps that occur when you request a capture or credit.

Figure 2 Processing a Capture or Credit



- 1 You send a request for capture or credit over a secure Internet connection.
- 2 CyberSource validates the order information then stores the capture or credit request in a batch file.
- 3 After midnight, CyberSource sends the batch file to your payment processor.
- 4 The processor settles the capture or credit request and transfers funds to the appropriate bank account.



Note

The processor does not notify CyberSource when a transaction is declined. To ensure that all captures and credits are processed, reconcile your system's reports with the reports from your processor. See [Getting Started with CyberSource Essentials](#) for information about reconciliation.

Due to the potential delay between authorization and capture, the authorization might expire with the issuing bank before you request capture. Most authorizations expire within five to seven days. If an authorization expires with the issuing bank before you request the capture, your bank or processor might require you to resubmit an authorization request and include a request for capture in the same message.



Note

CyberSource is not informed by the issuing bank when an authorization expires. By default, the authorization remains in the CyberSource system for 60 days after the authorization date, even after it expires with the issuing bank.

Creating a Capture Request

A capture is a follow-on transaction that uses the request ID returned from a previous authorization. The request ID links the capture to the authorization. CyberSource uses the request ID to look up the customer's billing and account information from the original authorization, so you are not required to include those fields in your capture request.

For information about requesting a follow-on service, see [Getting Started with CyberSource Essentials](#).

To create a capture request:

Step 1 Do not include any of these services in the request:

- Full authorization reversal (**ccAuthReversalService**)
- Credit (**ccCreditService**)
- Services for other payment methods, such as electronic checks, PayPal, bank transfers, and direct debits

Step 2 Include the required fields in the request:

Table 12 Required Fields for Captures

Field	Notes
ccCaptureService_run	Set to <code>true</code> .
ccCaptureService_authRequestID	Set to the request ID that was included in the authorization reply message. Optional when ccAuthService and ccCaptureService are in the same request.
merchantID	
merchantReferenceCode	
purchaseTotals_currency	
purchaseTotals_grandTotalAmount	Either purchaseTotals_grandTotalAmount or item#_unitPrice must be included in the request.

See [Appendix A, "API Fields,"](#) on page 117 for:

- Detailed descriptions of these required request fields
- Optional request fields
- Reply fields

Step 3 If needed, modify the request to accommodate additional information for your processor. See [Table 13, "Capture Information for Specific Processors,"](#) on page 32.

Step 4 Include optional features in the request.

There are several optional features that you can include in your request. These features are described in [Chapter 5, "Optional Features,"](#) on page 63.

Capture Information for Specific Processors

The following table provides additional information about captures for some processors.

Table 13 Capture Information for Specific Processors

Payment Processor	Capture Information
Chase Paymentech Solutions	<p>Multiple partial captures are supported. See "Multiple Partial Captures," page 35.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>
FDC Compass	<p>Multiple partial captures are supported. See "Multiple Partial Captures," page 35.</p> <p>Special request fields for multiple partial captures are recommended. See "Special Request Fields for Multiple Partial Captures," page 35.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>
FDC Nashville Global	<p>CyberSource always provides merchant descriptor information to the processor for you for all capture and credit transactions. See "Merchant Descriptors," page 76.</p> <p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>
FDMS Nashville	<p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>
FDMS South	<p>Important ARAV is supported. See "Authorization Reversal after Void (ARAV)," page 28.</p>
GPN	<p>GPN limits the authorization, capture, and credit amounts to 10 digits.</p> <p>Multiple partial captures are supported. See "Multiple Partial Captures," page 35.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>

Table 13 Capture Information for Specific Processors (Continued)

Payment Processor	Capture Information
TSYS Acquiring Solutions	<p>Multiple partial captures are supported. See "Multiple Partial Captures," page 35.</p> <p>Special request fields for multiple partial captures are required. See "Special Request Fields for Multiple Partial Captures," page 35.</p> <p>Important ARAV is supported. See "Multiple Partial Captures and Authorization Reversal after Void," page 36.</p>

Capture Features

Automatic Partial Authorization Reversals

Processors and card types:

See the following table.

Table 14 Processors That Support Automatic Partial Authorization Reversals

Processor	Card Types
Chase Paymentech Solutions ¹	Visa, Mastercard
FDC Compass ¹	Visa, Mastercard
FDC Nashville Global	Visa, Mastercard, Discover, Diners Club, JCB (US Domestic) ²
FDMS Nashville	Visa, Mastercard, Discover, Diners Club, JCB (US Domestic) ²
FDMS South	Visa, Mastercard, Discover, JCB (US Domestic) ²
GPN	Visa, Mastercard
	On GPN, automatic partial authorization reversal is performed as part of interchange optimization, which is described in "Interchange Optimization," page 34.
TSYS Acquiring Solutions	Visa, Mastercard, Discover, Diners Club, JCB

¹ The processor performs an automatic partial authorization reversal when there is an interchange benefit. The processor does not allow CyberSource to perform this functionality.

² For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.

In addition to credit cards, automatic partial authorization reversals are supported for:

- Debit cards and prepaid cards: see [Chapter 4, "Debit Cards and Prepaid Cards," on page 55](#).
- Quasi-cash: see ["Quasi-Cash," page 103](#).

If the capture amount is less than the authorization amount, CyberSource automatically performs a partial authorization reversal before it sends the capture request to the processor. The results of a successful partial authorization reversal are:

- The capture amount matches the new authorization amount at the payment card company.
- The hold on the unused credit card funds might be released. The issuing bank decides whether or not to release the hold on unused funds.



Note

Not all issuers act on a request for a partial authorization reversal. Therefore, CyberSource cannot guarantee that the funds will be released.

Interchange Optimization

Processor:

- GPN acquiring merchants: Visa

Interchange optimization helps you reduce your interchange fees. Interchange optimization consists of:

- Automatic authorization refresh: When the capture request occurs more than six days after the date of the original authorization, CyberSource automatically obtains a fresh authorization for the capture amount.

On GPN, the fresh authorization uses the same authorization indicator as the original authorization. For more information, see ["Final Authorization Indicator," page 68](#).

- Automatic partial authorization reversal: If the capture does not need a fresh authorization but the capture amount is less than the authorization amount, CyberSource automatically performs a partial authorization reversal which releases the hold on unused credit card funds and ensures that the settlement amount matches the authorization amount.



Note

Interchange optimization does not work for card-present transactions.

To enable interchange optimization, contact CyberSource Customer Support to have your account configured for this feature.

Multiple Partial Captures

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global: multiple partial captures are supported only for card-not-present transactions; they are not supported for card-present transactions.
- FDMS Nashville: multiple partial captures are supported only for card-not-present transactions; they are not supported for card-present transactions.
- GPN
- TSYs Acquiring Solutions

This feature enables you to request multiple partial captures for one authorization. You must ensure that the total amount of all the captures does not exceed the authorized amount.

Special Request Fields for Multiple Partial Captures

Processors:

- FDC Compass. To avoid a downgrade for a Visa transaction, the special request fields are required. For other card types, CyberSource strongly recommends that you include the special request fields.
- FDC Nashville Global. The special request fields are required for Visa and Mastercard transactions. They are not supported for other card types.
- FDMS Nashville. The special request fields are required for Visa and Mastercard transactions. They are not supported for other card types.
- TSYs Acquiring Solutions. The special request fields are required.

Include the following special request fields in each capture request when you are requesting multiple partial captures:

- ccCaptureService_sequence
- ccCaptureService_totalCount

If you do not know the total number of captures that you are going to request, set the capture total count to an estimated value or 99 for all capture requests except the final one. For the final capture request, set the capture total count and the capture sequence to the same value.

Multiple Partial Captures and Authorization Reversal after Void

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- GPN
- TSYS Acquiring Solutions

This feature enables you to reverse an authorization after you void the associated capture.



Important

This functionality enables you to meet the Visa mandate requirements to reverse unused authorizations, and it benefits the cardholder by releasing the hold on unused credit card funds.

For an authorization that has multiple associated captures:

- If you reverse the authorization, CyberSource declines subsequent capture requests.
- If you void only one of the multiple captures, CyberSource declines subsequent authorization reversal requests.
- If you void all of the multiple captures, you can reverse the authorization.

To reverse an authorization after a void for multiple captures:

- Step 1** Void each capture associated with the authorization. See ["Voiding a Capture or Credit," page 41](#).
 - Step 2** Reverse the authorization. See ["Reversing an Authorization," page 25](#).
-

Performing a Sale

A sale is a bundled authorization and capture. You can use a sale instead of a separate authorization and capture if there is no delay between taking a customer's order and shipping the goods. A sale is typically used for electronic goods and for services that you can turn on immediately.

To perform a sale, request the authorization and capture services at the same time. Include the request fields that are required for the authorization. No additional fields are required for the capture.

If the authorization is successful, CyberSource processes the capture immediately and the reply message includes results for the authorization and for the capture. If the authorization is declined, CyberSource does not process the capture and the reply message includes results only for the authorization.

For debit cards and prepaid cards, the issuing bank can approve a partial amount if the balance on the card is less than the requested authorization amount and if the transaction is enabled for partial authorization. When this happens, CyberSource does not process the capture. However, you can submit a capture request for the approved amount. For details about partial authorizations and for a list of the processors and card types supported for partial authorizations, see "[Partial Authorizations](#)," page 55.



For a limited number of processors and card types, partial authorizations are supported for credit cards in addition to debit cards and prepaid cards. See "[Partial Authorizations](#)," page 55.

For details about authorizations and captures, see "[Authorizing a Payment](#)," page 21, and "[Capturing an Authorization](#)," page 29.

Crediting a Payment

CyberSource supports credits for all processors.

When your request for a credit is successful, the issuing bank for the credit card takes money out of your merchant bank account and returns it to the customer. It usually takes two to four days for your acquiring bank to transfer funds from your merchant bank account.



Carefully control access to this service to prevent unauthorized credits. Do not request this service directly from your customer interface. Instead, incorporate this service as part of your customer service process.

Credit requests are batched in the same manner as captures. See "[Captures](#)," page 30.

Types of Credits

A *follow-on credit* is linked to a capture in the CyberSource system. You can request multiple follow-on credits against a single capture. You must request a follow-on credit within 60 days of the authorization.



When you combine a request for a follow-on credit with a request for another service, you must provide the customer's billing and account information.

A *stand-alone credit* is not linked to a capture. There is no time limit for requesting stand-alone credits. Instead of sending the request ID field in the credit request, the request must include the fields for the customer's billing and account information.



For stand-alone credits, CyberSource does not validate **billTo_postalCode** or **shipTo_postalCode**.

Creating a Credit Request

A follow-on credit uses the request ID returned from a previous capture to link the credit to the capture. CyberSource uses the request ID to look up the customer's billing and account information from the original authorization, so you are not required to include those fields in your credit request. To perform multiple partial follow-on credits, send the same request ID in each follow-on credit request.

For information about requesting a follow-on service, see [Getting Started with CyberSource Essentials](#).

To create a credit request:

Step 1 Do not include any of these services in the request:

- Any other credit card services (**ccAuthService**, **ccAuthReversalService**, or **ccCaptureService**)
- Services for other payment methods, such as electronic checks, PayPal, bank transfers, and direct debits

Step 2 Include the required fields in the request:

Table 15 Required Fields for Credits

Field	Notes
ccCreditService_run	Set to <code>true</code> .
ccCreditService_captureRequestID	For a follow-on credit, set to the request ID that was included in the capture reply message. Not used for a stand-alone credit.
merchantID	
merchantReferenceCode	
purchaseTotals_currency	
purchaseTotals_grandTotalAmount	Either purchaseTotals_grandTotalAmount or item#_unitPrice must be included in the request.

See [Appendix A, "API Fields,"](#) on page 117 for:

- Detailed descriptions of these required request fields
- Optional request fields
- Reply fields

Step 3 For a stand-alone credit, include additional required fields:

Table 16 Additional Required Fields for Stand-Alone Credits

Field	Notes
billTo_city ¹	
billTo_country ¹	
billTo_email ¹	
billTo_firstName ¹	
billTo_lastName ¹	
billTo_postalCode ¹	Required only for transactions in the U.S. and Canada.
billTo_state ¹	Required only for transactions in the U.S. and Canada.
billTo_street1 ¹	
card_accountNumber	
card_cardType	Required for certain card types. CyberSource strongly recommends that you send the card type even if it is optional for your processor. Omitting the card type can cause the transaction to be processed with the wrong card type.
card_expirationMonth ¹	
card_expirationYear ¹	
¹ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.	

Step 4 If needed, modify the request to accommodate additional information for your processor. See ["Credit Information for Specific Processors," page 41](#).

Step 5 Include optional features in the request. See [Chapter 5, "Optional Features," on page 63](#).

Credit Information for Specific Processors

The following table provides additional information about credits for some processors.

Table 17 Credit Information for Specific Processors

Payment Processor	Credit Information
FDC Nashville Global	CyberSource always provides merchant descriptor information to the processor for you for all capture and credit transactions. See " Merchant Descriptors ," page 76.
FDMS South	FDMS South no longer requires you to include all AVS data fields in your requests. The only required AVS data fields are the country code and postal code. All other AVS data fields are optional even though they are marked as required in Table 43, "Request Fields," on page 119. However, if you omit AVS data fields that were previously required, you might experience an increase in the number of declined transactions and chargebacks. For additional information, contact your processor.
GPN	GPN limits the authorization, capture, and credit amounts to 10 digits.
RBS WorldPay Atlanta	Follow-on refunds for verbal authorizations are not supported. You must process these refunds as stand-alone refunds.

Voiding a Capture or Credit

CyberSource supports voids for all processors.

A void cancels a capture or credit request that you submitted to CyberSource. A transaction can be voided only when CyberSource has not already submitted the capture or credit request to your processor. CyberSource usually submits capture and credit requests to your processor once a day, so your window for successfully voiding a capture or credit request is small. CyberSource declines your void request when the capture or credit request has already been sent to the processor.

You cannot perform a follow-on credit for a transaction that has been voided.

You cannot undo a void.

When you void a capture, a hold remains on the unused credit card funds. If you are not going to re-capture the authorization as described in "[Capture after Void](#)," page 42, and if your processor supports authorization reversal after void as described in "[Authorization Reversal after Void \(ARAV\)](#)," page 28, CyberSource recommends that you request an authorization reversal to release the hold on the unused credit card funds.

Capture after Void

If your processor supports multiple captures, you can capture an authorization after you void previous captures associated with the authorization. For example, you can perform the following sequence:

- 1 Authorize a payment.
- 2 Capture the authorization.
- 3 Void the capture.
- 4 Capture the authorization again.

To find out whether your processor supports multiple captures, see ["Multiple Partial Captures," page 35](#).

On all other processors, when you void a transaction the transaction is at the end of its life and cannot be the source of another follow-on capture or credit. For example, if you authorize and capture a transaction, and then you void the capture, you cannot submit another capture request that uses the authorization code or CyberSource request ID from the original authorization. If you still want to capture that transaction, you must re-authorize the transaction and capture the new authorization.

Creating a Void Request

A void is a follow-on transaction that uses the request ID returned from a capture or credit. The request ID links the void to the service that is being voided. CyberSource uses the request ID to look up the customer's billing and account information from the capture or credit, so you are not required to include those fields in your void request.

For information about requesting a follow-on service, see [Getting Started with CyberSource Essentials](#).

To create a void request:

Step 1 Do not include any other CyberSource services in the request.

Step 2 Include the required fields in the request:

Table 18 Required Fields for Voids

Field	Notes
merchantID	
merchantReferenceCode	
voidService_run	Set to <code>true</code> .
voidService_voidRequestID	Set to the request ID that was included in the capture or credit reply message.

See [Appendix A, "API Fields,"](#) on page 117 for:

- Detailed descriptions of these required request fields
 - Reply fields
-

Authorization Features

You must support the authorization features that your processor supports.

Address Verification System (AVS)



Note

AVS is supported only for cards issued in the U.K., the U.S., and Canada.

The following table lists the processors and card types for which CyberSource returns standard AVS results.

Table 19 Processors That Support Standard AVS

Processors	Credit Card Types
Chase Paymentech Solutions	Visa, Mastercard, and American Express: The billing country must be the U.S., Canada, or Great Britain.
	Discover, Diners Club, and JCB: The billing country must be the U.S.
FDC Compass	Visa, Mastercard, and American Express: The billing country must be the U.S., Canada, or Great Britain.
	Discover and Diners Club: The billing country must be the U.S.
FDC Nashville Global	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.
FDMS Nashville	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.

Table 19 Processors That Support Standard AVS (Continued)

Processors	Credit Card Types
FDMS South	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB
RBS WorldPay Atlanta	Visa, Mastercard, American Express, Discover, Diners Club
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Diners Club: The billing country must be the U.S.

Relaxed Requirements for Address Data and Expiration Date

Services:

- Authorization
- Stand-alone credit

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS South
- GPN

To enable relaxed requirements for address data and expiration date, contact CyberSource Customer Support to have your account configured for this feature.

Historically, this data was mandated by CyberSource. With the advent of digital payments and an increasingly global e-commerce environment, CyberSource decided to relax the requirements for address data and expiration date.

Relaxed requirements for address data and expiration date make the following fields optional for payment processing:

- billTo_city
- billTo_country
- billTo_email
- billTo_firstname
- billTo_lastname
- billTo_postalCode: if you include this field in your request, you must also include **billTo_country**.
- billTo_state
- billTo_street1
- card_expirationMonth: if you include this field in your request, you must also include **card_expirationYear**.
- card_expirationYear: If you include this field in your request, you must also include **card_expirationDate**.



Important

When relaxed requirements for address data and expiration date are enabled for your CyberSource account, and your service request does not include one or more of the fields in the preceding list, you increase the risk of declined transactions and fraud depending on your location, your processor, and the cardholder's issuing bank.

It is your responsibility to determine whether a field is required for the transaction you are requesting. For example, effective October 2014, an issuing bank can decline an authorization request for a recurring transaction with a Visa Europe card if the expiration date is incorrect, invalid, or missing. If you do not provide the correct expiration date for a recurring transaction the authorization request may be declined.

Processing AVS Codes

When a processor supports AVS for a transaction's card type, the issuing bank uses AVS to confirm that the customer has provided the correct billing address. When a customer provides incorrect information, the transaction might be fraudulent.

AVS occurs automatically with every authorization request. The authorization reply includes the **ccAuthReply_avsCode** field, which contains the AVS code from the issuing bank that indicates whether AVS matched the address and whether the address match was partial or complete. See [Appendix D, "AVS Codes," on page 172](#).

When AVS cannot verify the address, but the authorization is otherwise valid, you might receive an AVS decline. You can capture authorizations that receive an AVS decline.

However, you must review these orders to ensure that they are legitimate. Settling authorizations that fail the AVS check might have an impact on the fees charged by your bank. Contact your bank for details about how AVS management might affect your discount rate.

The **ccAuthReply_avsCodeRaw** field is the raw AVS code sent directly from the processor. Do not use this value to handle the AVS response. Use the value only for debugging purposes.

Electronic Verification (EV)

Processors:

- FDC Nashville Global
- TSYS Acquiring Solutions

Card types:

- American Express
- Discover—only on TSYS Acquiring Solutions. Only the first name and last name are checked.

EV confirms the customer's billing information. When a customer provides incorrect information, the transaction might be fraudulent.



Note

As part of EV for TSYS Acquiring Solutions, you can provide the IP address in the **billTo_ipAddress** field. When you provide the IP address, American Express does not send a response for it. Instead, American Express uses the IP address to run a check in their internal database to ensure that the IP address does not match previously fraudulent transactions with the same IP address and is not from countries that American Express has determined to be a high risk for fraud. If, based on the IP address, American Express determines that the transaction is fraudulent or is a high risk for fraud, American Express declines the transaction.

Request Fields

To receive an EV response code for a particular value, you must include that value in your authorization request. [Table 20, "Request Fields for Electronic Verification," on page 48](#) lists the request fields for each value that EV can verify. In the table, the R/O column indicates whether the field is required or optional for the authorization service.



Note

Some merchants use placeholder data for some required fields, such as addresses and phone numbers, because their customers do not provide them with the required information. The benefit of using certain specific placeholder values is that Smart Authorization ignores the values instead of attempting to process them. However, when you use placeholder data in any of the fields that are used for EV, the corresponding EV results are invalid.

Table 20 Request Fields for Electronic Verification

Value That Is Being Verified	R/O for Authorizations	Request Field
Email	R	billTo_email
First name	R	billTo_firstName
Last name	R	billTo_lastName
Phone number	O	billTo_phoneNumber
Postal code	R/O ¹	billTo_postalCode
Street address	R	billTo_street1

¹ Required when the billing country is the U.S. or Canada; otherwise, optional.

Reply Fields

For each verified value, EV returns a raw response code and a mapped response code:

- The *raw response code* is the value returned by the processor.
- The *mapped response code* is the pre-defined CyberSource value that corresponds to the raw response code. [Appendix G, "Electronic Verification Response Codes,"](#) on [page 177](#) describes the mapped response codes.

The following table lists the reply fields for each value that EV can verify.

Table 21 API Fields for Electronic Verification Responses

Value That Is Being Verified	API Field for Mapped Response	API Field for Raw Response
Email	ccAuthReply_evEmail	ccAuthReply_evEmailRaw
First name and last name	ccAuthReply_evName	ccAuthReply_evNameRaw
Phone number	ccAuthReply_evPhoneNumber	ccAuthReply_evPhoneNumberRaw
Postal code	ccAuthReply_evPostalCode	ccAuthReply_evPostalCodeRaw
Street address	ccAuthReply_evStreet	ccAuthReply_evStreetRaw

Card Verification Numbers (CVNs)

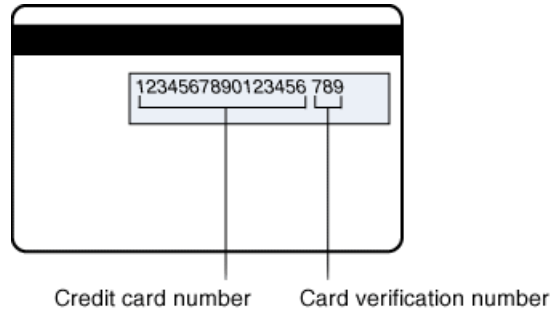
Table 22 Processors That Support CVNs

Processors	Credit Card Types
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover
FDC Compass	Visa, Mastercard, American Express, Discover
FDC Nashville Global	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) Note For JCB cards, “US Domestic” means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.
FDMS Nashville	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) Note For JCB cards, “US Domestic” means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.
FDMS South	Visa, Mastercard, American Express, Discover, Diners Club, JCB (US Domestic) Note For JCB cards, “US Domestic” means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.
GPN	Visa, Mastercard, American Express, Discover, Diners Club
RBS WorldPay Atlanta	Visa, Mastercard, American Express, Discover, Diners Club
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover, Diners Club

CVN Locations and Terminology

The CVN, which is printed or embossed on the back of the card, can be sent with the request and verified to help reduce the risk of fraud.

Figure 3 Example of a Visa Card Verification Number



Each payment card company has its own name for this value:

- Visa calls it the *Card Verification Value (CVV2)*.
- American Express and Discover call it the *Card Identification Digits (CID)*.
- Mastercard calls it the *Card Validation Code (CVC2)*.

To use the CVN, include the **card_cvNumber** field in the request. This number is never transferred during card swipes and should be known only by the cardholder.

CVN Codes

The reply message includes a raw response code and a mapped response code:

- The *raw response code* is the value returned by the processor. This value is returned in the **ccAuthReply_cvCodeRaw** field. Use this value only for debugging purposes; do not use it to determine the card verification response.
- The *mapped response code* is the pre-defined CyberSource value that corresponds to the raw response code. This value is returned in the **ccAuthReply_cvCode** field. [Appendix F, "CVN Codes," on page 176](#) describes the mapped response codes.

Even when the CVN does not match the expected value, the issuing bank might still authorize the transaction. You will receive a CVN decline from CyberSource, but you can still capture the transaction because it has been authorized by the bank. However, you must review the order to ensure that it is legitimate.

Settling authorizations that fail the CVN check might have an impact on the fees charged by your bank. Contact your bank for details about how card verification management might affect your discount rate.

Table 23 CVN Results for Each Card Type

Card Type	CVN Results
American Express	<p>A ccAuthReply_cvCode value of 1 indicates that your account is not configured for CVN. Contact CyberSource Customer Support to have your account enabled for this feature.</p> <p>To use the CVN with American Express, see "Testing American Express Card Verification," page 116.</p>
Discover	<p>For FDC Nashville Global, FDMS Nashville, and FDMS South:</p> <ul style="list-style-type: none"> CVN results can be returned for any of the card types on the Discover Network as described in "Discover Acquisitions and Alliances," page 13. The CVN results are returned to you and it is your responsibility to decide whether or not to accept the transaction. <p>For all other processors, when the CVN does not match:</p> <ul style="list-style-type: none"> Discover refuses the card and the request is declined. The reply message does not include the ccAuthReply_cvCode field, which indicates that the CVN failed.
Visa and Mastercard	<p>A CVN code of D or N causes CyberSource to decline the request with reason code 230. You can still capture the transaction, but you must review the order to ensure that it is legitimate.</p> <p>Note CyberSource, not the issuing bank, assigns the CVN decline to the authorization. You can capture any authorization that has a valid authorization code from the issuing bank, even when the request receives a CVN decline.</p> <p>When the issuing bank does not authorize the transaction and the CVN does not match, the request is declined because the card is refused. You cannot capture the transaction.</p>

Verbal Authorizations

CyberSource supports verbal authorizations for these processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- FDMS South
- GPN
- RBS WorldPay Atlanta
- TSYS Acquiring Solutions

When you request an authorization through CyberSource, the issuing bank might ask you to call the payment processor to answer questions about the transaction. When this happens, the processor gives you a verbal authorization code for the transaction. To capture a verbally authorized transaction, send the verbal authorization code in the capture request. Make sure your customer service and point-of-sale staff can enter verbal authorization codes into your system.

You can use a verbal authorization to capture an authorization that was declined for any of these reasons:

- Verbal authorization required
- Card expired
- Card refused
- Invalid card



Important

Do not confuse verbal authorizations with forced captures:

- With a verbal authorization, you obtain the authorization code directly from the processor or issuing bank after requesting an authorization through CyberSource and receiving a CyberSource decline.
- With a forced capture, you get the authorization code by authorizing a payment outside of CyberSource. See "[Forced Captures](#)," page 72.

In both cases, you must follow up with a capture that uses the CyberSource system.

A verbal authorization works as follows:

- 1 The authorization reply includes reason code 201, which indicates that the issuing bank is requiring a verbal authorization.

For the American Express card type on FDMS Nashville, the authorization reply also includes a referral response number in **ccAuthReply_referralResponseNumber**. You will be asked for this number, which identifies the failed transaction, when you call American Express for the verbal authorization.

- 2 You call the processor to answer questions about the transaction.
- 3 When the processor verbally authorizes the transaction, the processor gives you a verbal authorization code.

- 4 You include the verbal authorization code in your capture request:
- Send the verbal authorization code in the **ccCaptureService_verbalAuthCode** field.
 - Send the word `VERBAL` in the **ccCaptureService_authType** field.
If you don't set **ccCaptureService_authType** to `VERBAL`, the **ccCaptureService_verbalAuthCode** field is ignored.
 - For the American Express card type on FDMS South, the **ccCaptureService_posData** and **ccCaptureService_transactionID** fields are required to comply with the CAPN requirements.



American Express has indicated that capture requests submitted without a valid transaction ID, including transactions that originated as verbal authorizations, might incur additional transaction charges. Contact your American Express account representative to find out whether your processing is affected by these additional transaction charges.

Debit Cards and Prepaid Cards

Debit cards and prepaid cards are processed using the credit card services described in this document. This chapter describes the special features that are available for debit cards and prepaid cards.



Note

When you use the Simple Order API in XML format, you must use version 1.52 or later of the XML schema to implement partial authorizations or balance responses.

Partial Authorizations



Note

The partial authorization functionality does not apply to credit cards.

For debit cards and prepaid cards, the issuing bank can approve a partial amount if the balance on the card is less than the requested authorization amount.

Supported Processors and Card Types

The following table lists the processors and card types for which CyberSource supports partial authorizations. If your processor and card type are not listed in the table, see ["Unsupported Processors and Card Types," page 62](#).

Table 24 Processors Supported for Partial Authorizations

Processor	Card Types for Debit Cards and Prepaid Cards
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover, Diners Club
FDC Compass ¹	Visa, Mastercard, American Express, Discover
FDC Nashville Global	Visa, Mastercard, American Express, Discover ² , Diners Club ² , JCB (US Domestic) ^{2,3}
FDMS Nashville	Visa, Mastercard, American Express, Discover ² , Diners Club ² , JCB (US Domestic) ^{2,3}

Table 24 Processors Supported for Partial Authorizations (Continued)

Processor	Card Types for Debit Cards and Prepaid Cards
FDMS South ⁴	Visa, Mastercard, American Express, Discover ² , JCB (US Domestic) ^{2,3}
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover, Diners Club, JCB

1 FDC Compass might support partial authorizations for additional card types in the future so be prepared to handle partial authorizations for all card types if your account is enabled for partial authorizations.

2 For this card type on the specified processor, partial authorizations are supported for credit cards in addition to debit cards and prepaid cards.

3 For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands.

4 FDMS South might support partial authorizations for additional card types in the future so be prepared to handle partial authorizations for all card types if your account is enabled for partial authorizations.

Opting In



Note

If you accept American Express cards and Chase Paymentech Solutions is your processor, see ["Special Processing for American Express Cards on Chase Paymentech Solutions," page 58](#).

You must opt in to be able to receive and capture partial authorizations. There are two ways to opt in:

- You can call CyberSource Customer Support to have your account enabled for partial authorizations. When you do this, all your authorization requests are enabled for partial authorizations.

or

- You can set **ccAuthService_partialAuthIndicator** to `true` in your authorization or sale request. When you do this, only that specific transaction is enabled for partial authorization.



Note

When your account is enabled for partial authorizations, you can disable partial authorization for a specific transaction by setting **ccAuthService_partialAuthIndicator** to `false` in your authorization or sale request.

How a Partial Authorization Works



Support for your processor and card type, as listed in [Table 24, "Processors Supported for Partial Authorizations," on page 55](#), does not guarantee a partial authorization. The issuing bank decides whether or not to approve a partial amount.

When the balance on a debit card or prepaid card is less than the requested authorization amount, the issuing bank can approve a partial amount. When this happens, you can accept multiple forms of payment for the order starting with some or all of the approved amount followed by one or more different payment methods:

- 1 If your account is not configured for partial authorizations, you must enable partial authorizations for the transaction by setting `ccAuthService_partialAuthIndicator` to `true` in your request.



If you accept American Express cards and Chase Paymentech Solutions is your processor, see ["Special Processing for American Express Cards on Chase Paymentech Solutions," page 58](#).

- 2 You submit an authorization request or a sale request for a debit card or prepaid card.
- 3 The authorization reply message from CyberSource includes:
 - `ccAuthReply_requestAmount`: amount you requested
 - `ccAuthReply_requestCurrency`: currency for the amount you requested
 - `ccAuthReply_amount`: amount that was authorized
 - `purchaseTotals_currency`: currency for the amount that was authorized
 - `requestID`: value you can use to link this authorization request to subsequent transactions



If you requested a sale, the authorization was not captured.

- 4 You submit a capture request for the partial authorization.

If you capture only part of the approved amount, CyberSource or your processor might be able to perform an automatic partial authorization reversal for you. See ["Automatic Partial Authorization Reversals," page 33](#).



If you do not capture the partial authorization, you must request a full authorization reversal if this service is supported for your processor and card type. See ["Reversing an Authorization," page 25](#).

- 5 You use one or more different payment methods for the rest of the order amount.

When you process these payment methods through CyberSource, you can use the **linkToRequest** field to link the payment requests to the original authorization request. Set **linkToRequest** to the **requestID** value that was returned in the reply message for the original authorization request.

Special Processing for American Express Cards on Chase Paymentech Solutions

If you accept American Express cards and Chase Paymentech Solutions is your processor, perform the following procedure to opt in to partial authorizations.

To opt in to partial authorizations for American Express cards on Chase Paymentech Solutions:

- Step 1** Contact Chase Paymentech Solutions to have your account enabled for partial authorizations for the American Express card type. The transaction division for partial authorizations for American Express should be set to 3.



This step is only for the American Express card type on Chase Paymentech Solutions. For all other card types on Chase Paymentech Solutions, the transaction division for partial authorizations should be set to the default value of 0 (zero).

- Step 2** Contact CyberSource Customer Support to have your account enabled for partial authorizations.

After your accounts have been enabled for partial authorizations at Chase Paymentech Solutions and at CyberSource, you can disable partial authorizations for a specific transaction by setting **ccAuthService_partialAuthIndicator** to `false` in your authorization or sale request.

Real-Time Reversals

There are two kinds of real-time reversals:

- A *full authorization reversal* is a service that you can request.

If you do not capture a partial authorization and if full authorization reversals are supported for your processor and card type, you must request a full authorization reversal to release the hold that the authorization placed on the customer's funds. The amount of the reversal must be the amount that was authorized, not the amount that was requested. For details about this service and to see the processors and card types for which this service is supported, see ["Reversing an Authorization," page 25](#).

- An *automatic partial authorization reversal* is performed automatically by CyberSource or your processor under certain conditions.

If you capture a partial authorization for an amount that is less than the approved amount, CyberSource automatically performs a partial authorization reversal if it is supported for your processor and card type. CyberSource performs the automatic partial authorization reversal before sending the capture request to the processor.



Some processors perform an automatic partial authorization reversal when there is an interchange benefit. These processors do not allow CyberSource to perform this functionality.

For details about automatic partial authorization reversals and for a list of the processors and card types for which it is supported, see ["Automatic Partial Authorization Reversals," page 33](#).

Balance Responses



Note

Normally, balance responses are not returned for debit cards.

When there is a balance remaining on a prepaid card after an authorization, the authorization reply can include the balance amount. Depending on what data your processor sends to CyberSource, the following fields might be included in the reply:

- `ccAuthReply_accountBalance`: balance amount remaining on the prepaid card after the authorization



Note

For Discover, some processors return the balance in the `ccAuthReply_authorizationCode` field.

- `ccAuthReply_accountBalanceCurrency`: currency of the balance amount
- `ccAuthReply_accountBalanceSign`: sign for the balance amount

For descriptions of these fields, see [Appendix A, "API Fields," on page 117](#).

The following table lists the processors and card types for which balance responses are supported. Depending on what data your processor sends to CyberSource, the following fields might be included in the reply.

Table 25 Processors Supported for Balance Responses

Processor	Card Type	Balance Field ¹	Currency Field	Sign Field
Chase Paymentech Solutions	Visa	Yes	Yes	no
	Mastercard	Yes	Yes	no
	American Express	Yes	Yes	no
	Discover	Yes	Yes	no
	Diners Club	Yes	Yes	no
	Maestro (International)	Yes	Yes	no
FDC Compass	Visa	Yes	Yes	no
	Mastercard	Yes	Yes	no
	American Express	Yes	Yes	no
	Discover	Yes	Yes	no

¹ For Discover, some processors return the balance in the `ccAuthReply_authorizationCode` field.

Table 25 Processors Supported for Balance Responses (Continued)

Processor	Card Type	Balance Field ¹	Currency Field	Sign Field
FDC Nashville Global	Visa	Yes	Yes	Yes
	Mastercard	Yes	Yes	Yes
	American Express	Yes	Yes	Yes
	Discover	Yes	Yes	Yes
	Diners Club	Yes	Yes	Yes
	JCB	Yes	Yes	Yes
FDMS Nashville	Visa	Yes	Yes	Yes
	Mastercard	no	no	no
	American Express	Yes	Yes	Yes
	Discover	no	no	no
	Diners Club	no	no	no
	JCB	no	no	no
FDMS South	Visa	Yes	Yes	Yes
	Mastercard	no	no	no
	American Express	Yes	Yes	Yes
	Discover	no	no	no
	Diners Club	no	no	no
	JCB	no	no	no
GPN	Visa	Yes	Yes	Yes
	Mastercard	Yes	Yes	Yes
	American Express	Yes	Yes	Yes
	Discover	Yes	Yes	Yes
	Diners Club	Yes	Yes	Yes
	JCB	Yes	Yes	Yes
TSYS Acquiring Solutions	Visa	Yes	Yes	Yes
	Mastercard	Yes	Yes	Yes
	American Express	Yes	Yes	Yes
	Discover	Yes	Yes	Yes
	Diners Club	Yes	Yes	Yes
	JCB	Yes	Yes	Yes

¹ For Discover, some processors return the balance in the **ccAuthReply_authorizationCode** field.

Unsupported Processors and Card Types

Prepaid cards and debit cards that do not appear in [Table 24, "Processors Supported for Partial Authorizations,"](#) on page 55 are processed as follows:

- When the card balance is sufficient for the requested transaction, the transaction is successful.
- When the card balance is not sufficient for the requested transaction, the request is declined.

Optional Features

\$0 Authorizations

See "Zero Amount Authorizations," page 112.

Aggregator Support

This feature enables a third-party agent to act as a payment aggregator and process credit card transactions for sub-merchants. Independent sales organizations (ISOs) and member service providers (MSPs) are agents that can also leverage these aggregator features.

Contact CyberSource Customer Support to have your account configured for this feature.

Terminology

Table 26 Aggregator Terminology

Term	Definition
aggregator	Also known as <i>payment aggregator</i> . Organization that aggregates sub-merchants under a single account and settles funds directly to the sub-merchants. An aggregator is usually an ISO or MSP.
independent sales organization (ISO)	Organization that does one or more of the following: <ul style="list-style-type: none"> ■ Works with acquirers to sponsor merchant accounts and usually assumes the risks associated with the merchants' processing. ■ Procures new merchant relationships based on contracts with acquirers. ■ Connects with a gateway to process online credit card transactions for small businesses, usually in exchange for a fee or percentage of sales.
member service provider (MSP)	Same as an ISO although an MSP has no financial responsibility to the merchant.
payment facilitator	Payment aggregator.
service provider	Third-party or outsource provider of payment processing services. A service provider typically provides a single service with no role in settling funds to a merchant.
sub-merchant	Merchant whose transactions are submitted to CyberSource by a payment aggregator.
third-party agent	Umbrella term for independent sales organizations, member service providers, payment aggregators, and payment facilitators.

FDC Compass Aggregators

Services:

- Authorization
- Capture
- Credit

Card types:

- American Express
- Mastercard

The following fields are required for aggregator transactions with American Express or Mastercard when requesting an authorization, capture, or credit:

- `ccAuthService_aggregatorID`—required only for the authorization service
- `ccAuthService_aggregatorName`—required only for the authorization service with Mastercard
- `ccCaptureService_aggregatorID`—required only for the capture service
- `ccCaptureService_aggregatorName`—required only for the capture service with Mastercard
- `ccCreditService_aggregatorID`—required only for the credit service
- `ccCreditService_aggregatorName`—required only for the credit service with Mastercard
- `invoiceHeader_submerchantCity`
- `invoiceHeader_submerchantID`
- `invoiceHeader_submerchantName`
- `invoiceHeader_submerchantTelephoneNumber`

The following fields are optional for aggregator transactions:

- `invoiceHeader_submerchantCountry`
- `invoiceHeader_submerchantEmail`
- `invoiceHeader_submerchantPostalCode`
- `invoiceHeader_submerchantState`
- `invoiceHeader_submerchantStreet`
- `merchantCategoryCode`—supported only for the authorization service

All fields are described in [Appendix A, "API Fields," on page 117](#).

For Mastercard aggregator captures and credits, CyberSource combines the following two values to provide the business name information for the cardholder's statement:

- Aggregator name in the `ccCaptureService_aggregatorName` or `ccCreditService_aggregatorName` field.
- Sub-merchant name in the `invoiceHeader_submerchantName` field.

The total length of the value that CyberSource sends to the processor is 36 characters. It is formatted with an asterisk (*) between the aggregator name and the sub-merchant name:

```
aggregator name*sub-merchant name
```

Because the asterisk uses one character, 37 characters remain for the combined length of the aggregator name and sub-merchant name.



If the combined length of the aggregator name and sub-merchant name exceeds 37 characters, CyberSource declines the transaction.

FDC Nashville Global Aggregators

Services:

- Authorization
- Capture
- Credit

Card types:

- American Express
- Mastercard

The following fields are required for aggregator transactions with American Express or Mastercard when requesting an authorization, capture, or credit:

- ccAuthService_aggregatorID—required only for the authorization service
- ccAuthService_aggregatorName—required only for the authorization service
- ccCaptureService_aggregatorID—required only for the capture service
- ccCaptureService_aggregatorName—required only for the capture service
- ccCreditService_aggregatorID—required only for the credit service
- ccCreditService_aggregatorName—required only for the credit service
- invoiceHeader_submerchantCity
- invoiceHeader_submerchantCountry
- invoiceHeader_submerchantEmail
- invoiceHeader_submerchantID
- invoiceHeader_submerchantName
- invoiceHeader_submerchantPostalCode
- invoiceHeader_submerchantState
- invoiceHeader_submerchantStreet
- invoiceHeader_submerchantTelephoneNumber
- merchantCategoryCode

The following fields are optional for aggregator transactions:

- invoiceHeader_submerchantMerchantID—supported only for American Express
- invoiceHeader_submerchantRegion

All fields are described in [Appendix A, "API Fields," on page 117](#).

AVS Only

See ["Zero Amount Authorizations," page 112](#).

Bill Payments with Visa

See "Visa Bill Payments," page 110.

Card-Present Data

See the *Card-Present Transactions Supplement*.

Card Type Indicators (CTIs)

Service:

- Authorization

Processor:

- Chase Paymentech Solutions



Note

Contact CyberSource Customer Support to have your account configured for this feature.

This feature enables you to receive CTI information in your authorization reply messages. The processor can provide CTI information for approved or declined transactions, not for rejected transactions.

To receive CTI information:

Your authorization request message must comply with the CTI acceptance criteria as described in the following table.

Table 27 CTI Acceptance Criteria

Card Type	Acceptance Criteria
American Express	CTI is not supported.
Carte Blanche	CTI is not supported.
Diners Club	Currency is USD or CAD.
Discover	Currency is USD or CAD.
JCB	Currency is USD.
Mastercard	Any currency.
Visa	Amount is not 0 (zero). Any currency.

The CTI information is returned in the following fields:

- ccAuthReply_affluenceIndicator
- ccAuthReply_cardCommercial
- ccAuthReply_cardHealthcare
- ccAuthReply_cardIssuerCountry
- ccAuthReply_cardLevel3Eligible
- ccAuthReply_cardPayroll
- ccAuthReply_cardPINlessDebit
- ccAuthReply_cardPrepaid
- ccAuthReply_cardRegulated
- ccAuthReply_cardSignatureDebit

The CTI fields are described in [Appendix A, "API Fields," on page 117](#).

Customer Profiles

See ["Payment Tokenization," page 102](#).

Final Authorization Indicator

Service:

- Authorization

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- GPN
- TSYS Acquiring Solutions

Card type:

- Mastercard

This feature supports a mandate from Mastercard. The purpose of the mandate is to ensure that a customer's funds are available when there is a risk that the order will not be fulfilled.

For an authorization with an amount greater than zero, Mastercard recommends that you indicate whether the authorization is a final authorization, a preauthorization, or an undefined authorization.

Final Authorizations

For a final authorization:

- Authorization amount is greater than zero.
- Authorization amount is the final amount that the customer agrees to pay.
- Authorization should not be cancelled after it is approved except when a system failure occurs.
- Authorization must be submitted for capture within seven calendar days of its request.
- Capture amount and currency must be the same as the authorization amount and currency.
- Chargeback protection is in effect for seven days following the authorization.

Preauthorizations

For a preauthorization:

- Authorization amount is greater than zero.
- Authorization amount can be an estimate when the final amount is unknown, which is typical for hotel, auto rental, e-commerce, and restaurant transactions.
- Authorization must be submitted for capture within 30 calendar days of its request.
- If you do not capture the authorization, you must reverse it.



Note

Mastercard charges an additional fee for a preauthorization that is not captured and not reversed.

- Chargeback protection is in effect for 30 days following the authorization.

Undefined Authorizations



Note

Undefined authorizations are not supported on the following processors:

- Chase Paymentech Solutions
 - FDC Compass
 - FDC Nashville Global
 - FDMS Nashville
-

For an undefined authorization:

- Authorization amount is greater than zero.
- Authorization amount can be different from the final transaction amount.
- Authorization should not be cancelled after it is approved except when a system failure occurs.
- Authorization must be submitted for capture within seven calendar days of its request.
- If you do not capture the authorization, you must reverse it; otherwise, Mastercard charges an additional fee for the transaction.
- Chargeback protection is in effect for seven days following the authorization.



Note

An authorization is undefined when you set the default authorization type in your CyberSource account to `undefined` and do not include the **authIndicator** field in the authorization request. To set the default authorization type in your CyberSource account, contact CyberSource Customer Support.

Unmarked Authorizations



Note

Unmarked authorizations are supported only on the following processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville

For an unmarked authorization:

- CyberSource does not set a mark or indicator for the type of authorization in the request that is sent to the processor.
- Authorization amount is greater than zero.
- Authorization amount can be different from the final transaction amount.
- Your acquirer processes an unmarked authorization as a final authorization, a preauthorization, or an undefined authorization. Contact your acquirer to find out how they process unmarked authorizations.



Note

An authorization is unmarked when the default authorization type is not set in your CyberSource account and you do not include the **authIndicator** field in the authorization request. To set the default authorization type in your CyberSource account, contact CyberSource Customer Support.

To indicate whether an authorization is a final authorization or a preauthorization:

Include the **authIndicator** field in your authorization request. See "[Request Fields](#)," [page 119](#), for the field description.

The **authIndicator** field is included in the reply message for the following processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville

Forced Captures

Service:

- Authorization

Processors:

- Chase Paymentech Solutions
- FDC Nashville Global
- FDMS Nashville
- FDMS South
- GPN
- TSYS Acquiring Solutions

A forced capture occurs when you process an authorization outside the CyberSource system but then capture the order through CyberSource.

To perform a forced capture:

After you process the authorization outside the CyberSource system, request the CyberSource authorization and capture services at the same time as described in ["Creating an Authorization Request," page 23](#), and ["Creating a Capture Request," page 31](#):

- Include the request fields that are required for the authorization.
- Include these fields in the request:
 - `ccAuthService_authType=VERBAL`
 - `ccAuthService_verbalAuthCode=` the authorization code you received in the response for the authorization that was processed outside the CyberSource system
- No additional fields are required for the capture.

For the American Express card type on FDMS South, you must include the **ccCaptureService_posData** and **ccCaptureService_transactionID** fields in the capture request to support the CAPN requirements. Obtain the values for these fields from the response for the authorization that was processed outside the CyberSource system.

Installment Payments

Services:

- Authorization
- Capture—only on FDC Nashville Global

Processors and card types:

- See the following table.

Table 28 Processors That Support Installment Payments

Processors	Credit Card Types
Chase Paymentech Solutions	Visa See "Installment Payments on Chase Paymentech Solutions and FDC Compass," page 74.
FDC Compass	Visa See "Installment Payments on Chase Paymentech Solutions and FDC Compass," page 74.
FDC Nashville Global	Visa, Discover, Diners Club, JCB (US Domestic) For JCB cards, "US Domestic" means that the currency is USD and your location is the U.S., Puerto Rico, Guam, U.S. Virgin Islands, or Northern Mariana Islands. "Installment Payments on FDC Nashville Global," page 74.
FDMS Nashville	Visa See "Installment Payments on Other Processors," page 75.
FDMS South	Visa See "Installment Payments on Other Processors," page 75.
TSYS Acquiring Solutions	Visa See "Installment Payments on Other Processors," page 75.

Installment Payments on Chase Paymentech Solutions and FDC Compass

The customer pays for goods or services using an installment plan agreed upon by the customer and you.

To indicate that a transaction on Chase Paymentech Solutions or FDC Compass is an installment payment:

Step 1 Set `ccAuthService_commerceIndicator` to `install`.

Step 2 Include the following required fields in your authorization request:

- `invoiceHeader_merchantDescriptor`
- `invoiceHeader_merchantDescriptorContact`

For information about these fields, see "[Chase Paymentech Solutions Merchant Descriptors](#)," page 76, and "[FDC Compass Merchant Descriptors](#)," page 81.

Step 3 You can include the following optional fields in your authorization request:

- `installment_sequence`
- `installment_totalCount`

For information about these fields, see [Appendix A, "API Fields,"](#) on page 117.

Installment Payments on FDC Nashville Global

The customer pays for goods or services using an installment plan agreed upon by the customer and you.

To indicate that a transaction on FDC Nashville Global is an installment payment:

Step 1 When you request the authorization service, set `ccAuthService_commerceIndicator` to `install`.

Step 2 When you request the capture service, include the following required fields in the request:

- `installment_sequence`
- `installment_totalCount`

For information about these fields, see [Appendix A, "API Fields,"](#) on page 117.

Installment Payments on Other Processors

The customer pays for goods or services using an installment plan agreed upon by the customer and you.

To indicate that a transaction on any other supported processor is an installment payment:

Step 1 Set `ccAuthService_commerceIndicator` to `install`.

Step 2 Include the following required fields in your authorization request:

- `installment_sequence`
- `installment_totalCount`

For information about these fields, see [Appendix A, "API Fields,"](#) on page 117.

JCB J/Secure

See "Payer Authentication," page 95.

Level II Data

See the *Level II and Level III Transactions Supplement*.

Level III Data

See the *Level II and Level III Transactions Supplement*.

Mastercard SecureCode

See "Payer Authentication," page 95.

Merchant Descriptors

Processors:

- "Chase Paymentech Solutions Merchant Descriptors," page 76
- "FDC Compass Merchant Descriptors," page 81
- "FDC Nashville Global Merchant Descriptors," page 84
- "FDMS South Merchant Descriptors," page 89
- "GPN Merchant Descriptors," page 90
- "TSYS Acquiring Solutions Merchant Descriptors," page 92

Chase Paymentech Solutions Merchant Descriptors

Services:

- Authorization
- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.



Note

Chase Paymentech Solutions restricts the number of merchant descriptors you can use.

Before including merchant descriptors in your requests:

- Prepare a list of the merchant descriptors you plan to use.
- Contact Chase Paymentech Solutions for information about working with merchant descriptors.
- Contact CyberSource Customer Support to have your account enabled for this feature.

Chase Paymentech Solutions supports the merchant descriptors described in "[API Fields](#)," page 78. The information in that section supersedes the information in [Appendix A, "API Fields,"](#) on page 117.

Merchant Descriptor Logic

**Important**

Some of the logic described in this section might not apply to your implementation depending on which parts of the merchant descriptor functionality are enabled in your CyberSource account.

The logic described in this section applies to the **invoiceHeader_merchantDescriptor** and **invoiceHeader_merchantDescriptorContact** fields. It does not apply to the Transaction Advice Addendum (TAA) fields.

For authorizations, CyberSource provides merchant descriptor information to Chase Paymentech Solutions only if you include merchant descriptor information in the authorization request.

For captures, CyberSource provides merchant descriptor information to Chase Paymentech Solutions if you provide merchant descriptor information in the capture request, authorization request, or your CyberSource account. When you do not include the merchant descriptor values in a capture request, CyberSource uses the values from the authorization request. If you did not include the merchant descriptor values in the authorization request, CyberSource uses the corresponding values from your CyberSource account.

For follow-on credits, CyberSource provides merchant descriptor information to Chase Paymentech Solutions if you provide merchant descriptor information in the credit request, capture request, authorization request, or your CyberSource account. When you do not include the merchant descriptor values in a follow-on credit request, CyberSource uses the values from the capture request. If you did not include the merchant descriptor values in the capture request, CyberSource uses the values from the authorization request. If you did not include the merchant descriptor values in the authorization request, CyberSource uses the corresponding values from your CyberSource account.

For stand-alone credits, CyberSource provides merchant descriptor information to Chase Paymentech Solutions if you provide merchant descriptor information in the credit request or your CyberSource account. When you do not include the merchant descriptor values in a stand-alone credit request, CyberSource uses the corresponding values from your CyberSource account.

To add a merchant descriptor value to your CyberSource account, contact CyberSource Customer Support.

Characters

In the merchant descriptor fields, question marks are replaced with spaces.

Do not use the following punctuation characters in the merchant descriptor fields because they will cause the transaction to be rejected with reason code 233:

- caret (^)
- backslash (\)
- open bracket ([)
- close bracket (])
- tilde (~)
- accent (`)

API Fields

Table 29 Merchant Descriptor Fields for Chase Paymentech Solutions

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ amexDataTAA1	Four Transaction Advice Addendum (TAA) fields. These fields are used to display descriptive information about a transaction on the customer's American Express card statement. When you send TAA fields, start with invoiceHeader_amexDataTAA1 , then ...TAA2 , and so on. Skipping a TAA field causes subsequent TAA fields to be ignored.	ccCaptureService (O)	String (40)
invoiceHeader_ amexDataTAA2		ccCreditService (O)	
invoiceHeader_ amexDataTAA3			
invoiceHeader_ amexDataTAA4			
	These fields are frequently used for Level II transactions. See Level II and Level III Processing Using the Simple Order API .		

Table 29 Merchant Descriptor Fields for Chase Paymentech Solutions (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	<p>Merchant description that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.</p> <p>For an installment transaction, you must use one of the following formats:</p> <ul style="list-style-type: none"> ■ <12-character merchant name>*PYMT<N>OF<M> ■ <7-character merchant name>*PYMT<N>OF<M> ■ <3-character merchant name>*PYMT<N>OF<M> <p>where <N> is the payment number and <M> is the total number of payments. For example, for the third installment in a series of seven payments, the PYMT<N>OF<M> portion of the merchant descriptor would be PYMT3OF7.</p> <p>For other types of transactions, you must use one of the following formats:</p> <ul style="list-style-type: none"> ■ <12-character merchant name>*<9-character product description> ■ <7-character merchant name>*<14-character product description> ■ <3-character merchant name>*<18-character product description> <p>This field is supported only for Visa, Mastercard, and Discover.</p>	ccAuthService ccCaptureService ccCreditService Required when invoiceHeader_merchantDescriptorContact is included in the request.	String (22)

Table 29 Merchant Descriptor Fields for Chase Paymentech Solutions (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor Contact	<p>Merchant contact information, such as a phone number, that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.</p> <p>You must use one of the following formats:</p> <ul style="list-style-type: none"> ■ PCCCCCCCCCCCC ■ NNN-NNN-NNNN ■ NNN-NNN-NAAA ■ NNN-NNN-AAAA ■ NNN-AAAAAAA <p>where:</p> <ul style="list-style-type: none"> ■ A: Alphanumeric (alpha or numeric) ■ C: Character (alpha or blank) ■ N: Numeric ■ P: Alpha <p>This field is supported only for Visa, Mastercard, and Discover.</p>	<p>ccAuthService ccCaptureService ccCreditService</p> <p>Required when invoiceHeader_merchantDescriptor is included in the request.</p>	String (13)

FDC Compass Merchant Descriptors

Services:

- Authorization
- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.



Note

FDC Compass restricts the number of merchant descriptors you can use.

Before including merchant descriptors in your requests:

- Prepare a list of the merchant descriptors you plan to use.
- Contact FDC Compass for information about working with merchant descriptors.
- Contact CyberSource Customer Support to have your account enabled for this feature.

FDC Compass supports the merchant descriptors described in ["API Fields," page 82](#). The information in that section supersedes the information in [Appendix A, "API Fields," on page 117](#).

Characters

In the merchant descriptor fields, question marks are replaced with spaces.

Do not use the following punctuation characters in the merchant descriptor fields because they will cause the transaction to be rejected with reason code 233:

- caret (^)
- backslash (\)
- open bracket ([)
- close bracket (])
- tilde (~)
- accent (`)

API Fields

Table 30 Merchant Descriptor Fields for FDC Compass

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ amexDataTAA1 invoiceHeader_ amexDataTAA2 invoiceHeader_ amexDataTAA3 invoiceHeader_ amexDataTAA4	<p>Four Transaction Advice Addendum (TAA) fields. These fields are used to display descriptive information about a transaction on the customer's American Express card statement. When you send TAA fields, start with invoiceHeader_amexDataTAA1, then ...TAA2, and so on. Skipping a TAA field causes subsequent TAA fields to be ignored.</p> <p>These fields are frequently used for Level II transactions. See Level II and Level III Processing Using the Simple Order API.</p>	<p>ccCaptureService (O) ccCreditService (O)</p>	String (40)
invoiceHeader_ merchantDescriptor	<p>Merchant description that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.</p> <p>For an installment transaction, you must use one of the following formats:</p> <ul style="list-style-type: none"> ■ <12-character merchant name>*PYMT<N>OF<M> ■ <7-character merchant name>*PYMT<N>OF<M> ■ <3-character merchant name>*PYMT<N>OF<M> <p>where <N> is the payment number and <M> is the total number of payments. For example, for the third installment in a series of seven payments, the PYMT<N>OF<M> portion of the merchant descriptor would be PYMT3OF7.</p> <p>For other types of transactions, you must use one of the following formats:</p> <ul style="list-style-type: none"> ■ <12-character merchant name>*<9-character product description> ■ <7-character merchant name>*<14-character product description> ■ <3-character merchant name>*<18-character product description> 	<p>ccAuthService ccCaptureService ccCreditService</p> <p>Required when invoiceHeader_merchantDescriptorContact is included in the request.</p>	String (22)

Table 30 Merchant Descriptor Fields for FDC Compass (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor Contact	<p>Merchant contact information, such as a phone number, that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.</p> <p>You must use one of the following formats:</p> <ul style="list-style-type: none"> ■ PCCCCCCCCCCCC ■ NNN-NNN-NNNN ■ NNN-NNN-NAAA ■ NNN-NNN-AAAA ■ NNN-AAAAAAA <p>where:</p> <ul style="list-style-type: none"> ■ A: Alphanumeric (alpha or numeric) ■ C: Character (alpha or blank) ■ N: Numeric ■ P: Alpha 	<p>ccAuthService ccCaptureService ccCreditService</p> <p>Required when invoiceHeader_merchantDescriptor is included in the request.</p>	String (13)

FDC Nashville Global Merchant Descriptors

Services:

- Authorization
- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.

Before including merchant descriptors in your requests:

- Contact FDC Nashville Global to register to use merchant descriptors.
- Contact CyberSource Customer Support to have your account enabled for this feature.

FDC Nashville Global supports the merchant descriptors described in ["API Fields," page 86](#). The information in that section supersedes the information in [Appendix A, "API Fields," on page 117](#).

Merchant Descriptor Logic



Some of the logic described in this section might not apply to your implementation depending on which parts of the merchant descriptor functionality are enabled in your CyberSource account.



You are responsible for ensuring that all the merchant descriptor location information that CyberSource sends to the processor is compatible.

For example, if a request message includes one merchant descriptor location field, CyberSource might use the information in your CyberSource account to populate the remaining merchant descriptor location values that it sends to the processor. CyberSource does not check the merchant descriptor values to ensure that the combination of values from the request message and from your CyberSource account are compatible.

To avoid a mismatch of merchant descriptor location values, CyberSource recommends that you include all the merchant descriptor location fields in a request or do not include any merchant descriptor location fields in a request.

For authorizations, CyberSource provides merchant descriptor information to FDC Nashville Global only if you include merchant descriptor information in the authorization request. For each merchant descriptor, when you do not include the merchant descriptor value in an authorization request, CyberSource does not send a merchant descriptor value to FDC Nashville Global.

For captures, CyberSource provides merchant descriptor information to FDC Nashville Global if you provide merchant descriptor information in the capture request, authorization request, or your CyberSource account. For each merchant descriptor, when you do not include the merchant descriptor value in a capture request, CyberSource uses the value from the authorization request. If you did not include the merchant descriptor value in the authorization request, CyberSource uses the corresponding value from your CyberSource account. If the value is not included in your CyberSource account, FDC Nashville Global uses the value from your First Data merchant master file.

For follow-on credits, CyberSource provides merchant descriptor information to FDC Nashville Global if you provide merchant descriptor information in the credit request, capture request, authorization request, or your CyberSource account. For each merchant descriptor, when you do not include the merchant descriptor value in a follow-on credit request, CyberSource uses the value from the capture request. If you did not include the merchant descriptor value in the capture request, CyberSource uses the value from the authorization request. If you did not include the merchant descriptor value in the authorization request, CyberSource uses the corresponding value from your CyberSource account. If the value is not included in your CyberSource account, FDC Nashville Global uses the value from your First Data merchant master file.

For stand-alone credits, CyberSource provides merchant descriptor information to FDC Nashville Global if you provide merchant descriptor information in the credit request or your CyberSource account. For each merchant descriptor, when you do not include the merchant descriptor value in a stand-alone credit request, CyberSource uses the corresponding value from your CyberSource account. If the value is not included in your CyberSource account, FDC Nashville Global uses the value from your First Data merchant master file.

To add a merchant descriptor value to your CyberSource account, contact CyberSource Customer Support.

API Fields

Table 31 Merchant Descriptor Fields for FDC Nashville Global

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	<p>Business description. This value must consist of your business name. When payments are made in installments, this value must also include installment information such as "1 of 5" or "3 of 7."</p> <p>This value is displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p> <p>If you include this field in a request, you must also include invoiceHeader_merchantDescriptorContact and invoiceHeader_merchantDescriptorState.</p>	String (22)
invoiceHeader_ merchantDescriptor Alternate	<p>Alternate contact information for your business, such as an email address or URL.</p> <p>This value might be displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84. For authorizations, CyberSource does not provide this value to the processor. Instead, CyberSource stores this value and sends it to the processor for captures and follow-on credits.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p>	String (13)
invoiceHeader_ merchantDescriptor Contact	<p>Contact information for your business. For a card-present request, this value must be the city in which your store or outlet is located. For a card-not-present request, this value must be your customer service telephone number. When you include more than one consecutive space, extra spaces are removed.</p> <p>This value might be displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p> <p>If you include this field in a request, you must also include invoiceHeader_merchantDescriptor and invoiceHeader_merchantDescriptorState.</p>	String (11)

Table 31 Merchant Descriptor Fields for FDC Nashville Global (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor Country	<p>Country in which your business is located. Use the two-character <i>ISO Standard Country Codes</i>.</p> <p>This value might be displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (2)
invoiceHeader_ merchantDescriptor PostalCode	<p>Postal code for your business location.</p> <p>This value might be displayed on the cardholder's statement.</p> <p>When the merchant descriptor country is the U.S., the postal code must consist of five digits or nine digits. A 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the merchant descriptor country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</p> <p>Example A1B 2C3</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (10)

Table 31 Merchant Descriptor Fields for FDC Nashville Global (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor State	<p>State or territory in which your business is located. cardholder's statement.</p> <p>When the merchant descriptor country is the U.S. or Canada, use the <i>State, Province, and Territory Codes for the United States and Canada</i>.</p> <p>This value might be displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p> <p>If you include this field in a request, you must also include invoiceHeader_merchantDescriptor and invoiceHeader_merchantDescriptorContact.</p>	String (20)
invoiceHeader_ merchantDescriptor Street	<p>Street address for your business location.</p> <p>When you include this value in your request, CyberSource recommends the following:</p> <ul style="list-style-type: none"> ■ If you are located in the United States or Canada, also include the merchant descriptor country, merchant descriptor state, and merchant descriptor postal code in your request. ■ If you are not located in the United States or Canada, also include the merchant descriptor country and merchant descriptor postal code in your request. <p>This value might be displayed on the cardholder's statement.</p> <p>For information about what happens when you do not include this value in your request, see "Merchant Descriptor Logic," page 84.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p> <p>FDC Nashville Global recommends that you include this value for debit card requests and for American Express credit card requests.</p>	String (60)

FDMS South Merchant Descriptors

Services:

- Authorization
- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.

Before including merchant descriptors in your requests:

- Contact FDMS South to register to use merchant descriptors.
- Contact CyberSource Customer Support to have your account configured for this feature.

FDMS South permits you to send a unique merchant descriptor with every transaction. This is useful if you want to include the order number as part of the merchant descriptor.

FDMS South supports the merchant descriptor described in the following table.

Table 32 Merchant Descriptor Field for FDMS South

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	Merchant description that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.	ccAuthService ccCaptureService ccCreditService Required when invoiceHeader_ merchantDescriptor Contact is included in the request.	String (22)

GPN Merchant Descriptors

Services:

- Authorization
- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.

Before including merchant descriptors in your requests, contact your merchant account provider to register to use merchant descriptors.

GPN supports the merchant descriptors listed in the following table.

Table 33 Merchant Descriptor Fields for GPN

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	Merchant description that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.	ccAuthService ccCaptureService ccCreditService Required when invoiceHeader_ merchantDescriptor Contact is included in the request.	String (22)
invoiceHeader_ merchantDescriptor Contact	Merchant contact information, such as a phone number, that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (13)

Table 34 Merchant Descriptor Fields for OmniPay-Ireland

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	<p>Merchant description that is displayed on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed.</p> <p>You must use one of the following formats:</p> <ul style="list-style-type: none"> ■ <12-character merchant name>* <10-character product description> ■ <7-character merchant name>* <15-character product description> ■ <3-character merchant name>* <19-character product description> <p>This field is supported only for Visa, Mastercard, and Discover.</p>	ccAuthService ccCaptureService ccCreditService	String (23)

TSYS Acquiring Solutions Merchant Descriptors

Services:

- Capture
- Credit

This feature enables you to submit merchant descriptor values that are displayed on a cardholder's statement.

Before including merchant descriptors in your requests, contact CyberSource Customer Support to have your account configured for this feature.

TSYS Acquiring Solutions supports the merchant descriptor fields listed in the following table.

Table 35 Merchant Descriptor Fields for TSYS Acquiring Solutions

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ merchantDescriptor	Your business name. When you include more than one consecutive space, extra spaces are removed. When you do not include this value in your capture or credit request, CyberSource uses the business name from your CyberSource account. ¹	ccCaptureService ccCreditService Required when the merchant descriptor contact field is included in the request; otherwise, optional.	American Express card type: String (38) All other card types: String (23)
invoiceHeader_ merchantDescriptorCity	City for your business location. When you do not include this value in your request, CyberSource uses the value that is in your CyberSource account. ¹	ccCaptureService (O) ccCreditService (O)	American Express card type: String (21) All other card types: String (13)
invoiceHeader_ merchantDescriptor Contact	For card-present transactions, TSYS Acquiring Solutions recommends that this field contain the street address for your business location. For card-not-present transactions, TSYS Acquiring Solutions recommends that this field contain the phone number for your business or the URL for your web site. When you do not include this value in your request, CyberSource uses the value that is in your CyberSource account. ¹	ccCaptureService (O) ccCreditService (O)	String (13)

¹ To add this value to your CyberSource account, contact CyberSource Customer Support.

Merchant-Initiated Reversals and Voids

Services:

- Authorization
- Capture
- Credit

Processors:

- Chase Paymentech Solutions
- FDC Nashville Global

When you do not receive a reply message after sending a request to CyberSource, this feature enables you to reverse or void the transaction that you requested.

To use merchant-initiated reversals and voids:

- Step 1** Include the **merchantTransactionIdentifier** field in your original request for an authorization, capture, sale, follow-on credit, or stand-alone credit.



Note

The value of the merchant transaction ID must be unique for 60 days.

Step 2 When you do not receive a reply message for your original transaction request, reverse or void the original transaction as described in the following table.

Transaction to Reverse or Void	Procedure
Authorization	Request the full authorization reversal service as described in "Creating a Full Authorization Reversal Request," page 27 . Instead of including the request ID in your request message, include the merchantTransactionIdentifier field. The merchant transaction ID links your reversal request to your original request.
Capture or sale	<ol style="list-style-type: none"> 1 Request the void service as described in "Creating a Void Request," page 42. Instead of including the request ID in your request message, include the merchantTransactionIdentifier field. The merchant transaction ID links your void request to your original request. 2 Request the authorization reversal service as described in "Creating a Full Authorization Reversal Request," page 27. Instead of including the request ID in your request message, include the merchantTransactionIdentifier field. The merchant transaction ID links your reversal request to your original request.
Credit	Request the void service as described in "Creating a Void Request," page 42 . Instead of including the request ID in your request message, include the merchantTransactionIdentifier field. The merchant transaction ID links your void request to your original request.

Step 3 If the original transaction failed, the reply message for the reversal or void request includes the following fields:

- originalTransaction_amount
- originalTransaction_reasonCode

Micropayments

Services:

- Authorization
- Capture
- Credit

Processors:

- Most of the card types and processors that are supported by CyberSource

Micropayments are payments for less than one unit in the transaction's currency.

Payer Authentication

**Important**

Before you implement payer authentication, you must contact CyberSource Customer Support to have your account configured for this feature.

When you request an authorization using a supported card type and a supported processor, you can include payer authentication data in the request. You can use the CyberSource payer authentication services to add Verified by Visa, JCB J/Secure™, or Mastercard® SecureCode™ support to your web site without running additional software on your own server. For a description of the CyberSource payer authentication services, see the [Payer Authentication Using the Simple Order API](#).

Verified by Visa

Service:

- Authorization

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- FDMS South
- GPN
- RBS WorldPay Atlanta
- TSYS Acquiring Solutions

Verified by Visa reduces the risk of unauthorized use of a cardholder account. Verified by Visa enables you to verify a customer's identity through the use of a password, and provides results to you in real time during the checkout process. For details about signing up for and using Verified by Visa, contact your acquiring bank or go to the Visa web site:

<http://visa.com/>

To request the authorization of a Verified by Visa transaction:

- Step 1** Add the fields listed in the following table to your **ccAuthService** request. The values for these fields are in the reply from the validate authentication service **payerAuthValidateService**. When you request **payerAuthValidateService** and **ccAuthService** together, the data is automatically passed from one service to the other.

Table 36 Request Fields for Verified by Visa and JCB J/Secure

Value and Requirements	Request Field for the Authorization Service	Get the Value from this Payer Authentication Reply Field
<p>CAVV—cardholder authentication verification value. This value is a transaction identifier generated by the issuing bank during Verified by Visa or JCB J/Secure payer authentication. Must be 28-character base64 or 40-character hex binary.</p> <ul style="list-style-type: none"> ■ Used for all processors that support Verified by Visa and/or JCB J/Secure. ■ Required when the commerce indicator is <code>js</code>, <code>vbv</code>, or <code>vbv_attempted</code>. ■ Optional when the commerce indicator is <code>js_attempted</code>. ■ For Verified by Visa on FDC Nashville Global, CyberSource sets this field to the value for the transaction identifier (XID) if the XID is present in the authorization request and the CAVV is not present. 	<code>ccAuthService_cavv</code>	<code>payerAuthValidateReply_cavv</code>
<p>ECI—electronic commerce indicator.</p> <ul style="list-style-type: none"> ■ Used for all processors that support Verified by Visa and/or JCB J/Secure. ■ Always required. ■ Possible values for a Verified by Visa or JCB J/Secure transaction: <ul style="list-style-type: none"> • <code>js</code>: Successful JCB J/Secure transaction. • <code>js_attempted</code>: JCB J/Secure transaction was attempted but not authenticated. • <code>vbv</code>: Successful Verified by Visa transaction. • <code>vbv_attempted</code>: Verified by Visa transaction was attempted but not authenticated. 	<code>ccAuthService_commerceIndicator</code>	<code>payerAuthValidateReply_commerceIndicator</code>

Table 36 Request Fields for Verified by Visa and JCB J/Secure (Continued)

Value and Requirements	Request Field for the Authorization Service	Get the Value from this Payer Authentication Reply Field
<p>ECI Raw—raw electronic commerce indicator.</p> <ul style="list-style-type: none"> Used for all processors that support Verified by Visa and/or JCB J/Secure. Required when the payer authentication validation service returns a raw ECI value. Some processors require the raw ECI to guarantee chargeback protection. Contact CyberSource Customer Support for information about your processor's requirements. 	ccAuthService_eciRaw	payerAuthValidateReply_eciRaw
<p>XID—transaction identifier. Must be 28-character base64 or 40-character hex binary.</p> <ul style="list-style-type: none"> Used for all processors that support Verified by Visa and/or JCB J/Secure. Required when the commerce indicator is js or vbv. Optional when the commerce indicator is js_attempted or vbv_attempted. For Verified by Visa on FDC Nashville Global, CyberSource sets the cardholder authentication verification value (CAVV) field to the XID value if the XID is present in the authorization request and the CAVV is not present. 	ccAuthService_xid	payerAuthValidateReply_xid

JCB J/Secure

Service:

- Authorization

Processor:

- TSYS Acquiring Solutions

JCB J/Secure authenticates the customer by adding a password identification step to the online shopping process. For details about signing up for and using J/Secure, contact your acquiring bank or go to the JCB web site:

<http://www.jcb-global.com/>

To request the authorization of a JCB J/Secure transaction:

- Step 1** Add the fields listed in [Table 36, "Request Fields for Verified by Visa and JCB J/Secure," on page 96](#) to your **ccAuthService** request. The values for these fields are in the reply from the validate authentication service **payerAuthValidateService**. When you request **payerAuthValidateService** and **ccAuthService** together, the data is automatically passed from one service to the other.
-

Mastercard SecureCode

Service:

- Authorization

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- FDMS South
- GPN
- RBS WorldPay Atlanta
- TSYS Acquiring Solutions

Mastercard SecureCode adds security to online transactions by authenticating SecureCode account holders for specific transactions. SecureCode generates a unique, 32-character transaction token, called the account authentication value (AAV), each time a SecureCode-enabled account holder makes an online purchase. The AAV binds the account holder to a specific transaction. SecureCode transactions use the universal cardholder authentication field (UCAF) as a standard to collect and pass AAV data. For details about signing up for and using SecureCode or UCAF, contact your acquiring bank or go to the Mastercard web site:

<http://www.mastercard.com/>

To request the authorization of a Mastercard SecureCode transaction:

- Step 1** Add the fields in [Table 37, "Request Fields for Mastercard SecureCode,"](#) to your **ccAuthService** request. The values for these fields are in the reply from the validate authentication service **payerAuthValidateService**. When you request **payerAuthValidateService** and **ccAuthService** together, the data is automatically passed from one service to the other.
-

Table 37 Request Fields for Mastercard SecureCode

Value and Requirements	Request Field for the Authorization Service	Get the Value from this Payer Authentication Reply Field
<p>ECI—electronic commerce indicator.</p> <ul style="list-style-type: none"> Used for all processors that support Mastercard SecureCode. Always required. Value to use for a Mastercard SecureCode transaction: <code>spa</code>. 	<code>ccAuthService_commerceIndicator</code>	<code>payerAuthValidateReply_commerceIndicator</code>
<p>ECI Raw—raw electronic commerce indicator.</p> <ul style="list-style-type: none"> Used for all processors that support Mastercard SecureCode. Required when the payer authentication validation service returns a raw ECI value. Some processors require the raw ECI to guarantee chargeback protection. Contact CyberSource Customer Support for information about your processor's requirements. 	<code>ccAuthService_eciRaw</code>	<code>payerAuthValidateReply_eciRaw</code>
<p>UCAF Authentication Data—authentication data for the universal cardholder authentication field.</p> <ul style="list-style-type: none"> Used for all processors that support Mastercard SecureCode. Required when the UCAF collection indicator is 2 or 5. Optional when the UCAF collection indicator is 1. Do not include the UCAF authentication data in the authorization request if the UCAF collection indicator is not 1, 2, or 5. <p>Important Mastercard has indicated that an issuing bank can decline an authorization request for a Mastercard SecureCode transaction when the UCAF collection indicator is 1 and the UCAF authentication data is not present.</p>	<code>ucaf_authenticationData</code>	<code>payerAuthValidateReply_ucafAuthenticationData</code>

Table 37 Request Fields for Mastercard SecureCode (Continued)

Value and Requirements	Request Field for the Authorization Service	Get the Value from this Payer Authentication Reply Field
<p>UCAF Collection Indicator—collection indicator for the universal cardholder authentication field.</p> <ul style="list-style-type: none"> ■ Used for all processors that support Mastercard SecureCode. ■ Always required. ■ Possible values: <ul style="list-style-type: none"> ● 0: UCAF collection is not supported at your web site. ● 1: UCAF collection is supported at your web site and the UCAF might have been populated. ● 2: UCAF collection is supported at your web site and the UCAF was populated. This value indicates a successful Mastercard SecureCode transaction. 	ucaf_collectionIndicator	payerAuthValidateReply_ucafCollectionIndicator
<p>XID—transaction identifier. Must be 28-character base64 or 40-character hex binary.</p> <ul style="list-style-type: none"> ■ Used for all processors that support Mastercard SecureCode. ■ Required when the payer authentication validation service returns an XID value. 	ccAuthService_xid	payerAuthValidateReply_xid

American Express SafeKey

Service:

- Authorization

Processor:

- FDC Nashville Global

American Express SafeKey (AESK) authenticates the cardholder during an online purchase and protects payment information as it is transmitted over the Internet.

To request the authorization of an AESK transaction:

- Step 1** Add the fields in the following table to your **ccAuthService** request. The values for these fields are in the reply from the validate authentication service **payerAuthValidateService**. When you request **payerAuthValidateService** and **ccAuthService** together, the data is automatically passed from one service to the other.

The authorization service returns a raw response code and a mapped response code:

- The *raw response code* is the value returned by the processor. CyberSource returns this value in the **ccAuthReply_cavvResponseCodeRaw** field.
- The *mapped response code* is the predefined CyberSource value that corresponds to the raw response code. CyberSource returns this value in the **ccAuthReply_cavvResponseCode** field. [Appendix C, "American Express SafeKey Response Codes," on page 171](#), describes the mapped response codes.

Table 38 Request Fields for American Express SafeKey

Value and Requirements	Request Field for the Authorization Service	Get the Value from this Payer Authentication Reply Field
CAVV —cardholder authentication verification value. This value is a transaction identifier generated by the issuing bank during American Express SafeKey payer authentication. This value is required.	ccAuthService_cavv	payerAuthValidateReply_cavv
ECI —electronic commerce indicator. This value is required. Possible values: <ul style="list-style-type: none"> ■ aesk: Successful AESK transaction. ■ aesk_attempted: AESK transaction was attempted but not authenticated. 	ccAuthService_commerceIndicator	payerAuthValidateReply_commerceIndicator
XID —transaction identifier. This value is optional.	ccAuthService_xid	payerAuthValidateReply_xid

Payment Tokenization

**Note**

Payment network tokenization and *CyberSource payment tokenization* are not the same feature.

- With payment network tokenization, the token is created by a token service provider and can be used throughout the financial network.
- With CyberSource payment tokenization, the token is created by CyberSource and can be used only with CyberSource services.

When you use Payment Tokenization, you can process an authorization, capture, or credit by using information that is stored in a customer profile. CyberSource uses the subscription ID to reference the customer profile information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you only need to provide the following values:

- Merchant ID
- Merchant reference code
- Amount of the payment or credit
- Subscription ID

You can override most of the information stored in the customer profile by including the relevant API fields in the payment or credit request. For example, you could provide a different billing or shipping address in the request. You cannot override the credit card account number.

See [Payment Tokenization Using the Simple Order API for CyberSource Essentials](#).

POS Transactions

See the [Card-Present Transactions Supplement](#).

Quasi-Cash

Services:

- Authorization
- Full authorization reversal
- Capture
- Credit
- Void

Processors:

- GPN
- TSYS Acquiring Solutions

Before processing quasi-cash transactions, contact CyberSource Customer Support to have your account configured for this feature. If you have questions about the supported card types, contact your processor.

A quasi-cash transaction is a cash-like transaction for the sale of items that are directly convertible to cash, such as:

- Casino gaming chips
- Money orders
- Wire transfers

Automatic partial authorization reversals are supported for quasi-cash transactions. See ["Automatic Partial Authorization Reversals," page 33](#).

Recurring Billing

When you use Recurring Billing, you can process an authorization, capture, or credit by using information that is stored in a subscription. CyberSource uses the subscription ID to reference the subscription information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you only need to provide the following values:

- Merchant ID
- Merchant reference code
- Amount of the payment or credit
- Subscription ID

You can override most of the information stored in the subscription by including the relevant API fields in the payment or credit request. For example, you could provide a different billing or shipping address in the request. You cannot override the credit card account number.

See [Recurring Billing Using the Simple Order API for CyberSource Essentials](#).

Recurring Payments

Service:

- Authorization

Processors and card types:

- See the following table.

Table 39 Processors That Support Recurring Payments

Processors	Credit Card Types
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club, JCB
FDC Nashville Global	Visa, Mastercard, American Express, Discover
FDMS South	Visa, Mastercard, Discover On FDMS South, recurring payments are not supported for the CAD currency on the Visa card type.
FDMS Nashville	Visa, Mastercard, American Express, Discover
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB
RBS WorldPay Atlanta	Visa, Mastercard, American Express, Discover, Diners Club, JCB
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover



Note

American Express and Discover have programs that you must register for if you want to process recurring payments. Contact American Express and Discover for details about their programs.

Depending on the types of products and services you sell, you might want to process recurring payments for a customer. For example, you might want to charge a customer 19.95 USD each month to access a service that you offer.



Note

A customer's recurring payment does not have to be the same amount each time.

You must disclose clearly to customers when they make a purchase what the amount will be for the recurring payments. If the amount varies based on usage, make it clear.

To create a recurring payment:

Step 1 For the first payment, the type of request you need to send depends on which processor and card type you are using.

- For Mastercard and American Express transactions on FDC Nashville Global, include the following fields and values in the request for the first payment:

```
ccAuthService_commerceIndicator=recurring
```

```
ccAuthService_firstRecurringPayment=TRUE
```

```
card_cvNumber
```

- For all other processors and card types, request a non-recurring transaction for a credit card authorization.

If the first authorization is successful, you can submit subsequent authorizations for recurring payments using that card. If the first authorization is not successful, do not submit subsequent authorizations using that card.



You must perform Step 1 once per year to verify the account.

Step 2 For each subsequent recurring payment, send an authorization request using the e-commerce indicator to indicate that the payment is a recurring payment:

```
ccAuthService_commerceIndicator=recurring
```

CyberSource also offers services that enable you to create a subscription or customer profile for a customer in the CyberSource system and then use that subscription or customer profile later to manually or automatically bill the customer. The CyberSource system eliminates the need for you to handle or store the customer's sensitive credit card information or create your own system for billing the customer on a regular basis. For more information, see ["Payment Tokenization," page 102](#), and ["Recurring Billing," page 104](#).

AVS and Recurring Payments



Note

FDMS Nashville does not support AVS for recurring payments.

If AVS is supported for your processor and card type, AVS is run for every authorization request that you submit. For recurring payments, check the AVS result for the first payment to ensure that the payment information is accurate and to reduce the risk of fraud.

You must decide what to do with the AVS results for subsequent payments. You might want to ignore the AVS results for these payments because you have already confirmed with the first payment that the credit card number is valid and not fraudulent.

When you need to change the credit card number used for a series of recurring payments, follow [Step 1](#) in creating a recurring payment to verify the new account number. Closely evaluate the AVS results. If the first authorization is successful, you can submit subsequent authorizations for recurring payments using that card. If the first authorization is not successful, do not submit subsequent authorizations using that card. For subsequent payments, follow [Step 2](#) in creating a recurring payment. You can choose to ignore the AVS results.

CVN and Recurring Payments



Note

FDMS Nashville does not support CVN for recurring payments.

Replacement Expiration Dates for Recurring Payments

Service:

- Authorization

Processors and card types:

- See the following table.

Table 40 Processors That Support Replacement Expiration Dates for Recurring Payments

Processors	Credit Card Types
Chase Paymentech Solutions	Visa, Mastercard
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club
FDMS South	Visa, Mastercard

Normally when you request a credit card authorization, you must provide a valid expiration date for the credit card. If you are processing a recurring payment, and the credit card that you have on file for the customer has expired, you might still be able to request the authorization depending on which processor you use. Instead of sending the out-of-date expiration date, you can include a replacement expiration date in your request.



Important

Do not use a replacement expiration date for cards that have not expired. Use a replacement expiration date only for cards that have expired and only for recurring payments.

Using a replacement expiration date for a recurring payment does not guarantee that the authorization will be successful. The issuing bank determines whether a card is authorized; some issuing banks do not accept an expiration date that does not match the expiration date in the bank's database.

The replacement expiration date that CyberSource supports is 12/2099. To use this date, include these fields and values in your authorization request:

```
card_expirationMonth=12
card_expirationYear=2099
```

Recurring Profiles

See "Recurring Billing," page 104.

Retail POS Data

See the *Card-Present Transactions Supplement*.

Secure Data

See "Payment Tokenization," page 102.

Soft Descriptors

See "Merchant Descriptors," page 76.

Split Dial/Route

See "Forced Captures," page 72.

Subscriptions

See "Recurring Billing," page 104.

Type II Cards

See the *Level II and Level III Transactions Supplement*.

Verbal Authorizations

See "Verbal Authorizations," page 52.

Verified by Visa

See "Payer Authentication," page 95.

Visa Bill Payments

Services:

- Authorization
- Credit

Processors:

- Chase Paymentech Solutions
- FDC Compass
- FDC Nashville Global
- FDMS Nashville
- GPN
- TSYS Acquiring Solutions

Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. When you participate in this program, Visa requests that you flag the bill payments and credits so they can be easily identified. To flag these transactions, include the **ccAuthService_billPayment** field in your transaction requests.

Although CyberSource accepts the bill payment indicator no matter which processor you are using, do not use this indicator if you have not signed up with Visa to participate in the program.

Visa Debt Repayments

Services:

- Authorization
- Credit

Processors:

- FDC Nashville Global
- FDMS Nashville
- GPN

Visa provides a Debt Repayment program that enables customers to use their Visa debit cards to make a payment towards an existing contractual loan. The types of loans that can qualify for this program are:

- Consumer auto loans
- Consumer credit cards
- Consumer mortgages
- Student loans

To participate in this program, contact your processor for details and requirements.

When you participate in this program, Visa requests that you flag the debt repayments and credits so they can be easily identified. To flag these transactions, include these fields in your transaction requests:

- ccAuthService_billPayment
- debtIndicator

Zero Amount Authorizations

Service:

- Authorization

Processors and card types:

- See the following table.

Table 41 Processors That Support Zero Amount Authorizations

Processor	AVS	CVN	Card Types and Notes
Chase Paymentech Solutions	Yes	Yes	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ Diners Club
FDC Compass	Yes	Yes	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ American Express ■ Diners Club
FDC Nashville Global	Yes	Yes	<ul style="list-style-type: none"> ■ Visa ■ Mastercard
FDMS Nashville	Yes	Yes	<ul style="list-style-type: none"> ■ Visa
FDMS South	Yes	Yes for Visa. No for all other card types.	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ American Express ■ Diners Club ■ Discover ■ JCB (US Domestic)
GPN	Yes	Yes for all card types except American Express	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ American Express: CVN is not supported for zero amount authorizations with American Express. ■ Discover ■ JCB

Table 41 Processors That Support Zero Amount Authorizations (Continued)

Processor	AVS	CVN	Card Types and Notes
RBS WorldPay Atlanta	Yes	Yes	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ Diners Club
TSYS Acquiring Solutions	Yes	Yes for Visa and Mastercard. No for American Express and Discover.	<ul style="list-style-type: none"> ■ Visa ■ Mastercard ■ American Express: CVN is not supported for zero amount authorizations with American Express. ■ Discover: CVN is not supported for zero amount authorizations with Discover.

Authorizing a payment for a zero amount shows whether a credit card account is valid and whether the card is lost or stolen. You cannot capture a zero amount authorization.

Testing the Credit Card Services

To ensure that your requests are processed correctly, you must test the basic success and error conditions for each CyberSource service you plan to use.

Requirements for Testing

**Important**

Before you can test, you must contact CyberSource Customer Support to activate the credit card services and configure your account for testing. You must also contact your processor to set up your processor account.

- Use your regular CyberSource merchant ID when you test your system.
- Unless otherwise specified, use test credit card numbers, not real ones. See [Table 42, "Test Credit Card Numbers,"](#) on page 115.
- Use a real combination for the city, state, and postal code.
- Use a real combination for the area code and telephone number.
- Use a nonexistent account and domain name for the customer's email address.
- When testing the Simple Order API, use the test URL:

`https://ics2wstesta.ic3.com/commerce/1.x/transactionProcessor`

Testing the Services

Use the credit card numbers in the following table to test the authorization, capture, and credit services. Do not use real credit card numbers. To test card types not listed in the table, use an account number that is within the card's bin range. For best results, try each test with a different CyberSource service request and with different test credit card numbers.

Table 42 Test Credit Card Numbers

Credit Card Type	Test Account Number (Remove spaces when sending to CyberSource.)
American Express	3782 8224 6310 005
Discover	6011 1111 1111 1117
JCB	3566 1111 1111 1113
Mastercard	5555 5555 5555 4444
Visa	4111 1111 1111 1111

Using Amounts to Simulate Errors

You can simulate the CyberSource error messages by requesting authorization, capture, or credit services with specific amounts that trigger the error messages. These triggers work only on the test server, not on the production server. Each payment processor uses its own error messages.

For trigger amounts and responses, see [Using the Test Simulator](#).

Testing American Express Card Verification

Before using CVN with American Express, CyberSource strongly recommends that you perform this procedure.

To test American Express card verification:

- Step 1** Contact CyberSource Customer Support to have your account configured for CVN. Until you do this, you will receive a 1 in the **ccAuthReply_cvCode** reply field.
 - Step 2** Test your system in production using a small currency amount, such as one currency unit. Instead of using the test account numbers, use a real credit card account number, and send an incorrect CVN in the request for authorization. The card should be refused and the request declined.
-

API Fields

Formatting Restrictions

Unless otherwise noted, all field names are case sensitive and all fields accept special characters such as @, #, and %.

**Note**

The values of the **item_#_** fields must not contain carets (^) or colons (:) because these characters are reserved for use by the CyberSource services.

Values for request-level and item-level fields must not contain new lines or carriage returns. However, they can contain embedded spaces and any other printable characters. CyberSource removes all leading and trailing spaces.

Data Type Definitions

For more information about these data types, see the [World Wide Web Consortium \(W3C\) XML Schema Part 2: Datatypes specification](#).

Data Type	Description
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

Numbered Elements

The CyberSource XML schema includes several numbered elements. You can include these complex elements more than once in a request. For example, if a customer order includes more than one item, you need to include multiple `<item>` elements in your request. Each item is numbered, starting with 0. The XML schema uses an `id` attribute in the item's opening tag to indicate the number. For example:

```
<item id="0">
```

For the name-value pair field names, this tag is represented as **item_0**. In this portion of the field name, the underscore before the number does not indicate hierarchy in the XML schema. The item fields are generically referred to as **item_#_<element name>** in the documentation.

Below is an example of the numbered `<item>` element and the corresponding name-value pair field names. If you are using SOAP, the client contains a corresponding `Item` class.

Example Numbered XML Schema Element Names and Name-Value Pair Field Names

XML Schema Element Names	Corresponding Name-Value Pair Field Names
<pre><item id="0"> <unitPrice> <quantity> </item></pre>	<pre>item_0_unitPrice item_0_quantity</pre>
<pre><item id="1"> <unitPrice> <quantity> </item></pre>	<pre>item_1_unitPrice item_1_quantity</pre>



Important

When a request is in XML format and includes an `<item>` element, the element must include an `id` attribute. For example: `<item id="0">`.

Request Fields

See [Getting Started with CyberSource Essentials](#) for a description of how name-value pair names relate to their corresponding XML element names.



Note

When you use Payment Tokenization or Recurring Billing and you include a subscription ID in your request, many of the fields in the following table that are normally required for an authorization or credit become optional. See ["Payment Tokenization," page 102](#), and ["Recurring Billing," page 104](#).

Table 43 Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
authIndicator	Flag that specifies the purpose of the authorization. Possible values: <ul style="list-style-type: none"> ■ 0: Preauthorization ■ 1: Final authorization To set the default for this field, contact CyberSource Customer Support. See "Final Authorization Indicator," page 68 .	ccAuthService (Optional for Mastercard transactions; not used for other card types)	String (1)
billTo_city	City of the billing address.	ccAuthService (R) ⁴ ccCaptureService (O) ccCreditService (R) ^{1,4}	String (50)
billTo_company	Name of the customer's company.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (60)
billTo_country	Country of the billing address. Use the two-character ISO Standard Country Codes .	ccAuthService (R) ⁴ ccCaptureService (O) ccCreditService (R) ^{1,4}	String (2)
billTo_customerID	Your identifier for the customer. When a subscription or customer profile is being created, the maximum length for this field is 30. Otherwise, the maximum length is 100.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (100)

¹ Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

² For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

³ You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see [Getting Started with CyberSource Advanced for the Simple Order API](#).

⁴ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See ["Relaxed Requirements for Address Data and Expiration Date," page 45](#). **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
billTo_email	Customer's email address, including the full domain name.	ccAuthService (R) ⁴ ccCaptureService (O) ccCreditService (R) ^{1,4}	String (255)
billTo_firstName	Customer's first name. This name must be the same as the name on the card.	ccAuthService (R) ⁴ ccCaptureService (O) ccCreditService (R) ^{1,4}	String (60)
billTo_hostname	DNS resolved hostname from billTo_ipAddress .	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (60)
billTo_httpBrowserType	Customer's browser as identified from the HTTP header data. For example, Mozilla is the value that identifies the Netscape browser.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (40)
billTo_ipAddress	Customer's IP address.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (15)
billTo_lastName	Customer's last name. This name must be the same as the name on the card.	ccAuthService (R) ⁴ ccCaptureService (O) ccCreditService (R) ^{1,4}	String (60)
billTo_phoneNumber	Customer's phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (15)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
billTo_postalCode	<p>Postal code for the billing address. The postal code must consist of 5 to 9 digits.</p> <p>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</p> <p>Example A1B 2C3</p>	<p>ccAuthService (Required when the billing country is the U.S. or Canada; otherwise, optional.)⁴</p> <p>ccCaptureService (O)</p> <p>ccCreditService (Required when the billing country is the U.S. or Canada; otherwise, optional.)^{1,4}</p>	String (10)
billTo_state	<p>State or province of the billing address. Use the State, Province, and Territory Codes for the United States and Canada.</p>	<p>ccAuthService (Required when the billing country is the U.S. or Canada; otherwise, optional.)⁴</p> <p>ccCaptureService (O)</p> <p>ccCreditService (Required when the billing country is the U.S. or Canada; otherwise, optional.)^{1,4}</p>	String (2)
billTo_street1	<p>First line of the billing street address as it appears on the credit card issuer's records.</p>	<p>ccAuthService (R)⁴</p> <p>ccCaptureService (O)</p> <p>ccCreditService (R)^{1,4}</p>	String (60)
billTo_street2	<p>Additional address information.</p> <p>Example</p> <p>Attention: Accounts Payable</p> <p>Chase Paymentech Solutions, FDC Compass, and TSYS Acquiring Solutions</p> <p>This value is used for AVS.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p>	String (60)

¹ Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

² For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

³ You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

⁴ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_accountNumber	Customer's credit card number.	ccAuthService (R) ccCreditService (R) ¹	String with numbers only (20)
card_cardType	Type of card to authorize. To see which cards can be handled by each processor, see "Payment Processors," page 19 . Possible values: <ul style="list-style-type: none"> ■ 001: Visa ■ 002: Mastercard ■ 003: American Express ■ 004: Discover ■ 005: Diners Club: See "Discover Acquisitions and Alliances," page 13. ■ 006: Carte Blanche² ■ 007: JCB² 	ccAuthService ccCreditService ¹ Important CyberSource strongly recommends that you send the card type even if it is optional for your processor and card type. Omitting the card type can cause the transaction to be processed with the wrong card type.	String (3)
card_cvIndicator	Flag indicating whether a CVN code was sent. Possible values: <ul style="list-style-type: none"> ■ 0 (default): CVN service not requested. CyberSource uses this default value when you do not include card_cvNumber in the request. ■ 1 (default): CVN service requested and supported. CyberSource uses this default value when you include card_cvNumber in the request. ■ 2: CVN on credit card is illegible. ■ 9: CVN was not imprinted on credit card. 	ccAuthService (O)	String with numbers only (1)
card_cvNumber	CVN. See "Card Verification Numbers (CVNs)," page 50 , for a list of processors that support CVN.	ccAuthService (O)	String with numbers only (4)

¹ Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

² For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

³ You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

⁴ This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See *"Relaxed Requirements for Address Data and Expiration Date," page 45*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_expirationMonth	Two-digit month in which the credit card expires. Format: MM. Possible values: 01 through 12.	ccAuthService (R) ⁴ ccCreditService (R) ^{1,4}	String (2)
card_expirationYear	Four-digit year in which the credit card expires. Format: YYYY. FDC Nashville Global and FDMS South You can send in 2 digits or 4 digits. If you send in 2 digits, they must be the last 2 digits of the year.	ccAuthService (R) ⁴ ccCreditService (R) ^{1,4}	FDC Nashville Global and FDMS South: String (See description) All other processors: String (4)
ccAuthReversalService_authRequestID	Request ID for the authorization that you want to reverse.	ccAuthReversal Service (R)	String (26)
ccAuthReversalService_authRequestToken	Value of the request token returned from a previous request for ccAuthService . The field is an encoded string that contains no confidential information, such as an account number or card verification number. The string can contain a maximum of 256 characters.	ccAuthReversal Service (O)	String (256)
ccAuthReversalService_reversalReason	Reason for the authorization reversal. Possible value: ■ 34: Suspected fraud CyberSource ignores this field for processors that do not support this value.	ccAuthReversal Service (O)	String (3)
ccAuthReversalService_run	Whether to include ccAuthReversalService in your request. Possible values: ■ true: Include the service in your request. ■ false (default): Do not include the service in your request.	ccAuthReversal Service (R)	String (5)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.
2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.
3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.
4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccAuthService_ aggregatorID	Value that identifies you as a payment aggregator. Get this value from the processor. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccAuthService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (20) FDC Nashville Global: String (15)
ccAuthService_ aggregatorName	Your payment aggregator business name. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccAuthService FDC Compass: R for Mastercard aggregator transactions; otherwise, not used. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (37) FDC Nashville Global: String (12)
ccAuthService_ authType	Authorization type. Forced Capture Set this field to <code>verbal</code> and include it in your authorization request to indicate that you are performing a forced capture; therefore, you received the authorization code outside the CyberSource system. See "Forced Captures," page 72 .	ccAuthService Required for a forced capture; otherwise, not used.	String (6)
ccAuthService_ billPayment	Flag indicating that this is a payment for a bill or for an existing contractual loan. See "Visa Bill Payments," page 110 , and "Visa Debt Repayments," page 111 , for lists of processors that support these features. This value is case sensitive. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Bill payment or loan payment. ■ <code>false</code> (default): Not a bill payment or loan payment. 	ccAuthService (O)	String (5)

1 Optional for a follow-on credit request, which must include `ccCreditService_captureRequestID`.

2 For this card type, you must include the `card_cardType` field in your request for an authorization or a stand-alone credit.

3 You must include either `item_#_unitPrice` or `purchaseTotals_grandTotalAmount` in your request. For information about items and grand totals, see [Getting Started with CyberSource Advanced for the Simple Order API](#).

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See ["Relaxed Requirements for Address Data and Expiration Date," page 45](#). **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccAuthService_cavv	Cardholder authentication verification value (CAVV). For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (40)
ccAuthService_cavvAlgorithm	Algorithm used to generate the CAVV for Verified by Visa or the UCAF authentication data for Mastercard SecureCode. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (1)
ccAuthService_commerceIndicator	Type of transaction. Some payment card companies use this information when determining discount rates. Payer Authentication Transactions For the possible values and requirements, see "Payer Authentication," page 95 . Other Types of Transactions See Appendix E, "Commerce Indicators," on page 175 .	ccAuthService (Required for payer authentication transactions; otherwise, optional.)	String (20)
ccAuthService_eciRaw	Raw electronic commerce indicator (ECI). For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (2)
ccAuthService_firstRecurringPayment	Flag indicating whether this transaction is the first in a series of recurring payments. Possible values: <ul style="list-style-type: none"> ■ TRUE: Yes, this is the first payment in a series of recurring payments. ■ FALSE (default): No, this is not the first payment in a series of recurring payments. This field is supported only for FDC Nashville Global.	ccAuthService (O)	String (1)
ccAuthService_paresStatus	Payer authentication response status. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (1)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See *"Relaxed Requirements for Address Data and Expiration Date," page 45*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccAuthService_ partialAuthIndicator	Flag indicating whether the transaction is enabled for partial authorization. When your request includes this field, this value overrides the information in your CyberSource account. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Enable the transaction for partial authorization. ■ <code>false</code>: Do not enable the transaction for partial authorization. See "Partial Authorizations," page 55 .	ccAuthService (O)	String (5)
ccAuthService_run	Whether to include ccAuthService in your request. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. 	ccAuthService (R)	String (5)
ccAuthService_ verbalAuthCode	Authorization code you received from an authorization that you performed outside the CyberSource system. See "Forced Captures," page 72 .	ccAuthService Required for a forced capture; otherwise, not used.	String (6)
ccAuthService_ veresEnrolled	Verification response enrollment status. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (1)
ccAuthService_xid	Transaction identifier. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (40)
ccCaptureService_ aggregatorID	Value that identifies you as a payment aggregator. Get this value from the processor. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccCaptureService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (20) FDC Nashville Global: String (15)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See *"Relaxed Requirements for Address Data and Expiration Date," page 45*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccCaptureService_ aggregatorName	Your payment aggregator business name. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccCaptureService FDC Compass: R for Mastercard aggregator transactions; otherwise, not used. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (37) FDC Nashville Global: String (12)
ccCaptureService_ authRequestID	Value of the request ID returned from a previous ccAuthReply .	ccCaptureService Required unless ccAuthService and ccCaptureService are both called in the same request.	String (26)
ccCaptureService_ authRequestToken	Value of the request token returned from a previous request for ccAuthService . The field is an encoded string that contains no confidential information, such as an account number or card verification number. The string can contain a maximum of 256 characters.	ccCaptureService (O)	String (256)
ccCaptureService_ authType	Authorization type. When the transaction contains a verbally authorized transaction, this field must contain the value <code>verbal</code> .	ccCaptureService (O)	String (6)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccCaptureService_posData	<p>Point-of-sale data. On FDMS South, this field is required for verbal authorizations and forced captures with the American Express card type to comply with the CAPN requirements:</p> <ul style="list-style-type: none"> ■ Forced capture: Obtain the value for this field from the authorization response. ■ Verbal authorization: You cannot obtain a value for this field so CyberSource uses the default value. The default value is generated by CyberSource based on various factors of the transaction such as e-commerce or not, card present or not, and swiped or keyed. See "Verbal Authorizations," page 52. 	ccCaptureService (See the field description.)	String (12)
ccCaptureService_run	<p>Whether to include ccCaptureService in your request. Possible values:</p> <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. 	ccCaptureService (R)	String (5)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccCaptureService_ sequence	Capture number when requesting multiple partial captures for one authorization. Used along with ccCaptureService_totalCount to track which capture is being processed. For example, the second of five captures would be passed to CyberSource as ccCaptureService_sequence = 2 and ccCaptureService_totalCount = 5. See " Special Request Fields for Multiple Partial Captures ," page 35.	ccCaptureService (Required for multiple captures on TSYS Acquiring Solutions. Optional for multiple captures on FDC Compass. Otherwise, not used.)	Integer (2)
ccCaptureService_ totalCount	Total number of captures when requesting multiple partial captures for one authorization. Used along with ccCaptureService_sequence to track which capture is being processed. For example, the second of five captures would be passed to CyberSource as ccCaptureService_sequence = 2 and ccCaptureService_totalCount = 5. See " Special Request Fields for Multiple Partial Captures ," page 35.	ccCaptureService (Required for multiple captures on TSYS Acquiring Solutions. Optional for multiple captures on FDC Compass. Otherwise, not used.)	Integer (2)
ccCaptureService_ transactionID	Transaction ID (TID). On FDMS South, this field is required for verbal authorizations and forced captures with the American Express card type to comply with the CAPN requirements: <ul style="list-style-type: none"> ■ Forced capture: Obtain the value for this field from the authorization response. ■ Verbal authorization: You cannot obtain a value for this field so CyberSource uses the default value of 0000000000000000 (15 zeros). See "Verbal Authorizations," page 52, for important information about using this default value. 	ccCaptureService (See the field description.)	String (15)
ccCaptureService_ verbalAuthCode	Verbally received authorization code.	ccCaptureService (O)	String (6)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.
2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.
3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.
4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccCreditService_ aggregatorID	Value that identifies you as a payment aggregator. Get this value from the processor. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccCreditService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (20) FDC Nashville Global: String (15)
ccCreditService_ aggregatorName	Your payment aggregator business name. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccCreditService FDC Compass: R for Mastercard aggregator transactions; otherwise, not used. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (37) FDC Nashville Global: String (12)
ccCreditService_ billPayment	Flag indicating whether this is a credit for a bill the customer paid with a Visa card. See "Visa Bill Payments," page 110 , for a list of processors that support bill payments with Visa. This value is case sensitive. Possible values: <ul style="list-style-type: none"> ■ true: Credit for a bill payment. ■ false (default): Not a credit for a bill payment 	ccCreditService (O)	String (5)
ccCreditService_ captureRequestID	Value of the request ID returned from a previous request for ccCaptureService . Creates a follow-on credit by linking the credit to the previous capture. When you send this field, you do not need to send several other credit request fields. See "Crediting a Payment," page 38 , for a description of follow-on credits.	ccCreditService (O)	String (26)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.
2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.
3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.
4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ccCreditService_ captureRequestToken	Value of the request token returned from a previous request for ccCaptureService . The field is an encoded string that contains no confidential information, such as an account number or card verification number. The string can contain a maximum of 256 characters.	ccCreditService (O)	String (256)
ccCreditService_ commerceIndicator	Type of transaction. Use with stand-alone credits. Some payment card companies use this information when determining discount rates. Possible values: <ul style="list-style-type: none"> ■ internet (default) ■ moto ■ recurring ■ recurring_internet For details about these values, see Appendix E, "Commerce Indicators," on page 175 .	ccCreditService (O)	String (13)
ccCreditService_run	Whether to include ccCreditService in your request. Possible values: <ul style="list-style-type: none"> ■ true: Include the service in your request. ■ false (default): Do not include the service in your request. 	ccCreditService (R)	String (5)
debtIndicator	Flag indicating whether this is a payment towards an existing contractual loan. See "Visa Debt Repayments," page 111 , for a list of processors that support this feature. Possible values: <ul style="list-style-type: none"> ■ true: Loan payment ■ false (default): Not a loan payment 	ccAuthService (O) ccCreditService (O)	String (5)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
installment_sequence	<p>Installment number when making payments in installments. Used along with installment_totalCount to track which payment is being processed. For example, the second of 5 payments would be passed to CyberSource as installment_sequence = 2 and installment_totalCount = 5. See "Installment Payments," page 73.</p> <p>Chase Paymentech Solutions and FDC Compass This field is optional because this value is required in the merchant descriptors. See "Chase Paymentech Solutions Merchant Descriptors," page 76 and "FDC Compass Merchant Descriptors," page 81.</p>	<p>ccAuthService</p> <p>Chase Paymentech Solutions and FDC Compass: Optional.</p> <p>All other processors: Required for installment payments</p>	Integer (2)
installment_totalCount	<p>Total number of installments when making payments in installments. Used along with installment_sequence to track which payment is being processed. For example, the second of 5 payments would be passed to CyberSource as installment_sequence = 2 and installment_totalCount = 5. See "Installment Payments," page 73.</p> <p>Chase Paymentech Solutions and FDC Compass This field is optional because this value is required in the merchant descriptors. See "Chase Paymentech Solutions Merchant Descriptors," page 76 and "FDC Compass Merchant Descriptors," page 81.</p>	<p>ccAuthService</p> <p>Chase Paymentech Solutions and FDC Compass: Optional.</p> <p>All other processors: Required for installment payments</p>	Integer (2)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ amexDataTAA1	<p>Four Transaction Advice Addendum (TAA) fields. These fields are used to display descriptive information about a transaction on the customer's American Express card statement. When you send TAA fields, start with invoiceHeader_amexDataTAA1, then ...TAA2, and so on. Skipping a TAA field causes subsequent TAA fields to be ignored.</p> <p>To use these fields, contact CyberSource Customer Support to have your account enabled for this feature.</p> <p>For information about merchant descriptors, including which processors support this field, see "Merchant Descriptors," page 76.</p> <p>These fields are frequently used for Level II transactions. See the Level II and Level III Transactions Supplement.</p>	ccCaptureService (O)	String (40)
invoiceHeader_ amexDataTAA2		ccCreditService (O)	
invoiceHeader_ amexDataTAA3			
invoiceHeader_ amexDataTAA4			
invoiceHeader_ merchantDescriptor	<p>For the descriptions, used-by information, data types, and lengths for these fields, see "Merchant Descriptors," page 76.</p>		
invoiceHeader_ merchantDescriptor Alternate			
invoiceHeader_ merchantDescriptor City			
invoiceHeader_ merchantDescriptor Contact			
invoiceHeader_ merchantDescriptor Country			
invoiceHeader_ merchantDescriptor PostalCode			
invoiceHeader_ merchantDescriptor Street			
<p>1 Optional for a follow-on credit request, which must include ccCreditService_captureRequestID.</p> <p>2 For this card type, you must include the card_cardType field in your request for an authorization or a stand-alone credit.</p> <p>3 You must include either item #_unitPrice or purchaseTotals_grandTotalAmount in your request. For information about items and grand totals, see <i>Getting Started with CyberSource Advanced for the Simple Order API</i>.</p> <p>4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p>			

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ submerchantCity	Sub-merchant's city. See "Aggregator Support," page 63. FDC Compass This value must consist of uppercase characters.	ccAuthService ccCaptureService ccCreditService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (21) FDC Nashville Global: String (11)
invoiceHeader_ submerchantCountry	Sub-merchant's country. Use the two-character ISO Standard Country Codes . See "Aggregator Support," page 63. FDC Compass This value must consist of uppercase characters.	ccAuthService ccCaptureService ccCreditService FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (3)
invoiceHeader_ submerchantEmail	Sub-merchant's email address. See "Aggregator Support," page 63.	ccAuthService ccCaptureService ccCreditService FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (40) FDC Nashville Global: String (19)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ submerchantID	The ID you assigned to your sub-merchant. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters.	ccAuthService ccCaptureService ccCreditService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.W	FDC Compass: String (20) FDC Nashville Global: String (14)
invoiceHeader_ submerchant MerchantID	Unique identifier assigned by the payment card company to the sub-merchant. See "Aggregator Support," page 63 .	ccAuthService FDC Compass: not used. FDC Nashville Global: O for American Express aggregator authorizations; otherwise, not used.	String (15)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.
2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.
3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.
4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ submerchantName	<p>Sub-merchant's business name. See "Aggregator Support," page 63.</p> <p>FDC Compass This value must consist of uppercase characters.</p> <p>FDC Nashville Global With Mastercard, the maximum length of the sub-merchant name depends on the length of the aggregator name:</p> <ul style="list-style-type: none"> ■ If aggregator name length is 1 through 3, maximum sub-merchant name length is 21. ■ If aggregator name length is 4 through 7, maximum sub-merchant name length is 17. ■ If aggregator name length is 8 through 12, maximum sub-merchant name length is 12. 	<p>ccAuthService</p> <p>ccCaptureService</p> <p>ccCreditService</p> <p>FDC Compass: R for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>FDC</p> <p>Compass with American Express: String (19)</p> <p>FDC Compass with Mastercard: String (37)</p> <p>FDC Nashville Global with American Express: String (12)</p> <p>FDC Nashville Global with Mastercard: String (see description)</p>
invoiceHeader_ submerchantPostal Code	<p>Partial postal code for the sub-merchant's address. See "Aggregator Support," page 63.</p> <p>FDC Compass This value must consist of uppercase characters.</p>	<p>ccAuthService</p> <p>ccCaptureService</p> <p>ccCreditService</p> <p>FDC Compass: O for all aggregator transactions.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	<p>FDC</p> <p>Compass: String (15)</p> <p>FDC Nashville Global: String (9)</p>

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ submerchantRegion	Sub-merchant's region. Example NE indicates that the sub-merchant is in the northeast region. See " Aggregator Support ," page 63.	ccAuthService FDC Compass: not used. FDC Nashville Global: O for all aggregator authorizations; otherwise, not used.	String (3)
invoiceHeader_ submerchantState	Sub-merchant's state or province. Use the State, Province, and Territory Codes for the United States and Canada . See " Aggregator Support ," page 63. FDC Compass This value must consist of uppercase characters.	ccAuthService ccCaptureService ccCreditService FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	String (3)
invoiceHeader_ submerchantStreet	First line of the sub-merchant's street address. See " Aggregator Support ," page 63. FDC Compass This value must consist of uppercase characters.	ccAuthService ccCaptureService ccCreditService FDC Compass: O for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (38) FDC Nashville Global: String (25)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
invoiceHeader_ submerchantTelephone Number	Sub-merchant's telephone number. See "Aggregator Support," page 63 . FDC Compass This value must consist of uppercase characters. Use one of these recommended formats: NNN-NNN-NNNN NNN-AAAAAAA	ccAuthService ccCaptureService ccCreditService FDC Compass: R for all aggregator transactions. FDC Nashville Global: R for all aggregator transactions.	FDC Compass: String (13) FDC Nashville Global: String (10)
item_#_productCode	Type of product. This value is used to determine the category that the product is in: electronic, handling, physical, service, or shipping. The default value is default. See Table 51, "Product Codes," on page 182 for a list of valid values. For ccAuthService , when you set this field to a value other than default or any of the values related to shipping and/or handling, the item_#_quantity , item_#_productName , and item_#_productSKU fields are required. See "Numbered Elements," page 118 .	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (255)
item_#_productName	For ccAuthService and ccCaptureService , this field is required when item_#_productCode is not default or one of the values related to shipping and/or handling. See "Numbered Elements," page 118 .	ccAuthService (See the field description.) ccCaptureService (See the field description.)	String (255)
item_#_productSKU	Identification code for the product. For ccAuthService and ccCaptureService , this field is required when item_#_productCode is not default or one of the values related to shipping and/or handling. See "Numbered Elements," page 118 .	ccAuthService (See the field description.) ccCaptureService (See the field description.)	String (255)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.
2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.
3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.
4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See *"Relaxed Requirements for Address Data and Expiration Date," page 45*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_quantity	<p>The default is 1. For ccAuthService and ccCaptureService, this field is required when item_#_productCode is not default or one of the values related to shipping and/or handling.</p> <p>See "Numbered Elements," page 118.</p>	<p>ccAuthService (See the field description.)</p> <p>ccAuthReversal Service (O)</p> <p>ccCaptureService (See the field description.)</p> <p>ccCreditService (O)</p>	Integer (10)
item_#_taxAmount	<p>Total tax to apply to the product. This value cannot be negative. The tax amount and the unit price must be in the same currency.</p> <p>The tax amount field is additive. The following example uses a two-exponent currency such as USD:</p> <p>1 You include the following items in your request:</p> <pre> item_0_unitPrice=10.00 item_0_quantity=1 item_0_taxAmount=0.80 item_1_unitPrice=20.00 item_1_quantity=1 item_1_taxAmount=1.60 </pre> <p>2 The total amount authorized will be 32.40, not 30.00 with 2.40 of tax included.</p> <p>This field is frequently used for Level II and Level III transactions. See the Level II and Level III Transactions Supplement.</p> <p>See "Numbered Elements," page 118.</p>	<p>ccAuthService (O)</p> <p>ccCaptureService (O)</p> <p>ccCreditService (O)</p>	String (15)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_unitPrice	<p>Per-item price of the product. This value cannot be negative. You can include a decimal point (.) in this field, but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places.</p> <p>See "Numbered Elements," page 118.</p> <p>Important Some processors have specific requirements and limitations, such as maximum amounts and maximum field lengths. This information is covered in:</p> <ul style="list-style-type: none"> ■ Table 9, "Authorization Information for Specific Processors," on page 25 ■ Table 13, "Capture Information for Specific Processors," on page 32 ■ Table 17, "Credit Information for Specific Processors," on page 41 <p>Zero Amount Authorizations</p> <p>If your processor supports zero amount authorizations, you can set this field to 0 for the authorization to check if the card is lost or stolen. See "Zero Amount Authorizations," page 112.</p>	ccAuthService ³ ccAuthReversalService ³ ccCaptureService ³ ccCreditService ³	String (15)
linkToRequest	<p>Value that links the current authorization request to the original authorization request. Set this value to the request ID that was returned in the reply message from the original authorization request.</p> <p>This value is used for partial authorizations as described in "Partial Authorizations," page 55.</p>	ccAuthService (O)	String (26)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchantCategoryCode	<p>Four-digit number that the payment card industry uses to classify merchants into market segments. Visa assigned one or more of these values to your business when you started accepting Visa cards.</p> <p>If you do not include this field in your request, CyberSource uses the value in your CyberSource account.</p> <p>See "Aggregator Support," page 63.</p>	<p>ccAuthService ccCaptureService ccCreditService</p> <p>FDC Compass: O for all aggregator authorizations; otherwise, not used.</p> <p>FDC Nashville Global: R for all aggregator transactions.</p>	Integer (4)
merchantDefinedData_ field1 to merchantDefinedData_ field20	<p>Fields that you can use to store information.</p> <p>Important These fields have been replaced by merchantDefinedData_mddField_1 to 100. CyberSource recommends that you update your order management system to use the new fields.</p> <p>Warning Merchant-defined fields <i>must not</i> be used to capture personally identifying information as stated in the warning under the following field description for merchantDefinedData_mddField_1 to 100.</p>	<p>ccAuthService (O) ccCaptureService (O) ccCreditService (O)</p>	String (255)
<p>1 Optional for a follow-on credit request, which must include ccCreditService_captureRequestID.</p> <p>2 For this card type, you must include the card_cardType field in your request for an authorization or a stand-alone credit.</p> <p>3 You must include either item_#_unitPrice or purchaseTotals_grandTotalAmount in your request. For information about items and grand totals, see <i>Getting Started with CyberSource Advanced for the Simple Order API</i>.</p> <p>4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p>			

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchantDefinedData_ mddField_1 to merchantDefinedData_ mddField_100	<p>Fields that you can use to store information.</p> <p>Important These fields override the old merchant-defined data fields. For example, if you use the obsolete field merchantDefinedData_field15 and the new field merchantDefinedData_mddField_15 in the same request, the value for the new field overwrites the value for the obsolete field.</p> <p>Warning Merchant-defined data fields are not intended to and <i>must not</i> 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. Personally identifying information includes, but is not limited to, address, credit card number, social security number, driver's license number, state-issued identification number, passport number, and 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.</p>	ccAuthService (O) ccCaptureService (O) ccCreditService (O)	String (255)
merchantID	Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production.	Required for all credit card services.	String (30)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchantReference Code	Merchant-generated order reference or tracking number. CyberSource recommends that you send a unique value for each transaction so that you can perform meaningful searches for the transaction. For information about tracking orders, see Getting Started with CyberSource Essentials . FDC Nashville Global Certain circumstances can cause the processor to truncate this value to 15 or 17 characters for Level II and Level III processing, which can cause a discrepancy between the value you submit and the value included in some processor reports.	Required for all credit card services.	String (50)
merchantTransaction Identifier	Identifier that you assign to the transaction. See "Merchant-Initiated Reversals and Voids," page 93 .	ccAuthService (O) ccAuthReversal Service (O) ccCaptureService (O) ccCreditService (O) voidService (O)	String (15)
orderRequestToken	The request token value returned from a previous request. This value links the previous request to the current follow-on request. This field is an encoded string that does not contain any confidential information, such as account numbers or card verification numbers. The string can contain a maximum of 256 characters.	ccAuthReversal Service (O) ccCaptureService (O) ccCreditService (O) voidService (O)	String (256)
purchaseTotals_ currency	Currency used for the order. Use the three-character ISO Standard Currency Codes . For ccAuthReversalService and ccCaptureService , you must use the same currency that you used in your request for ccAuthService .	ccAuthService (R) ccAuthReversal Service (R) ccCaptureService (R) ccCreditService (R)	String (5)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see [Getting Started with CyberSource Advanced for the Simple Order API](#).

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
purchaseTotals_ grandTotalAmount	<p>Grand total for the order. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places.</p> <p>Important Some processors have specific requirements and limitations, such as maximum amounts and maximum field lengths. This information is covered in:</p> <ul style="list-style-type: none"> ■ Table 9, "Authorization Information for Specific Processors," on page 25 ■ Table 13, "Capture Information for Specific Processors," on page 32 ■ Table 17, "Credit Information for Specific Processors," on page 41 <p>If your processor supports zero amount authorizations, you can set this field to 0 for the authorization to check if the card is lost or stolen. See "Zero Amount Authorizations," page 112.</p>	ccAuthService ³ ccAuthReversalService ³ ccCaptureService ³ ccCreditService ³	String (15)
recurringSubscription Info_subscriptionID	<p>When you are using Payment Tokenization or Recurring Billing and you include this value in your request, many of the fields that are normally required for an authorization or credit become optional. See "Payment Tokenization," page 102, and "Recurring Billing," page 104.</p>	ccAuthService (O) ccCreditService (O)	String (26)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See ["Relaxed Requirements for Address Data and Expiration Date," page 45](#). **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
shipFrom_postalCode	<p>Postal code for the address from which the goods are shipped, which is used to establish nexus. The default is the postal code associated with your CyberSource account. The postal code must consist of 5 to 9 digits.</p> <p>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</p> <p>Example A1B 2C3</p> <p>This field is frequently used for Level II and Level III transactions. See the Level II and Level III Transactions Supplement.</p>	<p>ccCaptureService (O)</p> <p>ccCreditService (O)</p>	String (10)
shipTo_city	City of the shipping address.	<p>ccAuthService</p> <p>Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.</p>	String (50)
shipTo_country	Country of the shipping address. Use the two-character ISO Standard Country Codes .	<p>ccAuthService</p> <p>ccCaptureService</p> <p>ccCreditService</p> <p>Required if any shipping address information is included in the request; otherwise, optional.</p>	String (2)
shipTo_firstName	First name of the recipient.	ccAuthService (O)	String (60)
shipTo_lastName	Last name of the recipient.	ccAuthService (O)	String (60)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
shipTo_postalCode	<p>Postal code for the shipping address. The postal code must consist of 5 to 9 digits.</p> <p>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</p> <p>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</p>	<p>ccAuthService</p> <p>ccCaptureService</p> <p>ccCreditService</p> <p>Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.</p>	String (10)
shipTo_shippingMethod	<p>Shipping method for the product. Possible values:</p> <ul style="list-style-type: none"> ■ lowcost : Lowest-cost service ■ sameday : Courier or same-day service ■ oneday : Next-day or overnight service ■ twoday : Two-day service ■ threeday : Three-day service ■ pickup : Store pick-up ■ other : Other shipping method ■ none : No shipping method because product is a service or subscription 	ccAuthService (O)	String (10)
shipTo_state	<p>State or province of the shipping address. Use the State, Province, and Territory Codes for the United States and Canada.</p>	<p>ccAuthService</p> <p>Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.</p>	String (2)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 43 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
shipTo_street1	First line of the shipping address.	ccAuthService Required if any shipping address information is included in the request; otherwise, optional.	String (60)
shipTo_street2	Second line of the shipping address.	ccAuthService (O)	String (60)
ucaf_authenticationData	Universal cardholder authentication field (UCAF) data. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String (32)
ucaf_collectionIndicator	Universal cardholder authentication field (UCAF) collection indicator. For the description and requirements, see "Payer Authentication," page 95 .	ccAuthService	String with numbers only (1)
voidService_run	Whether to include voidService in your request. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. 	voidService (R)	String (5)
voidService_voidRequestID	Request ID of the capture or credit you want to void.	voidService (R)	String (26)
voidService_voidRequestToken	Value of the request token returned from a previous request for a service that you want to void. The field is an encoded string that contains no confidential information, such as an account number or card verification number. The string can contain a maximum of 256 characters.	voidService (O)	String (256)

1 Optional for a follow-on credit request, which must include **ccCreditService_captureRequestID**.

2 For this card type, you must include the **card_cardType** field in your request for an authorization or a stand-alone credit.

3 You must include either **item_#_unitPrice** or **purchaseTotals_grandTotalAmount** in your request. For information about items and grand totals, see *Getting Started with CyberSource Advanced for the Simple Order API*.

4 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 45. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Reply Fields

Table 44 Reply Fields

Field	Description	Returned By	Data Type & Length
authIndicator	<p>Flag indicating the type of authorization that was performed. Possible values:</p> <ul style="list-style-type: none"> ■ 0: Preauthorization ■ 1: Final authorization <p>See "Final Authorization Indicator," page 68. This field is not returned for unmarked authorizations.</p> <p>This field is returned only for Chase Paymentech Solutions, FDC Compass, FDC Nashville Global, and FDMS Nashville.</p>	ccAuthReply	String (1)
ccAuthReply_accountBalance	<p>Remaining balance on the prepaid card. See "Balance Responses," page 60.</p>	ccAuthReply	String (12)
ccAuthReply_accountBalanceCurrency	<p>Currency of the remaining balance on the prepaid card. For the possible values, see the ISO Standard Currency Codes. Also see "Balance Responses," page 60.</p>	ccAuthReply	String (5)
ccAuthReply_accountBalanceSign	<p>Sign for the remaining balance on the prepaid card. Returned only when the processor returns this value. Possible values:</p> <ul style="list-style-type: none"> ■ positive ■ negative 	ccAuthReply	String (8)
ccAuthReply_affluenceIndicator	<p>Chase Paymentech Solutions</p> <p>Indicates whether a customer has high credit limits. This information enables you to market high cost items to these customers and to understand the kinds of cards that high income customers are using.</p> <p>This field is supported for Visa, Mastercard, Discover, and Diners Club.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_amount	<p>Amount that was authorized.</p>	ccAuthReply	String (15)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ authFactorCode	Risk factor code from Smart Authorization. This value consists of one or more codes separated by carets (^). For the codes, see Appendix M, "Smart Authorization Factor Codes," on page 191 . For information about Smart Authorization, see the Business Center User Guide .	ccAuthReply	String (100)
ccAuthReply_ authorizationCode	Authorization code. Returned only when the processor returns this value. TSYS Acquiring Solutions The returned value for a successful zero amount authorization is 000000. See "Zero Amount Authorizations," page 112 .	ccAuthReply	String (7 or more) The length of this value depends on your processor.
ccAuthReply_ authorizedDateTime	Time of authorization. Format: YYYY-MM-DDThh:mm:ssZ Example 2012-08-11T22:47:57Z is equal to August 11, 2012, at 10:47:57 P.M. The T separates the date and the time. The Z indicates UTC.	ccAuthReply	String (20)
ccAuthReply_ avsCode	AVS results. See "Address Verification System (AVS)," page 44 , for a description of AVS. See Appendix D, "AVS Codes," on page 172 , for the list of AVS codes.	ccAuthReply	String (1)
ccAuthReply_ avsCodeRaw	AVS result code sent directly from the processor. Returned only when the processor returns this value. Important Do not use this field to evaluate the result of AVS. Use for debugging purposes only.	ccAuthReply	String (10)
ccAuthReply_ cardCategory	GPN Visa or Mastercard product ID. For the possible values, see Appendix K, "Product IDs," on page 183 . RBS WorldPay Atlanta Type of card used in the transaction. Possible values: <ul style="list-style-type: none">■ B: Business Card■ O: Noncommercial Card■ R: Corporate Card■ S: Purchase Card■ Blank: Purchase card not supported	ccAuthReply	GPN: String (3) RBS WorldPay Atlanta: String (1)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ cardCommercial	<p>Indicates whether the card is a commercial card, which enables you to include Level II data in your transaction requests.</p> <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cardHealthcare	<p>Indicates whether the card is a healthcare card.</p> <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cardIssuerCountry	<p>Country in which the card was issued. This information enables you to determine whether the card was issued domestically or internationally. Use the two-character ISO Standard Country Codes.</p> <p>This field is supported for Visa, Mastercard, Discover, Diners Club, JCB, and Maestro (International) on Chase Paymentech Solutions.</p> <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (3)
ccAuthReply_ cardLevel3Eligible	<p>Indicates whether the card is eligible for Level III interchange fees, which enables you to include Level III data in your transaction requests.</p> <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ cardPayroll	<p>Indicates whether the card is a payroll card.</p> <p>This field is supported for Visa, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cardPINlessDebit	<p>Indicates whether the card is a PINless debit card.</p> <p>This field is supported for Visa and Mastercard on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cardPrepaid	<p>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, installment, or deferred billing relationship.</p> <p>This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ cardRegulated	<p>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.</p> <p>This field is supported for Visa, Mastercard, Discover, Diners Club, and JCB on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes (assets greater than 10B USD) ■ N: No (assets less than 10B USD) ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cardSignatureDebit	<p>Indicates whether the card is a signature debit card. This information enables you to alter the way an order is processed. For example, you might not want to reauthorize a transaction for a signature debit card, or you might want to perform reversals promptly for a signature debit card.</p> <p>This field is supported for Visa, Mastercard, and Maestro (International) on Chase Paymentech Solutions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ Y: Yes ■ N: No ■ X: Not applicable / Unknown <p>See "Card Type Indicators (CTIs)," page 67.</p>	ccAuthReply	String (1)
ccAuthReply_ cavvResponseCode	<p>Mapped response code for Verified by Visa. See "Verified by Visa," page 95, and Appendix N, "Verified by Visa Response Codes," on page 192.</p>	ccAuthReply	String (3)
ccAuthReply_ cavvResponseCode Raw	<p>Raw response code sent directly from the processor for Verified by Visa. See "Verified by Visa," page 95.</p>	ccAuthReply	String (3)
ccAuthReply_ cvCode	<p>CVN result code. See "Card Verification Numbers (CVNs)," page 50, for a description of the card verification check. See Appendix F, "CVN Codes," on page 176 for the list of CVN codes.</p>	ccAuthReply	String (1)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ cvCodeRaw	CVN result code sent directly from the processor. Returned only when the processor returns this value. Important Do not use this field to evaluate the result of card verification. Use for debugging purposes only.	ccAuthReply	String (10)
ccAuthReply_ merchantAdviceCode	Reason the recurring payment transaction was declined. For some processors, this field is used only for Mastercard. For other processors, this field is used for Visa and Mastercard. And for other processors, this field is not implemented. Possible values: <ul style="list-style-type: none"> ■ 00: Response not provided. ■ 01: New account information is available. Obtain the new information. ■ 02: Try again later. ■ 03: Do not try again. Obtain another type of payment from the customer. ■ 21: Recurring payment cancellation service. ■ 99: An unknown value was returned from the processor. 	ccAuthReply	String (2)
ccAuthReply_ merchantAdviceCode Raw	Raw merchant advice code sent directly from the processor. This field is used only for Mastercard.	ccAuthReply	String (2)
ccAuthReply_ ownerMerchantID	Merchant ID that was used to create the subscription or customer profile for which the service was requested. Payment Tokenization When your account is enabled for Payment Tokenization, this field is returned only when you use profile sharing and when your merchant ID is in the same merchant ID pool as the owner merchant ID. See the profile sharing information in Payment Tokenization Using the Simple Order API for CyberSource Essentials . Recurring Billing When your account is enabled for Recurring Billing, this field is returned only when you use subscription sharing and when your merchant ID is in the same merchant ID pool as the owner merchant ID. See the subscription sharing information in Recurring Billing Using the Simple Order API for CyberSource Essentials .	ccAuthReply	String (30)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ paymentNetwork TransactionID	Network transaction ID. You can use this value to identify a specific transaction when discussing it with your processor. Not all processors provide this value. For details about this value for GPN, see Appendix I, "Network Transaction Identifiers," on page 181.	ccAuthReply	String (15)
ccAuthReply_ processorResponse	For most processors, this is the error message sent directly from the bank. Returned only when the processor returns this value. Important Do not use this field to evaluate the result of the authorization.	ccAuthReply	String (10)
ccAuthReply_ reasonCode	Numeric value corresponding to the result of the credit card authorization request. See Appendix L, "Reason Codes," on page 187.	ccAuthReply	Integer (5)
ccAuthReply_ reconciliationID	Reference number for the transaction. This value is not returned for all processors. See Table 6, "Fields for Reconciliation IDs," on page 19 for the list of processors for which this value is returned. See Getting Started with CyberSource Essentials for information about order tracking and reconciliation.	ccAuthReply	String (60)
ccAuthReply_ referralResponse Number	Referral response number for a verbal authorization with FDMS Nashville when using an American Express card. Give this number to American Express when you call them for the verbal authorization.	ccAuthReply	String (6)
ccAuthReply_ requestAmount	Amount you requested to be authorized. This value is returned for partial authorizations as described in "Partial Authorizations," page 55.	ccAuthReply	String (15)
ccAuthReply_ requestCurrency	Currency for the amount you requested to be authorized. This value is returned for partial authorizations as described in "Partial Authorizations," page 55. For the possible values, see the ISO Standard Currency Codes.	ccAuthReply	String (5)
ccAuthReversalReply_ amount	Amount that was reversed.	ccAuthReversal Reply	String (15)
ccAuthReversalReply_ authorizationCode	Authorization code. Returned only when the authorization code is returned by the processor.	ccAuthReversal Reply	String (6)
ccAuthReversalReply_ processorResponse	Processor response code.	ccAuthReversal Reply	String (10)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReversalReply_reasonCode	Numeric value corresponding to the result of the full authorization reversal request. See Appendix L, "Reason Codes," on page 187 .	ccAuthReversal Reply	Integer (5)
ccAuthReversalReply_requestDateTime	Date and time at which the service was requested. 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.	ccAuthReversal Reply	String (20)
ccCaptureReply_amount	Amount that was captured.	ccCaptureReply	String (15)
ccCaptureReply_reasonCode	Numeric value corresponding to the result of the capture request. See Appendix L, "Reason Codes," on page 187 .	ccCaptureReply	Integer (5)
ccCaptureReply_reconciliationID	Reference number that you use to reconcile your CyberSource reports with your processor reports. See Getting Started with CyberSource Essentials for information about order tracking and reconciliation.	ccCaptureReply	FDC Nashville Global: String (8) All other processors: String (60)
ccCaptureReply_requestDateTime	Date and time at which the service was requested. 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.	ccCaptureReply	String (20)
ccCreditReply_amount	Amount that was credited.	ccCreditReply	String (15)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccCreditReply_ownerMerchantID	<p>Merchant ID that was used to create the subscription or customer profile for which the service was requested.</p> <p>Payment Tokenization When your account is enabled for Payment Tokenization, this field is returned only when you use profile sharing and when your merchant ID is in the same merchant ID pool as the owner merchant ID. See the profile sharing information in Payment Tokenization Using the Simple Order API for CyberSource Essentials.</p> <p>Recurring Billing When your account is enabled for Recurring Billing, this field is returned only when you use subscription sharing and when your merchant ID is in the same merchant ID pool as the owner merchant ID. See the subscription sharing information in Recurring Billing Using the Simple Order API for CyberSource Essentials.</p>	ccCreditReply	String (30)
ccCreditReply_reasonCode	Numeric value corresponding to the result of the credit request. See Appendix L, "Reason Codes," on page 187 .	ccCreditReply	Integer (5)
ccCreditReply_reconciliationID	Reference number that you use to reconcile your CyberSource reports with your processor reports. See Getting Started with CyberSource Essentials for information about order tracking and reconciliation.	ccCreditReply	FDC Nashville Global: String (8) All other processors: String (60)
ccCreditReply_requestDateTime	<p>Date and time at which the service was requested.</p> <p>Format: YYYY-MM-DDThh:mm:ssZ</p> <p>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.</p>	ccCreditReply	String (20)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
decision	<p>Summarizes the result of the overall request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ ACCEPT ■ ERROR ■ REJECT <p>For details about these values, see the information about handling replies in Getting Started with CyberSource Essentials.</p>	All credit card services	String (6)
invalidField_0 through invalidField_N	<p>Fields in the request that have invalid data. For information about missing or invalid fields, see Getting Started with CyberSource Essentials.</p> <p>Note These fields are included as an aid to software developers only. Do not use these fields to interact with your customers.</p>	All credit card services	String (100)
merchantReference Code	<p>Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupted characters.</p> <p>FDC Nashville Global</p> <p>There are some special circumstances in which the processor truncates this value to 15 or 17 characters for Level II and Level III processing. This can cause a discrepancy between the value you submit and the value included in some processor reports.</p>	All credit card services	String (50)
missingField_0 through missingField_N	<p>Required fields that were missing from the request. For information about missing or invalid fields, see Getting Started with CyberSource Essentials.</p> <p>Note These fields are included as an aid to software developers only. Do not use these fields to interact with your customers.</p>	All credit card services	String (100)
originalTransaction_amount	Amount of the original transaction. See "Merchant-Initiated Reversals and Voids," page 93 .	ccAuthReversal Reply voidReply	String (15)
originalTransaction_reasonCode	Reason code for the original transaction. See "Merchant-Initiated Reversals and Voids," page 93 .	ccAuthReversal Reply voidReply	String (50)

Table 44 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
purchaseTotals_ currency	Currency used for the order. For the possible values, see the ISO Standard Currency Codes .	ccAuthReply ccAuthReversal Reply ccCaptureReply ccCreditReply	String (5)
reasonCode	Numeric value corresponding to the result of the overall request. See Appendix L, "Reason Codes," on page 187 .	All credit card services	Integer (5)
requestID	Identifier for the request.	All credit card services	String (26)
requestToken	Request token data created by CyberSource for each reply. The field is an encoded string that contains no confidential information such as an account or card verification number. The string can contain a maximum of 256 characters. Note When you request the authorization and capture services together, the request token is for the capture reply only.	All credit card services	String (256)
voidReply_ amount	Amount that was voided.	voidReply	String (15)
voidReply_ currency	Currency used for the order. For the possible values, see the ISO Standard Currency Codes .	voidReply	String (5)
voidReply_ reasonCode	Numeric value corresponding to the result of the void request. See Appendix L, "Reason Codes," on page 187 .	voidReply	Integer (5)
voidReply_ requestDateTime	Date and time at which the service was requested. 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.	voidReply	String (20)

Examples

Name-Value Pair Examples

Basic Credit Card Examples

Example 1 Credit Card Authorization Request

```
ccAuthService_run=true
merchantID=infodev
merchantReferenceCode=482046C3A7E94F5
billTo_firstName=John
billTo_lastName=Doe
billTo_street1=1295 Charleston Rd.
billTo_city=Mountain View
billTo_state=CA
billTo_postalCode=94043
billTo_country=US
billTo_phoneNumber=650-965-6000
billTo_email=jdoe@example.com
item_0_unitPrice=49.95
item_0_quantity=1
purchaseTotals_currency=USD
card_expirationMonth=12
card_expirationYear=2015
card_accountNumber=4111111111111111
```

Example 2 Credit Card Authorization Reply

```
requestID=0305782650000167905080
decision=ACCEPT
reasonCode=100
merchantReferenceCode=482046C3A7E94F5
purchaseTotals_currency=USD
ccAuthReply_reasonCode=100
ccAuthReply_amount=49.95
ccAuthReply_accountBalance=50.05
ccAuthReply_authorizationCode=123456
ccAuthReply_avsCode=Y
ccAuthReply_avsCodeRaw=YYY
ccAuthReply_processorResponse=A
```

Example 3 Credit Card Capture Request

```
ccCaptureService_authRequestID=0305782650000167905080
merchantID=infodev
merchantReferenceCode=482046C3A7E94F5BD1FE3C66C
ccCaptureService_run=true
item_0_unitPrice=49.95
purchaseTotals_currency=USD
```

Example 4 Credit Card Capture Reply

```
requestID=1019827520348290570293
merchantReferenceCode=482046C3A7E94F5BD1FE3C66C
decision=ACCEPT
reasonCode=100
ccCaptureReply_amount=49.95
purchaseTotals_currency=USD
ccCaptureReply_reasonCode=100
ccCaptureReply_reconciliationID=1094820975023470
```

Partial Authorization Examples

Fully Approved Request

The following two examples consist of an authorization request that is fully approved and the subsequent authorization reply, which includes balance information:

- Original request amount: 1500.00 USD
- Approved amount: 1500.00 USD
- Balance amount: 23.62 USD positive

Example 5 Fully Approved Authorization Request

```
ccAuthService_run=true
merchantID=OkGo
merchantReferenceCode=AB1234.1-1
billTo_firstName=John
billTo_lastName=Smith
billTo_street1=201 S. Division St.
billTo_street2=Suite 500
billTo_city=Ann Arbor
billTo_state=MI
billTo_country=US
billTo_postalCode=48104-2201
billTo_email=okgo@example.com
billTo_phoneNumber=123-456-7890
card_accountNumber=4111111111111111
card_cardType=001
card_cvNumber=xxx
card_expirationMonth=12
card_expirationYear=2015
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=1500.00
```

Example 6 Fully Approved Authorization Reply

```

merchantReferenceCode=AB1234.1-1
requestID=2688497722340000852964
decision=ACCEPT
reasonCode=100
ccAuthReply_reasonCode=100
ccAuthReply_amount=1500.00
ccAuthReply_avsCode=A
ccAuthReply_avsCodeRaw=A
ccAuthReply_authorizationCode=831000
ccAuthReply_processorResponse=000
ccAuthReply_accountBalance=23.62
ccAuthReply_accountBalanceCurrency=USD
ccAuthReply_accountBalanceSign=positive
ccAuthReply_cardCategory=J1
ccAuthReply_cvCode=3
ccAuthReply_merchantAdviceCode=00
purchaseTotals_currency=USD

```

Partially Approved Request

The following two examples consist of an authorization request that is partially approved and the subsequent authorization reply:

- Original request amount: 1401.00 USD
- Approved amount: 500.00 USD

Example 7 Partially Approved Authorization Request

```

ccAuthService_run=true
merchantID=OkGo
merchantReferenceCode=AB1234.1-1
billTo_firstName=John
billTo_lastName=Smith
billTo_street1=201 S. Division St.
billTo_street2=Suite 500
billTo_city=Ann Arbor
billTo_state=MI
billTo_country=US
billTo_postalCode=48104-2201
billTo_email=okgo@example.com
billTo_phoneNumber=123-456-7890
card_accountNumber=4111111111111111
card_cardType=001
card_cvNumber=xxx
card_expirationMonth=12
card_expirationYear=2015
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=1401.00

```

Example 8 Partially Approved Authorization Reply

```
merchantReferenceCode=AB1234.1-1  
requestID=2688497722340000852964  
decision=REJECT  
reasonCode=110  
ccAuthReply_reasonCode=110  
ccAuthReply_amount=500.00  
ccAuthReply_avsCode=A  
ccAuthReply_avsCodeRaw=A  
ccAuthReply_authorizationCode=831000  
ccAuthReply_processorResponse=010  
ccAuthReply_requestAmount=1401.00  
ccAuthReply_requestCurrency=USD  
ccAuthReply_cardCategory=J1  
ccAuthReply_cvCode=3  
ccAuthReply_merchantAdviceCode=00  
purchaseTotals_currency=USD
```

XML Examples

Basic Credit Card Examples

Example 9 Credit Card Authorization Request

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.23">
  <merchantID>infodev</merchantID>
  <merchantReferenceCode>482046C3A7E94F5</merchantReferenceCode>
  <billTo>
    <firstName>John</firstName>
    <lastName>Doe</lastName>
    <street1>1295 Charleston Rd.</street1>
    <city>Mountain View</city>
    <state>CA</state>
    <postalCode>94043</postalCode>
    <country>US</country>
    <phoneNumber>650-965-6000</phoneNumber>
    <email>jdoe@example.com</email>
  </billTo>
  <item id="0">
    <unitPrice>49.95</unitPrice>
    <quantity>1</quantity>
  </item>
  <purchaseTotals>
    <currency>USD</currency>
  </purchaseTotals>
  <card>
    <accountNumber>4111111111111111</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2015</expirationYear>
  </card>
  <ccAuthService run="true"/>
</requestMessage>
```

Example 10 Credit Card Authorization Reply

```

<c:replyMessage xmlns:c="urn:schemas-cybersource-com:transaction-data-1.23">
  <c:merchantReferenceCode>482046C3A7E94F5</c:merchantReferenceCode>
  <c:requestID>0305782650000167905080</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>49.95</c:amount>
    <c:authorizationCode>123456</c:authorizationCode>
    <c:avsCode>Y</c:avsCode>
    <c:avsCodeRaw>YY</c:avsCodeRaw>
    <c:processorResponse>A</c:processorResponse>
    <c:accountBalance>50.05</c:accountBalance>
  </c:ccAuthReply>
</c:replyMessage>

```

Example 11 Credit Card Capture Request

```

<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.37">
  <merchantID>infodev</merchantID>
  <merchantReferenceCode>482046C3A7E94F5BD1FE3C66C</merchantReferenceCode>
  <item id="0">
    <unitPrice>49.95</unitPrice>
    <quantity>1</quantity>
  </item>
  <purchaseTotals>
    <currency>USD</currency>
  </purchaseTotals>
  <ccCaptureService run="true">
    <authRequestID>0305782650000167905080</authRequestID>
  </ccCaptureService>
</requestMessage>

```

Example 12 Credit Card Capture Reply

```
<c:replyMessage xmlns:c="urn:schemas-cybersource-com:transaction-data-1.37">
  <c:merchantReferenceCode>482046C3A7E94F5BD1FE3C66C</c:merchantReferenceCode>
  <c:requestID>1019827520348290570293</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccCaptureReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>49.95</c:amount>
    <c:reconciliationID>1094820975023470</c:reconciliationID>
  </c:ccCaptureReply>
</c:replyMessage>
```

Partial Authorization Examples

Fully Approved Request

The following two examples consist of an authorization request that is fully approved and the subsequent authorization reply, which includes balance information:

- Original request amount: 1500.00 USD
- Approved amount: 1500.00 USD
- Balance amount: 23.62 USD positive

Example 13 Fully Approved Authorization Request

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.52">
  <merchantID>OkGo</merchantID>
  <merchantReferenceCode>AB1234.1-1</merchantReferenceCode>
  <billTo>
    <firstName>John</firstName>
    <lastName>Smith</lastName>
    <street1>201 S. Division St.</street1>
    <street2>Suite 500</street2>
    <city>Ann Arbor</city>
    <state>MI</state>
    <postalCode>48104-2201</postalCode>
    <country>US</country>
    <phoneNumber>123-456-7890</phoneNumber>
    <email>okgo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>1500.00</grandTotalAmount>
  </purchaseTotals>
  <card>
    <accountNumber>4111111111111111</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2015</expirationYear>
    <cvNumber>xxx</cvNumber>
    <cardType>001</cardType>
  </card>
  <ccAuthService run="true"/>
</requestMessage>
```

Example 14 Fully Approved Authorization Reply

```
<c:replyMessage xmlns:c="urn:schemas-cybersource-com:transaction-data-1.52">
  <c:merchantReferenceCode>AB1234.1-1</c:merchantReferenceCode>
  <c:requestID>2688497722340000852964</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:purchaseTotals><c:currency>USD</c:currency></c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>1500.00</c:amount>
    <c:authorizationCode>831000</c:authorizationCode>
    <c:avsCode>A</c:avsCode>
    <c:avsCodeRaw>A</c:avsCodeRaw>
    <c:cvCode>3</c:cvCode>
    <c:processorResponse>000</c:processorResponse>
    <c:merchantAdviceCode>00</c:merchantAdviceCode>
    <c:accountBalance>23.62</c:accountBalance>
    <c:cardCategory>J1</c:cardCategory>
    <c:accountBalanceCurrency>USD</c:accountBalanceCurrency>
    <c:accountBalanceSign>positive</c:accountBalanceSign>
  </c:ccAuthReply>
</c:replyMessage>
```

Partially Approved Request

The following two examples consist of an authorization request that is partially approved and the subsequent authorization reply:

- Original request amount: 1401.00 USD
- Approved amount: 500.00 USD

Example 15 Partially Approved Authorization Request

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.52">
  <merchantID>OkGo</merchantID>
  <merchantReferenceCode>AB1234.1-1</merchantReferenceCode>
  <billTo>
    <firstName>John</firstName>
    <lastName>Smith</lastName>
    <street1>201 S. Division St.</street1>
    <street2>Suite 500</street2>
    <city>Ann Arbor</city>
    <state>MI</state>
    <postalCode>48104-2201</postalCode>
    <country>US</country>
    <phoneNumber>123-456-7890</phoneNumber>
    <email>okgo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>1401.00</grandTotalAmount>
  </purchaseTotals>
  <card>
    <accountNumber>4111111111111111</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2015</expirationYear>
    <cvNumber>xxx</cvNumber>
    <cardType>001</cardType>
  </card>
  <ccAuthService run="true"/>
</requestMessage>
```

Example 16 Partially Approved Authorization Reply

```
<c:replyMessage xmlns:c="urn:schemas-cybersource-com:transaction-data-1.52">
  <c:merchantReferenceCode>AB1234.1-1</c:merchantReferenceCode>
  <c:requestID>2688497722340000852964</c:requestID>
  <c:decision>REJECT</c:decision>
  <c:reasonCode>110</c:reasonCode>
  <c:purchaseTotals><c:currency>USD</c:currency></c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>110</c:reasonCode>
    <c:amount>500.00</c:amount>
    <c:authorizationCode>831000</c:authorizationCode>
    <c:avsCode>A</c:avsCode>
    <c:avsCodeRaw>A</c:avsCodeRaw>
    <c:cvCode>3</c:cvCode>
    <c:processorResponse>010</c:processorResponse>
    <c:merchantAdviceCode>00</c:merchantAdviceCode>
    <c:cardCategory>J1</c:cardCategory>
    <c:requestAmount>1401.00</c:requestAmount>
    <c:requestCurrency>USD</c:requestCurrency>
  </c:ccAuthReply>
</c:replyMessage>
```

American Express SafeKey Response Codes

The American Express SafeKey response code is returned in **ccAuthReply_cavvResponseCode** in the reply message for an authorization request. See "[American Express SafeKey](#)," page 100, for a description of American Express SafeKey.

Table 45 American Express SafeKey Response Codes

Response Code	Description
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
U	Issuer does not participate or 3-D secure data was not used.
99	An unknown value was returned from the processor.

AVS Codes

The AVS code is returned in **ccAuthReply_avsCode** in the authorization reply message. See ["Address Verification System \(AVS\)," page 44](#), for a description of AVS.

Table 46 Types of AVS Codes

Type of Codes	Codes	Description
Codes for American Express Cards	F, H, K, L, O, T, V	Note For American Express cards only. For American Express cards, you can receive Visa and CyberSource AVS codes in addition to the American Express AVS codes.
International Visa Codes	B, C, D, G, I, M, P	<p>The international and domestic alphabetic AVS codes are the Visa standard AVS codes. CyberSource maps the standard AVS return codes for other types of credit cards, including American Express cards, to the Visa standard AVS codes.</p> <p>AVS is considered either domestic or international, depending on the location of the bank that issued the customer's credit card:</p> <ul style="list-style-type: none"> ■ When the bank is in the U.S., the AVS is domestic. ■ When the bank is outside the U.S., the AVS is international. <p>You should be prepared to handle both domestic and international AVS result codes:</p> <ul style="list-style-type: none"> ■ For international cards, you can receive domestic AVS codes in addition to the international AVS codes. ■ For domestic cards, you can receive international AVS codes in addition to the domestic AVS codes.
Domestic Visa Codes	A, E, N, R, S, U, W, X, Y, Z	
CyberSource Codes	1, 2	The numeric AVS codes are created by CyberSource and are not standard Visa codes. These AVS codes can be returned for any card type.

Table 47 AVS Codes

Code	Description
A	Partial match: street address matches, but 5-digit and 9-digit postal codes do not match.
B	Partial match: street address matches, but postal code is not verified. Returned only for Visa cards not issued in the U.S.
C	No match: street address and postal code do not match. Returned only for Visa cards not issued in the U.S.
D & M	Match: street address and postal code match. Returned only for Visa cards not issued in the U.S.
E	Invalid: AVS data is invalid or AVS is not allowed for this card type.
F	Partial match: card member's name does not match, but billing postal code matches.
G	Not supported: issuing bank outside the U.S. does not support AVS.
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. Returned only for Visa cards not issued in the U.S.
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	See the entry for D & M.
N	No match: one of the following: <ul style="list-style-type: none"> ■ 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 not verified. Returned only for Visa cards not issued in the U.S.
R	System unavailable.
S	Not supported: issuing bank in the U.S. 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: <ul style="list-style-type: none"> ■ The U.S. bank does not support AVS outside the U.S. ■ 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.
W	Partial match: street address does not match, but 9-digit postal code matches.
X	Match: street address and 9-digit postal code match.
Y	Match: street address and 5-digit postal code match.

Table 47 AVS Codes (Continued)

Code	Description
Z	Partial match: street address does not match, but 5-digit postal code matches.
1	Not supported: one of the following: <ul style="list-style-type: none"> ■ AVS is not supported for this processor or card type. ■ AVS is disabled for your CyberSource account. To enable AVS, contact CyberSource Customer Support.
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.
5	No match: no AVS code was returned by the processor.

Commerce Indicators

The commerce indicator is a request value that you send in the **ccAuthService_commerceIndicator** and **ccCreditService_commerceIndicator** fields.

Table 48 Commerce Indicators

Values	Description
aesk and aesk_attempted	See "American Express SafeKey," page 100.
install and install_internet	See "Installment Payments," page 73.
internet (default)	Note E-commerce order placed using a web site.
js and js_attempted	See "JCB J/Secure," page 97.
moto	Note Mail order or telephone order.
recurring and recurring_internet	See "Recurring Payments," page 105. <ul style="list-style-type: none"> ■ recurring—U.S. transaction or non-U.S. mail order / telephone order (MOTO) transaction ■ recurring_internet—non-U.S. e-commerce (internet) transaction
retail	See Card-Present Transactions Supplement.
spa and spa_failure	See "Mastercard SecureCode," page 98.
vbv, vbv_attempted, and vbv_failure	See "Verified by Visa," page 95.

CVN Codes

The CVN code is returned in **ccAuthReply_cvCode** in the authorization reply message. See "[Card Verification Numbers \(CVNs\)](#)," page 50, for a description of CVN.

Table 49 CVN Codes

Code	Description
D	The transaction was determined to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation check.
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 payment card company.
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.

Electronic Verification Response Codes

See "[Electronic Verification \(EV\)](#)," page 47, for a list of the fields in which the Electronic Verification response codes are returned. The following table describes the mapped response codes.

Table 50 Electronic Verification Mapped Response Codes

Response Code	Description
F	First name matches; last name does not match.
L	Last name matches; first name does not match.
M	First name and last name match.
N	No, the data does not match.
P	The processor did not return verification information.
R	The system is unavailable, so retry.
S	The verification service is not available.
U	Verification information is not available.
Y	Yes, the data matches.
1	Electronic verification did not generate a response.
2	The processor returned an unrecognized value.

Frequently Asked Questions

What kind of bank account do I need to accept credit card payments?

You need a merchant bank account that is configured to process card-not-present or mail order/telephone order (MOTO) transactions. See "[Acquiring \(Merchant\) Banks](#)," page 16.

What types of credit cards can my customers use?

CyberSource can accept payments made with numerous types of credit cards, including Visa, Mastercard, Discover, and American Express. In addition, CyberSource can accept most offline debit cards, which are also known as check cards, many private label cards, and Level II purchasing cards. Your payment processor can limit the types of cards that you can accept. See "[Payment Processors](#)," page 19, or contact your CyberSource account representative.

Do I need to sign agreements with the payment card companies?

Some credit card companies, such as American Express and Discover, require you to sign agreements with them. For other card types, such as Visa and Mastercard, you can usually sign a single contract with your acquiring bank or payment processor. Your acquiring bank can help ensure that you sign all of the necessary agreements.

Can I use more than one payment processor or merchant account provider?

Yes. CyberSource can provide you with multiple CyberSource merchant IDs and configure each one to use a different payment processor or merchant account provider.

What happens when my customers commit fraud?

You could be liable for fraudulent transactions. When customers complain that you charged their accounts improperly, you might be required to return their money at your expense; this is known as a chargeback. If you receive a large number of chargebacks, or if a large number of your customers commit fraud, your acquiring bank might raise your fees or revoke your merchant bank account. Contact your CyberSource account representative for information about CyberSource products that can help prevent fraud.

When do authorizations expire?

Most authorizations expire within five to seven days, but the bank or company that issued the card decides how long an authorization lasts.

When an authorization expires, will I be able to charge my customer?

Yes. CyberSource is not notified when an authorization expires, so it is possible to capture an expired authorization. However, the capture might be downgraded, which would increase your fees for the transaction. Additionally, the payment card company can decide not to capture expired authorizations.

If you believe that an authorization expired, you can request a new authorization, then capture the new authorization. However, the new authorization could be denied if the customer's credit limit has been exceeded, if the card has expired, or if the card has been cancelled.

Can I reverse an authorization?

Yes. Some processors allow you to reverse an authorization, which releases the hold that the authorization placed on the customer's credit card funds. For the list of processors that allow you to reverse an authorization, see "[Reversing an Authorization](#)," page 25.

If your processor does not support authorization reversals and you need to reverse an authorization, contact the customer's issuing bank or wait for the authorization to expire.

Can I cancel a capture or credit?

Yes. For some processors, you can use the void service to cancel a capture or credit that you have previously requested. You must request the void before CyberSource submits the capture or credit request to your payment processor. See "[Voiding a Capture or Credit](#)," page 41.

How can I prevent my customers from clicking the "Buy" button more than once?

Use one or more of these options:

- After a customer clicks the "Buy" button, send the customer to a new web page
- After a customer clicks the "Buy" button, hide or disable the button

The Support Center provides sample JavaScript code to disable the "Buy" button after a customer clicks it. The code is available at:

http://www.cybersource.com/support_center/implementation/best_practices/view.xml?page_id=415

Can I change the company name and phone number that appears on my customers' credit card statements?

CyberSource permits you to change these values, which are called merchant descriptors, when you use a payment processor that supports this feature. After your processor configures the merchant descriptors for your account, you can choose which merchant descriptor to use every time you request a transaction. You must also contact CyberSource and your processor to specify default merchant descriptors for your account. See "[Merchant Descriptors](#)," page 76.

When do my capture and credit transactions appear on my CyberSource reports?

Capture and credit transactions usually appear on your reports two calendar days after you request them. However, it might take longer for funds to be transferred.

When are funds transferred between my customer's bank account and my company's bank account?

Funds are usually transferred within two to three days after you request a capture or credit.

Network Transaction Identifiers

The network transaction identifier is returned in **ccAuthReply_paymentNetworkTransactionID** in the authorization reply message.

GPN

For GPN, the following values are returned for each card type:

- American Express: The payment card company generates this value. CyberSource saves this value and sends it to the processor in all subsequent capture requests.
- Discover: The payment card company generates this value. CyberSource saves this value and sends it to the processor in all subsequent requests for full authorization reversals and captures.
- Mastercard: The payment card company generates this value. CyberSource saves it and sends it to the processor in all subsequent requests for full authorization reversals and captures. Format:
 - Bits 1-9: Banknet reference number generated by Mastercard for each transaction
 - Bits 10-13: Banknet date
 - Bits 14-15: Spaces
- Visa: The payment card company generates this value. CyberSource saves it and sends it to the processor in all subsequent requests for full authorization reversals and captures.
- Other Card Types: Not used.

Product Codes

The following table lists the values you can use for the product code in the `item_#_productCode` request field.

Table 51 Product Codes

Product Code	Definition
<code>adult_content</code>	Adult content.
<code>coupon</code>	Coupon applied to the entire order.
<code>default</code>	Default value for the product code. CyberSource uses <code>default</code> when a request message does not include a value for the product code.
<code>electronic_good</code>	Electronic product other than software.
<code>electronic_software</code>	Software distributed electronically rather than on disks or other media.
<code>gift_certificate</code>	Gift certificate.
<code>handling_only</code>	Fee that you charge your customer to cover your administrative selling costs.
<code>service</code>	Service that you perform for your customer.
<code>shipping_and_handling</code>	The shipping portion is the charge for shipping the product to your customer. The handling portion is the fee you charge your customer to cover your administrative selling costs.
<code>shipping_only</code>	Charge for transporting tangible personal property from your location to your customer. You must maintain documentation that clearly establishes the location where the title to the property passed from you to your customer.
<code>subscription</code>	Subscription to a web site or other content.

Product IDs

The Visa or Mastercard product ID is returned in **ccAuthReply_cardCategory** in the authorization reply message.

Visa Product IDs



Note

You will probably not receive all the codes in the following table.

In the following table, the carat character (^) indicates a space.

Table 52 Visa Product IDs

Value	Description	Value	Description
A^	Visa Traditional	L^	Electron
AX	American Express	M^	Mastercard/Eurocard and Diners
B^	Visa Traditional Rewards	N^	Visa Platinum
C^	Visa Signature	N1	Visa Rewards
D^	Visa Signature Preferred	N2	Visa Select
DI	Discover	P^	Visa Gold
DN	Diners Club International	Q^	Private Label
E^	Reserved	Q1	Private Label Prepaid
F^	Visa Classic	Q2	Private Label Basic
G^	Visa Business	Q3	Private Label Standard
G1	Visa Signature Business	Q4	Private Label Enhanced
G2	Visa Business Check Card	Q5	Private Label Specialized
G3	Visa Business Enhanced	Q6	Private Label Premium
G4	Visa Infinite Business	R^	Proprietary
H^	Visa Check Card	S^	Visa Purchasing
I^	Visa Infinite	S1	Visa Purchasing with Fleet

Table 52 Visa Product IDs (Continued)

Value	Description	Value	Description
I1	Visa Infinite Privilege	S2	Visa GSA Purchasing
I2	Visa Ultra High Net Worth	S3	Visa GSA Purchasing with Fleet
J^	Reserved	S4	Government Services Loan
J1	Visa General Prepaid	S5	Commercial Transport EBT
J2	Visa Prepaid Gift	S6	Business Loan
J3	Visa Prepaid Healthcare	T^	Reserved/Interlink
J4	Visa Prepaid Commercial	U^	Visa TravelMoney
JC	JCB	V^	V Pay
K^	Visa Corporate T&E	W^ – Z^	Reserved
K1	Visa GSA Corporate T&E	0^ – 9^	Reserved

Mastercard Product IDs



Note

Mastercard can introduce new values for this field without advance notice. See the Mastercard technical documentation for additional information.

Table 53 Mastercard Product IDs

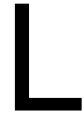
Value	Description	Value	Description
CBL	Carte Blanche	MNF	Mastercard Public Sector Commercial Card
DAG	Gold Debit Mastercard Salary	MOC	Standard Maestro Social
DAP	Platinum Debit Mastercard Salary	MPA	Prepaid Mastercard Payroll Card
DAS	Standard Debit Mastercard Salary	MPB	Mastercard Preferred BusinessCard
DCC	Diners Club	MPC	Mastercard Professional Card
DOS	Standard Debit Mastercard Social	MPF	Prepaid Mastercard Gift Card
JCB	Japanese Credit Bureau	MPG	Prepaid Mastercard Consumer Reloadable Card
MAB	World Elite Mastercard for Business	MPJ	Prepaid Debit Mastercard Card Gold
MAC	Mastercard Corporate World Elite	MPK	Prepaid Mastercard Government Commercial Card
MAP	Mastercard Commercial Payments Account product	MPL	Platinum Mastercard Card
MAQ	Mastercard Prepaid Commercial Payments Account	MPM	Prepaid Mastercard Consumer Promotion Card

Table 53 Mastercard Product IDs (Continued)

Value	Description	Value	Description
MAV	Mastercard Activation Verification	MPN	Prepaid Mastercard Insurance Card
MBB	Mastercard Prepaid Consumer	MPO	Prepaid Mastercard Other Card
MBC	Mastercard Prepaid Voucher	MPR	Prepaid Mastercard Travel Card
MBD	Deferred Debit Mastercard BusinessCard Card	MPT	Prepaid Mastercard Teen Card
MBE	Mastercard Electronic Business Card	MPV	Prepaid Mastercard Government Benefit Card
MBP	Mastercard Corporate Prepaid	MPW	Prepaid Mastercard Corporate Card
MBT	Mastercard Corporate Prepaid Travel	MPX	Prepaid Mastercard Flex Benefit Card
MCB	Mastercard BusinessCard Card/ Mastercard Corporate Card	MPY	Prepaid Mastercard Employee Incentive Card
MCC	Mastercard Card	MPZ	Prepaid Mastercard Emergency Assistance Card
MCE	Mastercard Electronic Card	MRB	Prepaid Mastercard Electronic BusinessCard
MCF	Mastercard Electronic Fleet Card	MRC	Prepaid Mastercard Electronic Card
MCG	Gold Mastercard Card	MRG	Prepaid Mastercard Card Outside U.S.
MCM	Mastercard Corporate Meeting Card	MRH	Mastercard Platinum Prepaid Travel Card
MCO	Mastercard Corporate	MRJ	Prepaid Mastercard Gold Card
MCP	Mastercard Corporate Purchasing Card	MRK	Prepaid Mastercard Electronic Commercial
MCS	Mastercard Standard Card	MRL	Prepaid Mastercard Electronic Commercial
MCW	World Mastercard Card	MRS	Prepaid Mastercard ISIC Student Card
MCX	Mastercard Card (international use)	MRW	Prepaid Mastercard BusinessCard Credit Outside U.S.
MDB	Debit Mastercard BusinessCard Card	MSI	Maestro point-of-sale debit program
MDG	Debit Gold Mastercard	MTP	Mastercard Platinum Prepaid Travel Card
MDL	Business Debit Other Embossed	MUS	Prepaid Mastercard Unembossed U.S.
MDM	Middle Market Fleet Card	MWB	World Mastercard for Business
MDN	Middle Market Purchasing Card	MWE	Mastercard World Elite
MDO	Debit Mastercard Other	MWO	Mastercard Corporate World
MDP	Debit Mastercard Platinum	PRO	Proprietary Card

Table 53 Mastercard Product IDs (Continued)

Value	Description	Value	Description
MDQ	Middle Market Corporate Card	PVL	Private label card
MDS	Debit Mastercard	SAG	Gold Mastercard Salary-Immediate Debit
MDT	Mastercard Business Debit	SAL	Standard Maestro Salary
MDW	Mastercard Black Debit/World Elite Debit Mastercard	SAP	Platinum Mastercard Salary-Immediate Debit
MEB	Mastercard Executive BusinessCard Card	SAS	Standard Mastercard Salary-Immediate Debit
MEC	Mastercard Electronic Commercial	SOS	Standard Mastercard Social-Immediate Debit
MEF	Mastercard Electronic Payment Account	SUR	Prepaid Mastercard Unembossed Outside U.S.
MEO	Mastercard Corporate Executive Card	TBE	Business-Immediate Debit
MET	Titanium Debit Mastercard	TCB	Mastercard Business Card-Immediate Debit
MGF	Mastercard Government Commercial Card	TCF	Mastercard Fleet Card-Immediate Debit
MHA	Mastercard Healthcare Prepaid Non-tax	TCO	Mastercard Corporate-Immediate Debit
MHB	Mastercard HSA Substantiated	TCP	Mastercard Purchasing Card-Immediate Debit
MHC	Mastercard Healthcare Credit Non-substantiated	TDN	Middle Market Mastercard Purchasing Card-Immediate Debit
MHH	Mastercard HSA Non-substantiated	TEB	Mastercard Executive BusinessCard Card-Immediate Debit
MIA	Mastercard Unembossed Prepaid Student Card	TEC	Mastercard Electronic Commercial-Immediate Debit
MIK	Mastercard Electronic Consumer Prepaid Non U.S. Student Card	TEO	Mastercard Corporate Executive Card-Immediate Debit
MIL	Mastercard Unembossed Prepaid Non U.S. Student Card	TLA	Mastercard Central Travel Solutions Air-Immediate Debit
MIP	Mastercard Debit Prepaid Student Card	TNF	Mastercard Public Sector Commercial Card-Immediate Debit
MLA	Mastercard Central Travel Solutions Air	TPB	Mastercard Preferred Business Card-Immediate Debit
MLC	Mastercard Micro-Business Card	TPC	Mastercard Professional Card-Immediate Debit
MLD	Mastercard Distribution Card	WDR	World Debit Mastercard Rewards
MLL	Mastercard Central Travel Solutions Land	WMR	World Mastercard Rewards



Reason Codes

The following table describes the reason codes returned by the Simple Order API for the credit card services. For a description of replies, decisions, and reason codes, see the information about handling replies in [Getting Started with CyberSource Essentials](#).



Because CyberSource can add reply fields and reason codes at any time:

- You must parse the reply data according to the names of the fields instead of the field order in the reply. For more information about parsing reply fields, see the documentation for your client.
- Your error handler should be able to process new reason codes without problems.
- Your error handler should use the **decision** field to determine the result if it receives a reason code that it does not recognize.

Table 54 Reason Codes

Reason Code	Description
100	Successful transaction.
101	The request is missing one or more required fields. Possible action: see the reply fields missingField_0 through missingField_N for which fields are missing. Resend the request with the complete information. For information about missing or invalid fields, see Getting Started with CyberSource Essentials .
102	One or more fields in the request contains invalid data. Possible action: see the reply fields invalidField_0 through invalidField_N for which fields are invalid. Resend the request with the correct information. For information about missing or invalid fields, see Getting Started with CyberSource Essentials .
104	The merchant reference code for this authorization request matches the merchant reference code of another authorization request that you sent within the past 15 minutes. Possible action: Resend the request with a unique merchant reference code.
110	Only a partial amount was approved. Possible action: see "Partial Authorizations," page 55 .

Table 54 Reason Codes (Continued)

Reason Code	Description
150	<p>General system failure.</p> <p>See the documentation for your CyberSource client for information about handling retries in the case of system errors.</p>
151	<p>The request was received but there was a server timeout. This error does not include timeouts between the client and the server.</p> <p>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center. See the documentation for your CyberSource client for information about handling retries in the case of system errors.</p>
152	<p>The request was received, but a service did not finish running in time.</p> <p>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center. See the documentation for your CyberSource client for information about handling retries in the case of system errors.</p>
200	<p>The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the Address Verification System (AVS) check.</p> <p>Possible action: You can capture the authorization, but consider reviewing the order for the possibility of fraud.</p>
201	<p>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.</p> <p>Possible action: Call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.</p>
202	<p>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.</p> <p>Possible action: Request a different card or other form of payment.</p>
203	<p>General decline of the card. No other information was provided by the issuing bank.</p> <p>Possible action: Request a different card or other form of payment.</p>
204	<p>Insufficient funds in the account.</p> <p>Possible action: Request a different card or other form of payment.</p>
205	<p>Stolen or lost card.</p> <p>Possible action: Review this transaction manually to ensure that you submitted the correct information.</p>
207	<p>Issuing bank unavailable.</p> <p>Possible action: Wait a few minutes and resend the request.</p>
208	<p>Inactive card or card not authorized for card-not-present transactions.</p> <p>Possible action: Request a different card or other form of payment.</p>

Table 54 Reason Codes (Continued)

Reason Code	Description
209	CVN did not match. 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.
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.
235	The requested capture amount exceeds the originally authorized amount. Possible action: Issue a new authorization and capture request for the new amount.
236	Processor failure. Possible action: Wait a few minutes and resend the request.
237	The authorization has already been reversed. Possible action: No action required.
238	The authorization has already been captured. Possible action: No action required.
239	The requested transaction amount must match the previous transaction amount. Possible action: Correct the amount and resend the request.
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.

Table 54 Reason Codes (Continued)

Reason Code	Description
241	<p>The request ID is invalid.</p> <p>Possible action: Request a new authorization, and if successful, proceed with the capture.</p>
242	<p>You requested a capture, but there is no corresponding, unused authorization record. Occurs if there was not a previously successful authorization request or if the previously successful authorization has already been used by another capture request.</p> <p>Possible action: Request a new authorization, and if successful, proceed with the capture.</p>
243	<p>The transaction has already been settled or reversed.</p> <p>Possible action: No action required.</p>
246	<p>One of the following:</p> <ul style="list-style-type: none"> ■ The capture or credit is not voidable because the capture or credit information has already been submitted to your processor. <p>- or -</p> <ul style="list-style-type: none"> ■ You requested a void for a type of transaction that cannot be voided. <p>Possible action: No action required.</p>
247	<p>You requested a credit for a capture that was previously voided.</p> <p>Possible action: No action required.</p>
250	<p>The request was received, but there was a timeout at the payment processor.</p> <p>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center.</p>
254	<p>Stand-alone credits are not allowed.</p> <p>Possible action: Submit a follow-on credit by including a request ID in the credit request. A follow-on credit must be requested within 60 days of the authorization. To process stand-alone credits, contact your CyberSource account representative to find out if your processor supports stand-alone credits.</p>
520	<p>The authorization request was approved by the issuing bank but declined by CyberSource based on your Smart Authorization settings.</p> <p>Possible action: Do not capture the authorization without further review. Review the ccAuthReply_avsCode, ccAuthReply_cvCode, and ccAuthReply_authFactorCode fields to discover why CyberSource rejected the request.</p> <p>For information about Smart Authorization, see the Business Center User Guide.</p>

Smart Authorization Factor Codes

The Smart Authorization factor code is returned in **ccAuthReply_authFactorCode** in the reply message for an authorization request. For information about Smart Authorization, see the [Business Center User Guide](#).

Table 55 Smart Authorization Factor Codes

Code	Description
J	Billing and shipping address do not match.
M	Cost of the order exceeds the maximum transaction amount.
N	Nonsensical input in the customer name or address fields.
O	Obscenities in the order form.
U	Unverifiable billing or shipping address.
X	Order does not comply with the USA PATRIOT Act.

Verified by Visa Response Codes

The Verified by Visa response code is returned in **ccAuthReply_cavvResponseCode** in the reply message for an authorization request. See ["Verified by Visa," page 95](#), for a description of Verified by Visa.

Table 56 Verified by Visa Response Codes

Response Code	Description
0	CAVV not validated because erroneous data was submitted.
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
6	CAVV not validated because the issuer does not participate.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
B	CAVV passed the validation with information only; no liability shift.
C	CAVV attempted but not validated; issuer did not return CAVV code.
D	CAVV not validated or authenticated; issuer did not return CAVV code.
I	Invalid security data.
U	Issuer does not participate or 3-D secure data was not used.
99	An unknown value was returned from the processor.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- AAV [98](#)
- account authentication values [98](#)
- account balances [60](#)
- acquirers [19](#)
- acquiring banks [16](#)
- Address Verification System
 - codes [172](#)
 - described [44](#)
 - and recurring payments [107](#)
 - relaxed requirements [45](#)
- aggregator [63](#)
- aggregator support [63](#)
- American Express SafeKey
 - described [95](#)
 - response codes [171](#)
- ARAV [28](#)
- authorization reversals
 - after void (ARAV) [28](#)
 - alternate methods [179](#)
 - full [25](#)
 - partial [33](#)
- authorizations
 - described [21](#)
 - examples, name-value pairs [159](#)
 - examples, XML [164](#)
 - expiration of [179](#)
 - for zero amounts [112](#)
 - partial [55](#)
 - verbal [52](#)
 - See also* ccAuthService
- automatic authorization reversals [33](#)
- automatic interchange optimization [34](#)
- AVS
 - codes [172](#)
 - described [44](#)
 - and recurring payments [107](#)
 - relaxed requirements [45](#)
- AVS only [112](#)

B

- balance responses [60](#)
- Bill Payment program (Visa) [110](#)
- business cards [75](#)

C

- captures
 - after void [42](#)
 - described [29](#)
 - examples, name-value pairs [159](#)
 - examples, XML [164](#)
 - multiple [35](#)
 - partial [35](#)
 - See also* ccCaptureService
- card associations [17](#)
- card identification digits. *See* CVNs
- card type indicators [67](#)
- card validation codes. *See* CVNs
- card verification numbers. *See* CVNs
- cardholder authentication verification values
 - API fields [125](#)
 - for American Express SafeKey [101](#)
 - for JCB J/Secure [96](#)
 - for Verified by Visa [96](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- card-not-present transactions [15](#)
- card-present data [67](#)
- card-present transactions [15](#)
- CAVV
 - API fields [125](#)
 - for American Express SafeKey [101](#)
 - for JCB J/Secure [96](#)
 - for Verified by Visa [96](#)
- ccAuthReversalService
 - described [25](#)
 - requesting [27](#)
 - required fields [28](#)
- ccAuthService
 - described [21](#)
 - requesting [23](#)
 - required fields [23](#)
- ccCaptureService
 - described [29](#)
 - requesting [31](#)
 - required fields [31](#)
- ccCreditService
 - described [38](#)
 - requesting [39](#)
 - required fields [39](#)
- characters, special [117](#)
- chargebacks
 - described [17](#)
 - fees [16](#)
- Chase Paymentech Solutions
 - ARAV [28](#)
 - authorizations [21](#)
 - automatic authorization reversals [33](#)
 - AVS [44](#)
 - balance responses [60](#)
 - captures [29](#)
 - card type indicators (CTIs) [67](#)
 - card types [20](#)
 - credits [38](#)
 - CVNs [50](#)
 - final authorization indicator [68](#)
 - forced captures [72](#)
 - full authorization reversals [26](#)
 - installment payments [73](#)
 - Mastercard SecureCode [98](#)
 - merchant descriptors [76](#)
 - merchant-initiated reversals [93](#)
 - multiple partial captures [35](#)
 - partial authorizations [55](#)
 - recurring payments [105](#)
 - relaxed requirements [45](#)
 - verbal authorizations [52](#)
 - Verified by Visa [95](#)
 - Visa Bill Payments [110](#)
 - voids [41](#)
 - zero amount authorizations [112](#)
- CID. See CVNs
- commerce indicators
 - API fields [125](#)
 - for American Express SafeKey [101](#)
 - for JCB J/Secure [96](#)
 - for Mastercard SecureCode [99](#)
 - for Verified by Visa [96](#)
 - values [175](#)
- consumer banks [17](#)
- corporate cards [75](#)
- credit card associations [17](#)
- credit card numbers for testing [115](#)
- credits
 - described [38](#)
 - See *also* ccCreditService

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- CTIs [67](#)
- customer profiles [102](#)
- CVC2. See CVNs
- CVNs
 - and recurring payments [105](#)
 - codes [176](#)
 - described [50](#)
- CVV2. See CVNs

- D**
- data types [117](#)
- date and time formats [149](#)
- debit cards [55](#)
- Debt Repayment program (Visa) [111](#)
- descriptors [76](#)

- E**
- ECI
 - API fields [125](#)
 - for American Express SafeKey [101](#)
 - for JCB J/Secure [96](#)
 - for Mastercard SecureCode [99](#)
 - for Verified by Visa [96](#)
 - values [175](#)
- electronic commerce indicators
 - API fields [125](#)
 - for American Express SafeKey [101](#)
 - for JCB J/Secure [96](#)
 - for Mastercard SecureCode [99](#)
 - for Verified by Visa [96](#)
 - values [175](#)
- Electronic Verification
 - described [47](#)
 - response codes [177](#)
- errors
 - reason codes [187](#)
 - simulating during testing [115](#)
- EV
 - described [47](#)
 - response codes [177](#)
- example code [159](#)
- expiration dates
 - for recurring payments [105](#)
 - relaxed requirements [45](#)
- expiration of authorizations [179](#)

- F**
- factor codes for Smart Authorization [191](#)
- FAQ [178](#)
- FDC Compass
 - aggregators [64](#)
 - ARAV [28](#)
 - authorizations [21](#)
 - automatic authorization reversals [33](#)
 - AVS [44](#)
 - balance responses [60](#)
 - captures [29](#)
 - card types [20](#)
 - credits [38](#)
 - CVNs [50](#)
 - final authorization indicator [68](#)
 - full authorization reversals [26](#)
 - installment payments [73](#)
 - Mastercard SecureCode [98](#)
 - merchant descriptors [81](#)
 - multiple partial captures [35](#)
 - partial authorizations [55](#)
 - recurring payments [105](#)
 - relaxed requirements [45](#)
 - verbal authorizations [52](#)
 - Verified by Visa [95](#)
 - Visa Bill Payments [110](#)
 - voids [41](#)
 - zero amount authorizations [112](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

FDC Nashville Global

aggregators **66**
 American Express SafeKey **100**
 ARAV **28**
 authorizations **21**
 automatic authorization reversals **33**
 AVS **44**
 balance responses **61**
 captures **29**
 card types **20**
 credits **38**
 CVNs **50**
 Electronic Verification **47**
 final authorization indicator **68**
 forced captures **72**
 full authorization reversals **26**
 installment payments **73**
 Mastercard SecureCode **98**
 merchant descriptors **84**
 merchant-initiated reversals **93**
 multiple partial captures **35**
 partial authorizations **55**
 recurring payments **105**
 relaxed requirements **45**
 verbal authorizations **52**
 Verified by Visa **95**
 Visa Bill Payments **110**
 Visa Debt Repayments **111**
 voids **41**
 zero amount authorizations **112**

FDMS Nashville

ARAV **28**
 authorizations **21**
 automatic authorization reversals **33**
 AVS **44**
 balance responses **61**
 captures **29**
 card types **20**
 credits **38**
 CVNs **50**
 final authorization indicator **68**
 forced captures **72**
 full authorization reversals **26**
 installment payments **73**
 Mastercard SecureCode **98**
 multiple partial captures **35**
 partial authorizations **55**
 recurring payments **105**
 verbal authorizations **52**
 Verified by Visa **95**
 Visa Bill Payments **110**
 Visa Debt Repayments **111**
 voids **41**
 zero amount authorizations **112**

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

FDMS South

- ARAV [28](#)
 - authorizations [21](#)
 - automatic authorization reversals [33](#)
 - AVS [45](#)
 - balance responses [61](#)
 - captures [29](#)
 - card types [20](#)
 - credits [38](#)
 - CVNs [50](#)
 - forced captures [72](#)
 - full authorization reversals [27](#)
 - installment payments [73](#)
 - Mastercard SecureCode [98](#)
 - merchant descriptors [89](#)
 - partial authorizations [56](#)
 - recurring payments [105](#)
 - relaxed requirements [45](#)
 - verbal authorizations [52](#)
 - Verified by Visa [95](#)
 - voids [41](#)
 - zero amount authorizations [112](#)
- follow-on credits [38](#)
- forced captures [72](#)
- fraud [178](#)
- full authorization reversals
- described [25](#)
 - See *also* [ccAuthReversalService](#)

G

- GMT [149](#)
- GPN
 - ARAV [29](#)
 - authorizations [21](#)
 - automatic authorization reversals [33](#)
 - AVS [45](#)
 - balance responses [61](#)
 - captures [29](#)
 - card types [20](#)
 - credits [38](#)
 - CVNs [50](#)
 - final authorization indicator [68](#)
 - forced captures [72](#)
 - full authorization reversals [27](#)
 - interchange optimization [34](#)
 - Mastercard SecureCode [98](#)
 - merchant descriptors [90](#)
 - multiple partial captures [35](#)
 - partial authorizations [56](#)
 - product IDs [183](#)
 - quasi-cash [103](#)
 - recurring payments [105](#)
 - relaxed requirements [45](#)
 - verbal authorizations [52](#)
 - Verified by Visa [95](#)
 - Visa Bill Payments [110](#)
 - Visa Debt Repayments [111](#)
 - voids [41](#)
 - zero amount authorizations [112](#)

I

- installment payments [73](#)
- interchange fees [16](#)
- interchange optimization [34](#)
- issuing banks [17](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

J

J/Secure [95](#)
 JCB J/Secure [95](#)

L

Level II [75](#)
 Level III [75](#)

M

Mastercard
 payment card company [17](#)
 SecureCode [95](#)
 merchant banks [16](#)
 merchant descriptors [76](#)
 merchant-initiated reversals [93](#)
 merchant-initiated voids [93](#)
 micropayments [94](#)
 multiple captures [35](#)

N

network transaction identifiers [181](#)

O

open to buy [21](#)
 order tracking [18](#)

P

partial authorization reversals [33](#)
 partial authorizations
 described [55](#)
 examples, name-value pairs [161](#)
 examples, XML [167](#)
 partial captures [35](#)
 payer authentication [95](#)
 payment aggregator [63](#)
 payment card companies [17](#)
 payment network transaction identifiers [181](#)

payment processors [19](#)
 payment tokenization [102](#)
 Paymenttech. See Chase Paymenttech Solutions
 POS transactions [67](#)
 prepaid cards [55](#)
 processors [19](#)
 procurement cards [75](#)
 product codes [182](#)
 product IDs [183](#)
 profiles [102](#)
 purchasing cards [75](#)

Q

quasi-cash [103](#)

R

RBS WorldPay Atlanta
 authorizations [21](#)
 AVS [45](#)
 captures [29](#)
 card types [20](#)
 credits [38](#)
 CVNs [50](#)
 full authorization reversals [27](#)
 Mastercard SecureCode [98](#)
 recurring payments [105](#)
 verbal authorizations [52](#)
 Verified by Visa [95](#)
 voids [41](#)
 zero amount authorizations [113](#)
 reason codes [187](#)
 reconciliation IDs [18](#)
 recurring billing [104](#)
 recurring indicators [105](#)
 recurring payments [105](#)
 recurring profiles [104](#)
 recurring transactions [105](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

refunds
 described [38](#)
 See *also* [ccCreditService](#)

Repayment program (Visa) [111](#)

replacement dates for recurring payments [105](#)

request fields [119](#)

request IDs [18](#)

retail POS transactions [67](#)

reversals, authorization
 alternate methods [179](#)
 full [25](#)
 partial [33](#)

reversals, merchant-initiated [93](#)

reversals, transaction
 described [17](#)
 fees [16](#)

S

SafeKey
 described [95](#)
 response codes [171](#)

sample code [159](#)

secure data [102](#)

secure storage [102](#)

SecureCode [95](#)

settlements. See *captures and credits*

Smart Authorization factor codes [191](#)

soft descriptors [76](#)

special characters [117](#)

split dial/route [72](#)

stand-alone credits [38](#)

subscriptions [104](#)

T

TAA fields [76](#)

testing your system [114](#)

time formats [149](#)

Transaction Advice Addendum fields [76](#)

transaction identifiers
 API field [126](#)
 for American Express SafeKey [101](#)
 for Mastercard SecureCode [100](#)
 for Verified by Visa [97](#)
 JCB J/Secure [97](#)

transaction reversals
 described [17](#)
 fees [16](#)

TSYS Acquiring Solutions
 ARAV [29](#)
 authorizations [21](#)
 automatic authorization reversals [33](#)
 AVS [45](#)
 balance responses [61](#)
 captures [29](#)
 card types [20](#)
 credits [38](#)
 CVNs [50](#)
 Electronic Verification [47](#)
 final authorization indicator [68](#)
 forced captures [72](#)
 full authorization reversals [27](#)
 installment payments [73](#)
 JCB J/Secure [97](#)
 Mastercard SecureCode [98](#)
 merchant descriptors [92](#)
 multiple partial captures [35](#)
 partial authorizations [56](#)
 quasi-cash [103](#)
 recurring payments [105](#)
 verbal authorizations [52](#)
 Verified by Visa [95](#)
 Visa Bill Payments [110](#)
 voids [41](#)
 zero amount authorizations [113](#)

Type II cards [75](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**U**

UCAF

API fields [147](#)for Mastercard SecureCode [99](#)

universal cardholder authentication fields

API fields [147](#)for Mastercard SecureCode [99](#)UTC (in authorization reply) [149](#)**V**verbal authorizations [52](#)

Verified by Visa

described [95](#)response codes [192](#)

Visa

Bill Payment program [110](#)Debt Repayments [111](#)payment card company [17](#)Verified by Visa response codes [192](#)Verified by Visa, described [95](#)

Vital. See TSYS Acquiring Solutions

voids, merchant-initiated [93](#)

voidService

described [41](#)requesting [42](#)required fields [43](#)**X**

XID

API field [126](#)for American Express SafeKey [101](#)for JCB J/Secure [97](#)for Mastercard SecureCode [100](#)for Verified by Visa [97](#)**Z**zero amount authorizations [112](#)