Card-Present Processing
Using the SCMP API

Supplement to Credit Card Services
Using the SCMP API
and
PIN Debit Processing
Using the SCMP API

June 2019

CyberSource
the power of payment
CyberSource Contact Information
For general information about our company, products, and services, go to http://www.cybersource.com.

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

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

Copyright
© 2019 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 Unpublished rights reserved under the copyright laws of the United States.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**  
5

**About This Guide**  
6  
About Audience and Purpose 6  
Conventions 6  
Related Documentation 7  
Customer Support 7

### Chapter 1  Introduction to Card-Present Transactions  
8  
Supported Processors 8  
Prerequisites 9

### Chapter 2  Optional Features  
10  
CyberSource Integration 10  
Dynamic Currency Conversion (DCC) 10  
Europay, Mastercard, Visa (EMV) 11  
  Apple Pay and Google Pay 14  
  EMV Host Validation and Device Certification 14  
  EMV Cards and Cardholder Verification Methods (CVMs) 15  
  EMV Transactions 16  
Payment Network Tokenization 16  
PCI P2P Encryption with Bluefin 17  
  Requirements 17  
  Overview 18  
  Bluefin P2PE Contact Center 18  
  Creating a Request for an Authorization or Stand-Alone Credit That Uses Bluefin PCI P2PE 19  
Relaxed Requirements for Address Data and Expiration Date 19
## Recent Revisions to This Document

<table>
<thead>
<tr>
<th>Release</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>This revision contains only editorial changes and no technical updates.</td>
</tr>
</tbody>
</table>
| December 2018 | CyberSource integrations:  
  - Added new section "CyberSource Integration," page 10.  
  - Added the `terminal_type` request field. See "General Card-Present Request-Level Fields," page 28. |
| October 2018 | Added support for Credit Mutuel-CIC. See "Supported Processors," page 8.  
  FDC Nashville Global: added information about PIN data decryption. See  
  "EMV Cards and Cardholder Verification Methods (CVMs)," page 15. |
| August 2018 | All processors that support online PIN transactions: added support for the following PIN data fields. For field descriptions, see  
  "EMV Request-Level Fields," page 22.  
  - `pin_data_encrypted_pin`  
  - `pin_data_key_serial_number`  
  - `pin_data_pin_block_encoding_format` |
About This Guide

Audience and Purpose

This guide is written for application developers who want to use the CyberSource SCMP API to integrate credit card processing with card-present data into their order management system. Credit Card Services Using the SCMP API provides the basic information about credit card processing with CyberSource. This supplement provides information about additional requirements and options for card-present transactions.

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.

Note

Information in this guide about Europay, Mastercard, and Visa (EMV) applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global.

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.
The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Text Conventions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention</strong></td>
<td><strong>Meaning</strong></td>
</tr>
</tbody>
</table>
| **Bold** | • API field names  
| | • API service names  
| | • Graphical user interface elements that you must act upon |
| **Screen text** | • XML elements  
| | • Code examples  
| | • Values for API fields; for example:  
| | Set the ics_applications field to ics_auth. |

**Related Documentation**

- *Getting Started with CyberSource Advanced for the SCMP API* (PDF | HTML) describes how to get started using the SCMP API.
- *Credit Card Services Using the SCMP API* (PDF | HTML) describes how to integrate CyberSource payment processing services into your business.
- The *CyberSource API Versions page* provides information about the CyberSource API versions.
- *PIN Debit Processing Using the SCMP API* (PDF | HTML) describes how to integrate CyberSource PIN debit services into your business.

Refer to the Support Center for complete CyberSource technical documentation:

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

**Customer Support**

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

http://www.cybersource.com/support
This supplement to *Credit Card Services Using the SCMP API* describes card-present processing with CyberSource.

Information in this guide about Europay, Mastercard, and Visa (EMV) applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global.

### Supported Processors

CyberSource supports card-present credit card transactions for the processors shown in the following table.

**Table 2  Processors that CyberSource Supports for Card-Present Transactions**

<table>
<thead>
<tr>
<th>Processor</th>
<th>EMV</th>
<th>Magnetic Stripe</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express Direct—supports card-present processing only for merchants in the U.S. who are transacting in U.S. dollars.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Chase Paymentech Solutions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credit Mutuel-CIC</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FDC Nashville Global</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FDMS Nashville</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GPN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>JCN Gateway—Visa is the only card type supported on JCN Gateway for card-present transactions.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OmniPay Direct—First Data Merchant Solutions (Europe) only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RBS WorldPay Atlanta</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1 For information about EMV support, see "Europay, Mastercard, Visa (EMV)," page 11.
Prerequisites

Before you start your implementation:

- Contact your acquirer to find out whether you are allowed to process card-present transactions.
- Find out from your acquirer and CyberSource Customer Support whether you must have a separate CyberSource merchant ID for your card-present transactions.
- Contact CyberSource Customer Support to have your account configured to process card-present transactions.
- Make sure that you are familiar with the CyberSource SCMP API for processing e-commerce and mail order/telephone order (MOTO) transactions as described in Credit Card Services Using the SCMP API. Use the fields in this guide in addition to the fields in Credit Card Services Using the SCMP API.

Table 2 Processors that CyberSource Supports for Card-Present Transactions (Continued)

<table>
<thead>
<tr>
<th>Processor</th>
<th>EMV ¹</th>
<th>Magnetic Stripe</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIX</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TSYS Acquiring Solutions</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Worldpay VAP—Worldpay VAP was previously called Litle.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹ For information about EMV support, see "Europay, Mastercard, Visa (EMV)," page 11.
Optional Features

CyberSource Integration

Supported Processors:
- American Express Direct
- Credit Mutuel-CIC
- FDC Nashville Global
- OmniPay Direct
- SIX

CyberSource can provide the client software for your POS terminals. The client software sends the CyberSource service requests, parses the information in the CyberSource service replies, and provides information to your POS system. For details, contact your CyberSource account manager.

Dynamic Currency Conversion (DCC)

For information about dynamic currency conversion, see Credit Card Services Using the SCMP API.
Europay, Mastercard, Visa (EMV)

Information in this guide about EMV applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global.

Services:
- Authorization
- Authorization reversal
- Capture
- Credit
- PIN debit credit—supported only on FDC Nashville Global
- PIN debit purchase—supported only on FDC Nashville Global
- PIN debit reversal—supported only on FDC Nashville Global

Processors:
- American Express Direct
- Chase Paymentech Solutions
- Credit Mutuel-CIC
- FDC Nashville Global
- GPN
- JCN Gateway—Visa card type only
- OmniPay Direct—First Data Merchant Solutions (Europe) only
- SIX
Card Types:

- Contact EMV:

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Supported Card Types for Contact Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Card Type</strong></td>
<td><strong>American Express Direct</strong></td>
</tr>
<tr>
<td>American Express</td>
<td>Yes</td>
</tr>
<tr>
<td>Cartes Bancaires</td>
<td>No</td>
</tr>
<tr>
<td>China UnionPay</td>
<td>No</td>
</tr>
<tr>
<td>Diners Club</td>
<td>No</td>
</tr>
<tr>
<td>Discover</td>
<td>No</td>
</tr>
<tr>
<td>JCB</td>
<td>No</td>
</tr>
<tr>
<td>Maestro (International)</td>
<td>No</td>
</tr>
<tr>
<td>Maestro (UK Domestic)</td>
<td>No</td>
</tr>
<tr>
<td>Mastercard</td>
<td>No</td>
</tr>
<tr>
<td>Visa</td>
<td>No</td>
</tr>
<tr>
<td>Visa Electron</td>
<td>No</td>
</tr>
</tbody>
</table>
Contactless EMV:

Table 4  Supported Card Types for Contactless Transactions

<table>
<thead>
<tr>
<th>Card Type</th>
<th>American Express Direct</th>
<th>Chase Paymentech Solutions</th>
<th>Credit Mutual-CIC</th>
<th>FDC Nashville Global</th>
<th>GPN</th>
<th>JCN Gateway</th>
<th>Omnipay Direct</th>
<th>SIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express ExpressPay</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cartes Bancaires</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>China UnionPay</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Diners Club</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Discover</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>JCB</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mastercard PayPass</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Visa payWave</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

EMV is a global standard for exchanging information between chip cards and POS terminals. A chip card is a credit or debit card with an embedded microchip. A chip card also has a magnetic stripe on the back of the card that can be used for a back-up transaction when the card’s chip cannot be read. The EMV standards define the protocols for all levels of transmission between chip cards and chip card processing devices: physical, electrical, data, and application.
Apple Pay and Google Pay

CyberSource supports contactless EMV for Apple Pay and Google Pay transactions.

Processors:
- FDC Nashville Global
- OmniPay Direct
- SIX

Card Types:

Table 5  Supported Card Types for Contactless Apple Pay and Google Pay Transactions

<table>
<thead>
<tr>
<th>Card Type</th>
<th>FDC Nashville Global</th>
<th>OmniPay Direct</th>
<th>SIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Discover</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mastercard</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Visa</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

EMV Host Validation and Device Certification

As a payment services provider, CyberSource uses a two-step process for host validation and device certification for EMV. Both steps must be completed to have a fully certified EMV solution.

1 Host validation: CyberSource obtained host validation for the following processors:
- American Express Direct
- Chase Paymentech Solutions
- Credit Mutuel-CIC
- FDC Nashville Global
- GPN
- JCN Gateway
- OmniPay Direct—First Data Merchant Solutions (Europe) only
- SIX
Device certification: CyberSource is working on device certification with Credit Mutuel-CIC, FDC Nashville Global, and SIX.

Before you purchase a device for use with EMV, contact your CyberSource representative.

**EMV Cards and Cardholder Verification Methods (CVMs)**

<table>
<thead>
<tr>
<th>Processor</th>
<th>Chip and PIN</th>
<th>Chip and Online PIN</th>
<th>Chip and Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express Direct</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Chase Paymentech Solutions</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Credit Mutuel-CIC</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>FDC Nashville Global</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GPN</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>JCN Gateway</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>OmniPay Direct</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SIX</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Most chip-and-PIN cards allow a cardholder to provide a signature as a back-up option. Other EMV cards are chip-and-signature cards. For these cards, a signature is the preferred CVM, and a PIN can be used as a back-up option.

Chip-and-signature cards are more widespread in the U.S. Chip-and-PIN cards are more widespread outside the U.S.

On FDC Nashville Global, there are two ways to decrypt PIN data:

- With the CyberSource solution, which is the default solution, CyberSource injects the terminal with a fixed key and decrypts the PIN data.
- With the third-party solution, CyberSource sends the encrypted PIN data to a third party who decrypts it and forwards it to the processor on your behalf. To enable third-party PIN data decryption for your CyberSource account, contact CyberSource Customer Support.
EMV Transactions

EMV transactions are more secure from fraud than are magnetic stripe transactions, which require a visual inspection of the card. Chip-and-PIN cards are more secure from fraud than chip-and-signature cards. When an EMV chip card is used in a POS environment, it generates a cryptogram that changes with each transaction. This dynamic authentication provides an extra layer of security for POS transactions.

For an EMV transaction, use the fields documented in "EMV Request-Level Fields," page 22. The following fields and values are specifically for EMV:

- Request fields: see "EMV Request-Level Fields," page 22.
- Reply fields: see "Reply Fields," page 52.
- Values for pos_entry_mode:
  - contact: Read from direct contact with chip card.
  - contactless: Read from a contactless interface using chip data.
  - msd: Read from a contactless interface using magnetic stripe data (MSD). The msd value is not supported on OmniPay Direct.
- Values for terminal_capability:
  - 4: Terminal can read chip cards.
  - 5: Terminal can read contactless chip cards.

Payment Network Tokenization

Payment network tokenization enables you to request a credit card authorization with a token instead of a primary account number (PAN). For information about adding payment network tokenization to an order management system that already uses CyberSource credit card services, see Payment Network Tokenization Using the SCMP API.
PCI P2P Encryption with Bluefin

Services:
- Authorization
- Stand-alone credit

Processors:
CyberSource supports this feature for all processors that are supported for card-present transactions. See "Supported Processors," page 8.

Device:
- ID TECH SREDKey PCI Key Pad with Encrypted MagStripe Reader

You must use a device that meets the following requirements:
- Is provided by Bluefin Payment Systems unless otherwise agreed to by CyberSource and Bluefin
- Is injected with encryption keys for the CyberSource payment card industry (PCI) point-to-point encryption (P2PE) solution, which is powered by Bluefin
You must have separate devices for sandbox testing and production.

Requirements
You must have a contractual relationship with Bluefin Payment Systems for PCI-validated P2PE services, which include:
- Key injection
- Decryption, which is performed by CyberSource
- Hardware
You must manage your Bluefin devices through the Bluefin P2PE Manager portal, which enables you to:
- Track device shipments
- Deploy or terminate devices
- Manage users and administrators
- View P2PE transactions
- Download and export reports for PCI compliance

Do not use terminal configuration #3 or #5, which causes the device to prompt you for the cardholder's street address. To include the cardholder's street address in your order management system, include the CyberSource API field for the billing street address in your request to CyberSource.
Overview

The CyberSource PCI P2PE solution, which is powered by Bluefin, does the following:

- Safeguards card data at the terminal hardware level
- Reduces your PCI burden by minimizing the number of PCI audit questions to which you must respond
- Provides device life cycle management through the Bluefin P2PE Manager portal
- Supports magnetic stripe read (MSR) and manual key entry

The following diagram illustrates the steps in a transaction that uses encryption:

1. When a customer swipes a card through the Bluefin device, the device encrypts the card details at the hardware level and in accordance with PCI P2PE standards. The device sends the encrypted payload to your order management system.

2. Your order management system sends the encrypted payload to CyberSource in an authorization request or stand-alone credit request.

3. CyberSource sends the encrypted payload to Bluefin to be decrypted and parsed. Bluefin sends the decrypted data to CyberSource over a secure channel.

4. CyberSource sends the decrypted data and additional transaction information to your processor.

Bluefin P2PE Contact Center

The Bluefin P2PE Contact Center solution is supported on the Virtual Terminal in the CyberSource Business Center. For details, see the Business Center Overview.
Creating a Request for an Authorization or Stand-Alone Credit That Uses Bluefin PCI P2PE

For examples that use Bluefin PCI P2PE, see "Authorization Using Bluefin PCI P2PE," page 69.

---

**Step 1** Include the following fields in the request:
- encrypted_payment_data
- encrypted_payment_descriptor

These fields are described in "P2PE Request Fields," page 51.

**Step 2** Include general card-present request fields in the request as needed. See "General Card-Present Request-Level Fields," page 28, and "General Card-Present Offer-Level Fields," page 50.

**Step 3** Follow instructions in *Credit Card Services Using the SCMP API* for creating an authorization request or stand-alone credit request.

---

**Important**

Most of the fields that are normally required for an authorization request or stand-alone credit request are not required for a Bluefin PCI P2PE request because the encrypted data includes most of the required data.

---

**Relaxed Requirements for Address Data and Expiration Date**

To enable relaxed requirements for address data and expiration date, contact CyberSource Customer Support to have your account configured for this feature. For details about relaxed requirements, see the Relaxed Requirements for Address Data and Expiration Date page.
API Fields

### Formatting Restrictions

When you send an authorization, authorization reversal, capture, or credit request that includes card-present data, you must include the basic fields required for every authorization, authorization reversal, capture, or credit request. For information about card-not-present fields required for these requests, see [Credit Card Services Using the SCMP API](#).

**Important**

Values for request-level and offer-level fields must not contain carets (^) or colons (:). However, they can contain embedded spaces and any other printable characters. When you use more than one consecutive space, CyberSource removes the extra spaces.
## Data Type Definitions

Table 7  Data Type Definitions

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time</td>
<td>Format is YYYY-MM-DDThh:mm:ssZ, where:</td>
</tr>
<tr>
<td></td>
<td>- T separates the date and the time</td>
</tr>
<tr>
<td></td>
<td>- Z indicates Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT)</td>
</tr>
<tr>
<td>Decimal</td>
<td>Number that includes a decimal point</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> 23.45, -0.1, 4.0, 90809.0468</td>
</tr>
<tr>
<td>Integer</td>
<td>Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}</td>
</tr>
<tr>
<td>Nonnegative integer</td>
<td>Whole number greater than or equal to zero {0, 1, 2, 3, ...}</td>
</tr>
<tr>
<td>Positive integer</td>
<td>Whole number greater than zero {1, 2, 3, ...}</td>
</tr>
<tr>
<td>String</td>
<td>Sequence of letters, numbers, spaces, and special characters</td>
</tr>
</tbody>
</table>
Appendix A  API Fields

## EMV Request-Level Fields

### Table 8  EMV Request-Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| cardholder_verification_method | Method that was used to verify the cardholder's identity. See "Europay, Mastercard, Visa (EMV)," page 11. Possible values:  
  - 0: No verification  
  - 1: Signature  
  - 2: PIN  
  This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10. | ics_auth (R for successful EMV transactions and EMV fallback transactions) | Integer (1)       |
| emv_request_card_sequence_number | Number assigned to a specific card when two or more cards are associated with the same primary account number. This value enables issuers to distinguish among multiple cards that are linked to the same account. This value can also act as a tracking tool when the issuer reissues cards. When this value is available, it is provided by the chip reader. When the chip reader does not provide this value, do not include this field in your request. See "Europay, Mastercard, Visa (EMV)," page 11.  
  **Note**  
  Information in this guide about EMV applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global. | ics_auth (O)  
  ics_pin_debit_credit (O)  
  ics_pin_debit_purchase (O)  
  **Note** The PIN debit services are supported only on FDC Nashville Global. | American Express Direct: String with numbers only (2)  
  All other processors: String with numbers only (3) |

---

American Express Direct: String with numbers only (2)  
All other processors: String with numbers only (3)
### Table 8  EMV Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>emv_request_combined_tags</td>
<td>EMV data that is transmitted from the chip card to the issuer and from the issuer to the chip card. The EMV data is in the tag-length-value format and includes chip card tags, terminal tags, and transaction detail tags. See &quot;Europay, Mastercard, Visa (EMV),&quot; page 11. For information about the individual tags, see the &quot;Application Specification&quot; section in the EMV 4.3 Specifications: <a href="http://emvco.com">http://emvco.com</a></td>
<td>ics_auth (O) ics_auth_reversal (O) ics_bill (See description) ics_credit (See description) ics_pin_debit_credit (O) ics_pin_debit_purchase (O) ics_pin_debit_reversal (O)</td>
<td>JCN Gateway: 199 bytes All other processors: String (999)</td>
</tr>
</tbody>
</table>

**Important** The following tags contain sensitive information and must not be included in this field:
- 56: Track 1 equivalent data
- 57: Track 2 equivalent data
- 5A: Application PAN
- 5F20: Cardholder name
- 5F24: Application expiration date
- 99: Transaction PIN
- 9F0B: Cardholder name (extended)
- 9F1F: Track 1 discretionary data
- 9F20: Track 2 discretionary data

For information about the individual tags, see the "Application Specification" section in the EMV 4.3 Specifications: http://emvco.com

For captures, this field is required for contact EMV transactions. Otherwise, it is optional.

For credits, this field is required for contact EMV stand-alone credits and contactless EMV stand-alone credits. Otherwise, it is optional.

**Important** For contact EMV captures, contact EMV stand-alone credits, and contactless EMV stand-alone credits, you must include the following tags in this field. For all other types of EMV transactions, the following tags are optional.
- 95: Terminal verification results
- 9F10: Issuer application data
- 9F26: Application cryptogram

**Note** Information in this guide about EMV applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global.

*continued on next page...*
### Table 8  EMV Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| `emv_request_fallback_condition` | Reason for the EMV fallback transaction. An EMV fallback transaction occurs when an EMV transaction fails for one of these reasons:  
  - Technical failure: the EMV terminal or EMV card cannot read and process chip data.  
  - Empty candidate list failure: the EMV terminal does not have any applications in common with the EMV card. EMV terminals are coded to determine whether the terminal and EMV card have any applications in common. EMV terminals provide this information to you.  
  See "Europay, Mastercard, Visa (EMV)," page 11. Possible values:  
  - 1: Transaction was initiated with information from a magnetic stripe, and the previous transaction at the EMV terminal either used information from a successful chip read or it was not a chip transaction.  
  - 2: Transaction was initiated with information from a magnetic stripe, and the previous transaction at the EMV terminal was an EMV fallback transaction because the attempted chip read was unsuccessful.  
  This field is supported only on GPN and JCN Gateway. | ics_auth (R with all card types for an EMV fallback transaction that occurs when an EMV transaction fails for a technical reason; otherwise, not used.)  
ics_bill (R for a forced capture with Visa for an EMV fallback transaction that occurs when an EMV transaction fails for a technical reason; otherwise, not used.)  
ics_credit (R for a stand-alone credit with Visa for an EMV fallback transaction that occurs when an EMV transaction fails for a technical reason; otherwise, not used.) | String (1) |
| `pin_data_encrypted_pin` | Encrypted PIN. This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10, and only for processors that support chip and online PIN transactions as indicated in Table 6, "Processor Support for CVMs," on page 15. | ics_auth (R for online PIN transactions) | String (16) |
## Appendix A

### API Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By:</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pin_data_key_serial_number</code></td>
<td>Combination of the POS terminal's unique identifier and a transaction counter that is used when decrypting the encrypted PIN. The entity that injected the PIN encryption keys into the terminal decrypts the encrypted PIN and creates this value. This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10, and only for processors that support chip and online PIN transactions as indicated in Table 6, &quot;Processor Support for CVMs,&quot; on page 15.</td>
<td>ics_auth (R for online PIN transactions)</td>
<td>String (20)</td>
</tr>
<tr>
<td><code>pin_data_pin_block_encoding_format</code></td>
<td>Format that is used to encode the PIN block. Possible values:</td>
<td>ics_auth (R for online PIN transactions)</td>
<td>Integer (1)</td>
</tr>
<tr>
<td></td>
<td>■ 0: ISO 9564 format 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 1: ISO 9564 format 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 2: ISO 9564 format 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 3: ISO 9564 format 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10, and only for processors that support chip and online PIN transactions as indicated in Table 6, &quot;Processor Support for CVMs,&quot; on page 15.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
Table 8  EMV Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| pos_environment | Operating environment. Possible values for all card types except Mastercard:  
|              | ■ 0: No terminal used or unknown environment.                     | ics_auth (O)                         | String (1)         |
|              | ■ 1: On merchant premises, attended.                              |                                       |                    |
|              | ■ 3: Off merchant premises, attended. Examples: portable POS devices at trade shows, at service calls, or in taxis. |                                       |                    |
|              | ■ 4: Off merchant premises, unattended. Examples: vending machines, home computer, mobile telephone, PDA. |                                       |                    |
|              | ■ 5: On premises of cardholder, unattended.                       |                                       |                    |
|              | ■ 9: Unknown delivery mode.                                       |                                       |                    |
|              | ■ S: Electronic delivery of product. Examples:  
|              | music, software, or eTickets that are downloaded over the internet. |                                       |                    |
|              | ■ T: Physical delivery of product. Examples:  
|              | music or software that is delivered by mail or by a courier.      |                                       |                    |
|              | Possible values for Mastercard:  
|              | ■ 4: Off merchant premises, unattended, or cardholder terminal. Examples: vending machines. |                                       |                    |

This field is supported only on American Express Direct.
## Clear Text Request-Level Fields

### Table 9 Clear Text Request-Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| track_data | Card’s track 1 and 2 data. For all processors except FDMS Nashville, this value consists of one of the following:  
- Track 1 data  
- Track 2 data  
- Data for both tracks 1 and 2  
For FDMS Nashville, this value consists of one of the following:  
- Track 1 data  
- Data for both tracks 1 and 2  
**Example**  
%B411111111111111^SMITH/JOHN ~1612101976110000868000000?;4111111111111111=161210197611868000?    |  
|            | ics_auth:  
- Chase Paymentech Solutions, Credit Mutuel-CIC, FDC Nashville Global, JCN Gateway, OmniPay Direct, and SIX: required if pos_entry_mode = contact, contactless, msd, or swiped; otherwise, not used.  
- All other processors: required if pos_entry_mode = swiped; otherwise, not used. | String (119) |
# General Card-Present Request-Level Fields

Table 10  General Card-Present Request-Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_address1</td>
<td>Credit card billing street address as it appears in credit card issuer’s records.</td>
<td>ics_auth:</td>
<td>FDMS Nashville:</td>
</tr>
<tr>
<td></td>
<td><strong>FDMS Nashville</strong>&lt;br&gt;When the street name is numeric, it must be sent in numeric format. For example, if the address is One First Street, it must be sent as 1 1st Street.</td>
<td></td>
<td>String (20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FDMS Nashville: required if keyed; not used if swiped.</td>
<td>All other processors:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td>String (60)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All other processors: optional</td>
<td></td>
</tr>
<tr>
<td>bill_address2</td>
<td>Used for additional address information. For example: Attention: Accounts Payable</td>
<td>ics_auth (O)</td>
<td>FDMS Nashville:</td>
</tr>
<tr>
<td></td>
<td><strong>FDMS Nashville</strong>&lt;br&gt;bill_address1 and bill_address2 together cannot exceed 20 characters.</td>
<td></td>
<td>String (20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All other processors: String (60)</td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_city</td>
<td>Credit card billing city.</td>
<td>ics_auth:</td>
<td>String (50)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chase Paymentech Solutions: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Credit Mutuel-CIC: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OmniPay Direct: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIX: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All other processors: not used.</td>
<td></td>
</tr>
</tbody>
</table>

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 19. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.
## Appendix A  API Fields

### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Chase Paymentech Solutions: optional.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Credit Mutuel-CIC: optional.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- OmniPay Direct: optional.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SIX: optional.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- All other processors: not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bill_payment</td>
<td>Indicates payment for bill or payment towards existing contractual loan. For information about Visa Bill Payments and Visa Debt Repayments, see <a href="https://www.cybersource.com">Credit Card Services Using the SCMP API</a>.</td>
<td>ics_auth (O)</td>
<td>String (5)</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- false (default): Not a bill payment or loan payment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- true: Bill payment or loan payment.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10 General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_state</td>
<td>Credit card billing state or province. Use the State, Province, and Territory Codes for the United States and Canada.</td>
<td>ics_auth:</td>
<td>String (2)</td>
</tr>
<tr>
<td></td>
<td>- TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td>- Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- All other processors: not used.</td>
<td>- All other processors: not used.</td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
Card-Present Processing Using the SCMP API

Appendix A  API Fields

Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_zip</td>
<td>Postal code for billing address. Postal code must consist of 5 to 9 digits.</td>
<td>ics_auth:</td>
<td>String (10)</td>
</tr>
<tr>
<td></td>
<td>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</td>
<td>FDMS Nashville: required if pos_entry_mode=keyed and the address is in the U.S. or Canada. Optional if pos_entry_mode=keyed and the address is not in the U.S. or Canada. Not used if swiped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> 12345-6789</td>
<td>RBS WorldPay Atlanta: for best card-present keyed rates, send the postal code if pos_entry_mode=keyed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha] [numeric]</td>
<td>TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> A1B 2C3</td>
<td>All other processors: optional.</td>
<td></td>
</tr>
</tbody>
</table>

| card_present | Indicates whether the card is present at the time of the transaction. Possible values: | ics_auth: | String (1) |
|--------------|------------------------------------------------------------------------|FDMS Nashville: not used. |                    |
|              | **N**: Card is not present.                                          | **Y**: Card is present. |All other processors: required. |

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 19. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.
## Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>card_type</td>
<td>Three-digit value that indicates the card type.</td>
<td>ics_auth (Required for Carte Blanche and JCB. Optional for other card types.)</td>
<td>String (3)</td>
</tr>
<tr>
<td></td>
<td>For the possible values, see Appendix D, &quot;Card Types,&quot; on page 71.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important**

CyberSource strongly recommends that you send the card type even when 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.

---

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat_level</td>
<td>Type of cardholder-activated terminal. Possible values:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1: Automated dispensing machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2: Self-service terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3: Limited amount terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4: In-flight commerce (IFC) terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5: Radio frequency device</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6: Mobile acceptance terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7: Electronic cash register</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8: E-commerce device at your location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9: Terminal or cash register that uses a dial-up connection to connect to the transaction processing network</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chase Paymentech Solutions</strong></td>
<td>Only values 1, 2, and 3 are supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FDC Nashville Global</strong></td>
<td>Only values 7, 8, and 9 are supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>GPN</strong></td>
<td>Only values 6, 7, 8, and 9 are supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>JCN Gateway</strong></td>
<td>Only values 6, 7, 8, and 9 are supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TSYS Acquiring Solutions</strong></td>
<td>Only value 6 is supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>Chase Paymentech Solutions</strong>: required if <code>terminal_id</code> is included in the request; otherwise, optional.</td>
<td></td>
<td>Nonnegative integer (1)</td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>FDC Nashville Global</strong>: optional for EMV transactions; otherwise, not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>GPN</strong>: required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>JCN Gateway</strong>: required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>TSYS Acquiring Solutions</strong>: required for transactions from mobile devices; otherwise, not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ics_auth</td>
<td><strong>All other processors</strong>: not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>comments</td>
<td>Brief description or comments for the order.</td>
<td>ics_auth (O)</td>
<td>String (255)</td>
</tr>
<tr>
<td>currency</td>
<td>Currency used for order. For possible values, see the ISO Standard Currency Codes.</td>
<td>ics_auth (R)</td>
<td>String (5)</td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| **customer_cc_cv_indicator** | Indicates whether a CVN code was sent. Possible values:  
  0 (default): CVN service not requested. CyberSource uses this default when you do not include **customer_cc_cv_number** in the request.  
  1 (default): CVN service requested and supported. CyberSource uses this default when you include **customer_cc_cv_number** in the request.  
  2: CVN on credit card is illegible.  
  9: CVN not imprinted on credit card. | ics_auth:  
  FDMS Nashville: required for American Express cards; otherwise, optional.  
  TSYS Acquiring Solutions: optional if **pos_entry_mode**=keyed; otherwise, not used.  
  All other processors: optional. | Nonnegative integer (1) |
| **customer_cc_cv_number** | CVN. See the CVN information in *Credit Card Services Using the SCMP API*. | ics_auth:  
  FDMS Nashville: required for American Express or if swiped; otherwise, optional.  
  TSYS Acquiring Solutions: optional if **pos_entry_mode**=keyed; otherwise, not used.  
  All other processors: optional. | Nonnegative integer (4) |
| **customer_cc_expmo** | Two-digit month in which credit card expires. Format: MM. Possible values: 01 through 12. Leading 0 is required. | ics_auth:  
  FDMS Nashville: required.  
  All other processors: required if **pos_entry_mode**=keyed. | String (2) |

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Appendix A  
### API Fields

#### customer_cc_expyr
Four-digit year in which credit card expires.  
**Format:** YYYY.  
**ics_auth:**  
- FDMS Nashville: required.  
- All other processors: required if `pos_entry_mode=keyed`.  
**Data Type & Length:** Nonnegative integer (4)

#### customer_cc_number
Customer’s credit card number.  
**ics_auth:**  
- FDMS Nashville: required.  
- All other processors: required if `pos_entry_mode=keyed`.  
**Data Type & Length:**  
- FDMS Nashville: Nonnegative integer (19)  
- All other processors: Nonnegative integer (20)

#### customer_email
Customer’s email address, including full domain name.  
**Format:** name@host.domain  
**ics_auth:**  
- Chase Paymentech Solutions: optional.  
- Credit Mutuel-CIC: optional.  
- OmniPay Direct: optional  
- SIX: optional  
- TSYS Acquiring Solutions: required when `bill_payment=true` and `pos_entry_mode=keyed`.  
- Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)  
- All other processors: not used.  
**Data Type & Length:** String (255)

---

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_firstname</td>
<td>Customer’s first name. Value should match value on card.</td>
<td>ics_auth:</td>
<td>String (60)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Chase Paymentech Solutions: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Credit Mutuel-CIC: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ OmniPay Direct: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SIX: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ TSYS Acquiring Solutions: required when bill_payment=true and pos_entry_mode=keyed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ All other processors: not used.</td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_lastname</td>
<td>Customer’s last name. Value should match value on card.</td>
<td>ics_auth:</td>
<td>String (60)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Chase Paymentech Solutions: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Credit Mutuel-CIC: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ OmniPay Direct: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ RBS WorldPay Atlanta: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SIX: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ TSYS Acquiring Solutions: required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>when bill_payment=true and pos_entry_ mode=keyed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ All other processors: not used.</td>
<td></td>
</tr>
<tr>
<td>customer_phone</td>
<td>Customer’s phone number. CyberSource recommends that you include the country code when order is from outside the U.S.</td>
<td>ics_auth:</td>
<td>String (15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Chase Paymentech Solutions: optional.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Credit Mutuel-CIC: optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ OmniPay Direct: optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SIX: optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ TSYS Acquiring Solutions: optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Worldpay VAP: optional. (Worldpay VAP was previously called Litle.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ All other processors: not used</td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By:</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>e_commerce_indicator</td>
<td>Type of transaction. For a card-present transaction, you must set this field to <em>retail</em>.</td>
<td>ics_auth (R)</td>
<td>String (13)</td>
</tr>
<tr>
<td>grand_total_amount</td>
<td>Grand total for the order. You must include either this field or <em>offer0</em> and the offer-level field <em>amount</em>. For information about offers and grand totals, see <em>Getting Started with CyberSource Advanced for the SCMP API</em>.</td>
<td>ics_auth (See description)</td>
<td>String (15)</td>
</tr>
<tr>
<td>ics_applications</td>
<td>CyberSource services to process for the request.</td>
<td>ics_auth (R)</td>
<td>String (255)</td>
</tr>
<tr>
<td>jpo_jcca_terminal_id</td>
<td>Unique Japan Credit Card Association (JCCA) terminal identifier that is provided by CyberSource.</td>
<td>ics_auth (O)</td>
<td>Integer (13)</td>
</tr>
<tr>
<td>jpo_jis2_track_data</td>
<td>Japanese Industrial Standard Type 2 (JIS2) track data from the front of the card.</td>
<td>ics_auth (O)</td>
<td>String (69)</td>
</tr>
<tr>
<td>merchandise_code</td>
<td>Identifier for the merchandise. This field is supported only on the processors listed in this field description.</td>
<td>ics_auth (O)</td>
<td>Integer (7)</td>
</tr>
<tr>
<td>merchant_id</td>
<td>Your CyberSource merchant ID.</td>
<td>ics_auth (R)</td>
<td>String (30)</td>
</tr>
</tbody>
</table>

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 19. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10 General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>merchant_ref_number</td>
<td>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 Advanced for the SCMP API.</td>
<td>ics_auth (R)</td>
<td>String (50)</td>
</tr>
<tr>
<td></td>
<td><strong>FDC Nashville Global</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value for this field must be numeric and must be less than 9 digits. When you do not send a valid value, CyberSource creates one for you. However, the value is not returned to you, so you cannot use the merchant reference number to track the order.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>partner_original_transaction_id</td>
<td>Value that links the previous transaction to the current follow-on request. This value is assigned by the client software that is installed on the POS terminal, which makes it available to the terminal’s software and to CyberSource. Therefore, you can use this value to reconcile transactions between CyberSource and the terminal’s software. CyberSource does not forward this value to the processor. Instead, the value is forwarded to the CyberSource reporting software. This field is supported only for CyberSource integrations as described in “CyberSource Integration,” page 10.</td>
<td>ics_auth (O) ics_auth_reversal (O) ics_bill (O) ics_credit (O)</td>
<td>String (32)</td>
</tr>
<tr>
<td>partner_sdk_version</td>
<td>Version of the software installed on the POS terminal. CyberSource does not forward this value to the processor. Instead, the value is forwarded to the CyberSource reporting software. This field is supported only for CyberSource integrations as described in “CyberSource Integration,” page 10.</td>
<td>ics_auth (O) ics_credit (O)</td>
<td>String (32)</td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>pos_device_id</td>
<td>Value created by the client software that uniquely identifies the POS device.</td>
<td>ics_auth (O) ics_credit (O)</td>
<td>String (32)</td>
</tr>
<tr>
<td></td>
<td>CyberSource does not forward this value to the processor. Instead, the value is forwarded to the CyberSource reporting software.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pos_entry_mode</td>
<td>Method of entering credit card information into the POS terminal. Possible values:</td>
<td>ics_auth (R)</td>
<td>String (11)</td>
</tr>
<tr>
<td></td>
<td>- contact: Read from direct contact with chip card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- contactless: Read from a contactless interface using chip data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- keyed: Manually keyed into POS terminal. This value is not supported on OmniPay Direct.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- msd: Read from a contactless interface using magnetic stripe data (MSD). This value is not supported on OmniPay Direct.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- swiped: Read from credit card magnetic stripe.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The contact, contactless, and msd values are supported only for EMV transactions. See &quot;Europay, Mastercard, Visa (EMV),&quot; page 11.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sales_slip_number</td>
<td>Transaction identifier that you generate. If you do not include this field in your request, CyberSource generates this value for you.</td>
<td>ics_auth (O)</td>
<td>Integer (5)</td>
</tr>
<tr>
<td></td>
<td>This field is supported only on JCN Gateway.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ship_to_address1</td>
<td>First line of shipping address.</td>
<td>ics_auth (Required if any shipping address information is included in the request; otherwise, optional.)</td>
<td>String (60)</td>
</tr>
<tr>
<td>ship_to_address2</td>
<td>Second line of shipping address.</td>
<td>ics_auth (O)</td>
<td>String (60)</td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>ship_to_city</td>
<td>City of shipping address.</td>
<td>ics_auth</td>
<td>String (50)</td>
</tr>
<tr>
<td></td>
<td>(Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ship_to_country</td>
<td>Country of shipping address. Use the ISO Standard Country Codes.</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
<tr>
<td></td>
<td>(Required if any shipping address information is included in the request; otherwise, optional.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ship_to_firstname</td>
<td>First name of the person receiving the shipment.</td>
<td>ics_auth (O)</td>
<td>String (60)</td>
</tr>
<tr>
<td>ship_to_lastname</td>
<td>Last name of the person receiving the shipment.</td>
<td>ics_auth (O)</td>
<td>String (60)</td>
</tr>
<tr>
<td>ship_to_state</td>
<td>State or province to ship the product to. Use the State, Province, and Territory Codes for the United States and Canada.</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
<tr>
<td></td>
<td>(Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ship_to_zip</td>
<td>Postal code for the shipping address. The postal code must consist of 5 to 9 digits. When the shipping country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] <strong>Example</strong> 12345-6789 When the shipping country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha] [numeric] <strong>Example</strong> A1B 2C3</td>
<td>ics_auth</td>
<td>String (10)</td>
</tr>
<tr>
<td></td>
<td>(Required if any shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, optional.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| store_and_forward_indicator | When connectivity is unavailable, the client software that is installed on the POS terminal can store a transaction in its memory and send it for authorization when connectivity is restored. CyberSource does not forward this value to the processor. Instead, the value is forwarded to the CyberSource reporting software. Possible values:  
  - Y: Transaction was stored and then forwarded.  
  - N (default): Transaction was not stored and then forwarded.  
   This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10, but is not supported for Credit Mutuel-CIC. |
|                            | ics_auth (O)                                                                | ics_credit (O)                         | String (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 19. Important: It is your responsibility to determine whether a field is required for the transaction you are requesting.
## Appendix A API Fields

### Table 10 General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| terminal_capability | POS terminal’s capability. Possible values:  
- 1: Terminal has a magnetic stripe reader only.  
- 2: Terminal has a magnetic stripe reader and manual entry capability.  
- 3: Terminal has manual entry capability only.  
- 4: Terminal can read chip cards.  
- 5: Terminal can read contactless chip cards.  
The values of 4 and 5 are supported only for EMV transactions. See "Europay, Mastercard, Visa (EMV)," page 11. | ccAuthService:  
- For the following processors, this field is required:  
  - American Express Direct  
  - Chase Paymentech Solutions  
  - Credit Mutuel-CIC  
  - FDC Nashville Global  
  - FDMS Nashville  
  - OmniPay Direct  
  - SIX  
  - Worldpay VAP (Worldpay VAP was previously called Litle.)  
- For the following processors, this field is optional:  
  - GPN  
  - JCN Gateway  
  - RBS WorldPay Atlanta  
  - TSYS Acquiring Solutions | Integer (1) |
| terminal_card_capture_capability | Indicates whether the terminal can capture the card. Possible values:  
- 1: Terminal can capture card.  
- 0: Terminal cannot capture card.  
This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10, but is not supported for FDC Nashville Global or SIX. | ics_auth (O)  
ics_credit (O) | String (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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Appendix A – API Fields

#### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal_cvm_capabilities_#</td>
<td>Complete list of cardholder verification methods (CVMs) supported by the terminal. Possible values: PIN, Signature</td>
<td>ics_auth (O) ics_credit (O)</td>
<td>String (15)</td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10 General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal_id</td>
<td>Identifier for the terminal at your retail location. You can define this value yourself, but consult the processor for requirements.</td>
<td>ics_auth:</td>
<td>String (8)</td>
</tr>
<tr>
<td></td>
<td><strong>FDC Nashville Global</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To have your account configured to support this field, contact CyberSource Customer Support. This value must be a value that FDC Nashville Global issued to you.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ics_auth:**
- For the following processors, this field is optional. If not provided, CyberSource uses the value in your CyberSource account.
  - American Express Direct
  - Credit Mutuel-CIC
  - FDC Nashville Global
  - SIX
  - Chase Paymentech Solutions: optional. If you include this field in your request, you must also include `cat_level`.
  - FDMS Nashville: CyberSource uses the value in your CyberSource account.
  - OmniPay Direct: optional.
  - For the following processors this field is not used.
    - GPN
    - JCN Gateway
    - RBS WorldPay Atlanta
    - TSYS Acquiring Solutions
    - Worldpay VAP (Worldpay VAP was previously called Litle.)

---

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| terminal_id_alternate | Identifier for an alternate terminal at your retail location. You define the value for this field. This field is supported only for Mastercard transactions on FDC Nashville Global. Use the terminal_id field to identify the main terminal at your retail location. If your retail location has multiple terminals, use this terminal_id_alternate field to identify the terminal used for the transaction. This field is a pass-through, which means that CyberSource does not check the value or modify the value in any way before sending it to the processor. | ics_auth:  
- FDC Nashville Global: optional for Mastercard transactions; otherwise, not used.  
- All other processors: not used. | String (8)          |
| terminal_input_capabilities | Complete list of card input methods supported by the terminal. Possible values:  
- Keyed: Terminal can accept card data that is entered manually.  
- Swiped: Terminal can accept card data from a magnetic stripe reader.  
- Contact: Terminal can accept card data in EMV contact mode.  
- Contactless: Terminal can accept card data in EMV contactless mode.  
- BarCode: Terminal can read bar codes.  
- QRcode: Terminal can read QR codes.  
- OCR: Terminal can perform optical character recognition (OCR).  
This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10. | ics_auth (O)  
ics_credit (O) | String (15) |

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 19. Important: It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10  General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal_output_</td>
<td>Indicates whether the terminal can print or display messages. Possible values:</td>
<td>ics_auth (O)</td>
<td>String (1)</td>
</tr>
<tr>
<td>capability</td>
<td></td>
<td>ics_credit (O)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 1: Neither</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 2: Print only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 3: Display only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 4: Print and display</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>terminal_pin_capability</td>
<td>Maximum PIN length that the terminal can capture. Possible values:</td>
<td>ics_auth (R for PIN transactions)</td>
<td>Integer (2)</td>
</tr>
<tr>
<td></td>
<td>■ 0: No PIN capture capability</td>
<td>ics_credit (R for PIN transactions)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 1: PIN capture capability unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 4: Four characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 5: Five characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 6: Six characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 7: Seven characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 8: Eight characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 9: Nine characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 10: Ten characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 11: Eleven characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 12: Twelve characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10, but is not supported on FDC Nashville Global.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>terminal_serial_number</td>
<td>Terminal serial number assigned by the hardware manufacturer.</td>
<td>ics_auth (O)</td>
<td>String (32)</td>
</tr>
<tr>
<td></td>
<td>CyberSource does not forward this value to the processor. Instead, the value is forwarded to the CyberSource reporting software.</td>
<td>ics_credit (O)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 10: General Card-Present Request-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By:</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal_type</td>
<td>Type of terminal. Possible values:</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
<tr>
<td></td>
<td>21: Attended terminal, online only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>22: Attended terminal, offline with online capability</td>
<td>ics_auth_reversal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>23: Attended terminal, offline only</td>
<td>ics_credit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24: Unattended terminal, online only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>25: Unattended terminal, offline with online capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>26: Unattended terminal, offline only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>transaction_local_date_time</td>
<td>Date and time at your physical location. Format: YYYYMMDDhhmms, where:</td>
<td>ics_auth</td>
<td>String (14)</td>
</tr>
<tr>
<td></td>
<td>YYYY = year</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MM = month</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DD = day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hh = hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mm = minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ss = seconds</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 19. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
## General Card-Present Offer-Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>amount</td>
<td>Per-item price of the product. You must include either offer0 and this field or the request-level field grand_total_amount in your request. The value for this field cannot be negative. For information about offers and grand totals, see Getting Started with CyberSource Advanced for the SCMP API. You can include a decimal point (.) in the value for this field, but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places.</td>
<td>ics_auth (See description)</td>
<td>For GPN and JCN Gateway: Decimal (10) All other processors: Decimal (15)</td>
</tr>
<tr>
<td>merchant_product_sku</td>
<td>Product identifier code. Required when product_code is not default or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>String (15)</td>
</tr>
<tr>
<td>product_code</td>
<td>Type of product. The value for this field is used to identify the product category (electronic, handling, physical, service, or shipping). The default value is default. For a list of valid values, see the information about product codes in Credit Card Services Using the SCMP API. When the value for this field is not default or one of the values related to shipping and/or handling, the quantity, product_name, and merchant_product_sku fields are required. For information about offers and grand totals, see Getting Started with CyberSource Advanced for the SCMP API.</td>
<td>ics_auth (O)</td>
<td>String (30)</td>
</tr>
<tr>
<td>product_name</td>
<td>Required when product_code is not default or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>String (30)</td>
</tr>
</tbody>
</table>
Table 11  General Card-Present Offer-Level Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>quantity</td>
<td>Default is 1. Required when product_code is not default or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>Nonnegative integer (10)</td>
</tr>
</tbody>
</table>
| tax_amount         | Total tax to apply to the product. This value cannot be negative. The tax amount and the offer amount must be in the same currency. The tax amount field is additive. The following example uses a two-exponent currency such as USD:  
1 You include the following offer lines in your request:  
   offer0=amount:10.00^quantity:1^tax_amount:0.80  
   offer1=amount:20.00^quantity:1^tax_amount:1.60  
2 The total amount authorized will be 32.40, not 30.00 with 2.40 of tax included.  
If you want to include tax_amount and also request the ics_tax service, see Tax Calculation Service Using the SCMP API. | ics_auth (O) | Decimal (15) |

Table 12  P2PE Request Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| encrypted_payment_data | Encrypted Bluefin PCI P2PE payment data. Obtain the encrypted payment data from a Bluefin-supported device. See "PCI P2P Encryption with Bluefin," page 17. | ics_auth (R for authorizations that use Bluefin PCI P2PE)  
  ics_credit (R for standalone credits that use Bluefin PCI P2PE) | String (3072) |
| encrypted_payment_descriptor | Format of the encrypted payment data. The value for Bluefin PCI P2PE is Ymx1ZWNzpbg==. See "PCI P2P Encryption with Bluefin," page 17. | ics_auth (R for authorizations that use Bluefin PCI P2PE)  
  ics_credit (R for standalone credits that use Bluefin PCI P2PE) | String (128) |
## Reply Fields

Table 13  Reply Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>acquirer_merchant_number</td>
<td>Identifier that was assigned to you by your acquirer. This value must be printed on the receipt. This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td>ics_auth</td>
<td>String (15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ics_credit</td>
<td></td>
</tr>
<tr>
<td>card_suffix</td>
<td>Last four digits of the cardholder’s account number. This field is included in the reply message when the client software that is installed on the POS terminal uses the token management service (TMS) to retrieve tokenized payment details. You must contact CyberSource Customer Support to have your account enabled to receive these fields in the credit reply message. This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td>ics_credit</td>
<td>String (4)</td>
</tr>
<tr>
<td>card_type</td>
<td>Three-digit value that indicates the card type. For the possible values, see Appendix D, &quot;Card Types,&quot; on page 71. <strong>CyberSource Integrations</strong> This field is included in the reply message when the client software that is installed on the POS terminal uses the token management service (TMS) to retrieve tokenized payment details. You must contact CyberSource Customer Support to have your account enabled to receive these fields in the credit reply message. See &quot;CyberSource Integration,&quot; page 10.</td>
<td>ics_credit</td>
<td>String (3)</td>
</tr>
</tbody>
</table>
### Table 13 Reply Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>emv_reply_combined_tags</td>
<td>EMV data that is transmitted from the chip card to the issuer and from the issuer to the chip card. The EMV data is in the tag-length-value format and includes chip card tags, terminal tags, and transaction detail tags. See &quot;Europay, Mastercard, Visa (EMV),&quot; page 11. For information about the individual tags, see the “Application Specification” section in the EMV 4.3 Specifications: <a href="http://emvco.com">http://emvco.com</a> <strong>Note</strong> Information in this guide about EMV applies to credit card processing and PIN debit processing. All other information in this guide applies only to credit card processing. PIN debit processing is available only on FDC Nashville Global.</td>
<td>ics_auth, ics_author, ics_author_reversal, ics_pin_debit_credit, ics_pin_debit_purchase, ics_pin_debit_reversal</td>
<td>String (999)</td>
</tr>
<tr>
<td>encrypted_payment_error_code</td>
<td>Error code returned by Bluefin when the decryption fails. See Appendix C, &quot;Bluefin PCI P2PE Error Codes,&quot; on page 70.</td>
<td>ics_auth, ics_credit</td>
<td>String (4)</td>
</tr>
<tr>
<td>encrypted_payment_reference_id</td>
<td>Unique transaction identifier returned by Bluefin. You can use this value for tracking and reporting. See &quot;PCI P2P Encryption with Bluefin,&quot; page 17.</td>
<td>ics_auth, ics_credit</td>
<td>Integer (25)</td>
</tr>
<tr>
<td>issuer_response_code</td>
<td>Additional authorization code that must be printed on the receipt when returned by the processor. This value is generated by the processor and is returned only for a successful transaction. This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10, but is supported only for FDC Nashville Global and SIX.</td>
<td>ics_auth, ics_author_reversal</td>
<td>Integer (6)</td>
</tr>
<tr>
<td>routing_network_label</td>
<td>Name of the network on which the transaction was routed. This field is supported only on FDC Nashville Global.</td>
<td>ics_auth</td>
<td>String (10)</td>
</tr>
<tr>
<td>routing_network_type</td>
<td>Indicates whether the transaction was routed on a credit network, a debit network, or the STAR signature debit network. Possible values: &lt;ul&gt; &lt;li&gt;C: Credit network&lt;/li&gt; &lt;li&gt;D: Debit network (without signature)&lt;/li&gt; &lt;li&gt;S: STAR signature debit network&lt;/li&gt; &lt;/ul&gt; This field is supported only on FDC Nashville Global.</td>
<td>ics_auth</td>
<td>String (1)</td>
</tr>
</tbody>
</table>
### Appendix A  API Fields

**routing_signature_cvm_required**
- Indicates whether you need to obtain the cardholder's signature. Possible values:
  - **Y**: You need to obtain the cardholder's signature.
  - **N**: You do not need to obtain the cardholder's signature.
- This field is supported only on FDC Nashville Global.

**sales_slip_number**
- Transaction identifier. If you included this field in the request, the returned value is the value that you sent in the request. If you did not include this field in the request, CyberSource generated this value for you.
- The difference between this field and the `receiptNumber` field is that CyberSource generates the receipt number, and you must print the receipt number on the receipt; whereas you can generate the sales slip number, and you can choose to print the sales slip number on the receipt.
- This field is supported only on JCN Gateway.

**terminal_id**
- Terminal identifier assigned by the acquirer. This value must be printed on the receipt.
- This field is supported only for CyberSource integrations as described in "CyberSource Integration," page 10.

**terminal_id_alternate**
- Identifier for an alternate terminal at your retail location. You defined the value for this field in the request message. This value must be printed on the receipt.
- This field is supported only for MasterCard transactions on FDC Nashville Global.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing_signature_cvm_required</td>
<td>Indicates whether you need to obtain the cardholder's signature. Possible values: Y: You need to obtain the cardholder's signature. N: You do not need to obtain the cardholder's signature. This field is supported only on FDC Nashville Global.</td>
<td>ics_auth</td>
<td>String (1)</td>
</tr>
<tr>
<td>sales_slip_number</td>
<td>Transaction identifier. If you included this field in the request, the returned value is the value that you sent in the request. If you did not include this field in the request, CyberSource generated this value for you. The difference between this field and the <code>receiptNumber</code> field is that CyberSource generates the receipt number, and you must print the receipt number on the receipt; whereas you can generate the sales slip number, and you can choose to print the sales slip number on the receipt. This field is supported only on JCN Gateway.</td>
<td>ics_auth</td>
<td>Integer (5)</td>
</tr>
<tr>
<td>terminal_id</td>
<td>Terminal identifier assigned by the acquirer. This value must be printed on the receipt. This field is supported only for CyberSource integrations as described in &quot;CyberSource Integration,&quot; page 10.</td>
<td>ics_auth ics_credit</td>
<td>String (8)</td>
</tr>
<tr>
<td>terminal_id_alternate</td>
<td>Identifier for an alternate terminal at your retail location. You defined the value for this field in the request message. This value must be printed on the receipt. This field is supported only for MasterCard transactions on FDC Nashville Global.</td>
<td>ics_auth ics_auth_reversal</td>
<td>String (8)</td>
</tr>
</tbody>
</table>
Sale Using Swiped Track Data

Example 1  Request Message: Sale Using Swiped Track Data

```
merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=swiped
card_present=Y
terminal_capability=2
track_data=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
                ***??*;4111111111111111=16121200XXXX0000000000?*
ics_applications=ics_auth,ics_bill
ecommerce_indicator=retail
```
Example 2  Reply Message: Sale Using Swiped Track Data

```
merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=0412MCCNYJPWY
auth_card_category=J1
auth_card_group=0
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=260371
```

Sale Using Keyed Data

Example 3  Request Message: Sale Using Keyed Data

```
merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=keyed
card_present=Y
terminal_capability=2
customer_cc_number=4111111111111111
customer_cc_expmo=12
customer_cc_expyr=2016
card_type=001
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
```
Example 4 Reply Message: Sale Using Keyed Data

```plaintext
merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=0412MCCNYJPWY
auth_card_category=J1
auth_card_group=0
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_bill_ref_no=1094820975023470
receipt_number=260371
```
Appendix B  Examples

Sale Using EMV Technology with a Contact Read

American Express Direct

Example 5  Request Message: Sale on American Express Direct Using EMV Technology with a Contact Read

```
merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contact
pos_device_id=123lkjd10bk34981svli39bj
card_present=Y
terminal_capability=4
terminal_serial_number=01043191
terminal_input_capabilities_0=contact
terminal_input_capabilities_1=contactless
terminal_input_capabilities_2=keyed
terminal_input_capabilities_3=swiped
terminal_cvm_capabilities_0=pin
terminal_cvm_capabilities_1=signature
track_data=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
***?*;4111111111111111=16121200XXXX00000000?*
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
cardholder_verificationMethod=2
emv_request_combined_tags=9F33032040009505000000009F3704518823719F100
7060111103A00009F26081E1756ED0E2134E29F3602015820200909C0109F1A020
8409A030006219F020600000000020005F2A020849F0306000000000000
emv_request_card_sequence_number=001
partner_original_transaction_id=510be4aef90711e6acbc7d88388d803d
partner_sdk_version=2.18.0
```
Example 6  Reply Message: Sale on American Express Direct Using EMV Technology with a Contact Read

merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_amount=75.00
auth_code=831000
auth_avs=2
auth_response=00
auth_trans_ref_no=1094820975023470
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=260371
emv_reply_combined_tags=9F330320400095050000000009F3704518823719F100
706011103A000009F26081E1756ED0E213E29F360200158202000009C01009F1A02
8409A03006219F020600000000020005F2A020849F03060000000000
acquirer_merchant_number=1234567890
issuer_response_code=721100
terminal_id=ABCD1234
Example 7 Request Message: Sale on Credit Mutuel-CIC, FDC Nashville Global, or SIX Using EMV Technology with a Contact Read

```plaintext
merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contact
pos_device_id=1231kjdiOBK34981sviLi39bj
card_present=Y
terminal_capability=4
terminal_serial_number=01043191
terminal_input_capabilities_0=contact
terminal_input_capabilities_1=contactless
terminal_input_capabilities_2=keyed
terminal_input_capabilities_3=swiped
terminal_cvm_capabilities_0=pin
terminal_cvm_capabilities_1=signature
track_data=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
cardholder_verificationMethod=2
emv_request_combined_tags=9F3303204000950500000000009F3704518823719F100
706011103AO00009F2608E175EDE023134E29F3602001582000009C0109F1A020
8409A30006219F0206000000000020005F2A020849F0306000000000000
emv_request_card_sequence_number=001
partner_original_transaction_id=510be4aeef90711e6abc7d85388d803d
partner_sdk_version=2.18.0
```
### Example 8  
**Reply Message: Sale on Credit Mutuel-CIC, FDC Nashville Global, or SIX Using EMV Technology with a Contact Read**

```plaintext
merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=260371
emv_reply_combined_tags=9F33032040009505000000009F3704518823719F100
  706011103A000009F26081E175ED0E213E29F3602001582080009CD01009F1A020
  8490A3D006219F020600000000200005F2A020849F030600000000000
acquirer_merchant_number=1234567890
issuer_response_code=721100
terminal_id=ABCD1234
```
Dynamic Currency Conversion on FDC Nashville Global or SIX

Example 9  
Request Message: Sale on FDC Nashville Global or SIX Using Dynamic Currency Conversion and EMV Technology with a Contact Read

```plaintext
merchant_id=Merchant12345
merchant_ref_number=FDE Contact Auth 1
currency=EUR
grand_total_amount=30
foreign_amount=30
foreign_currency=EUR
original_amount=25.44
original_currency=GBP
exchange_rate=1.1789
exchange_rate_timeStamp=20170824 10:21
dcc_indicator=1
pos_entry_mode=contact
card_present=Y
terminal_capability=4
track_data=%B4111111111111111110^SMITH/BETTY^20121200123456012**XXX***
**??;41111111111111111111D02121200XXXX00000??
terminal_id=99D11001
pos_device_id=device1
terminal_input_capabilities_0=swiped
terminal_input_capabilities_1=contact
terminal_input_capabilities_2=contactless
terminal_cvm_capabilities_0=signature
terminal_cvm_capabilities_1=pin
card_type=001
ics_applications=ics_auth
e_commerce_indicator=retail
cardholder_verification_method=2
partner_original_transaction_id=510be4aef90711e6acbc7d88388d803d
dev_request_combined_tags=9F3303204000950500000000000009F3704518823719F100
706011103A000009F260812175EDD02234E29F36020015820000000C010091A020
8409A0300621F0206000000000020005SF2A0208409F03060000000000000
emv_request_card_sequence_number=001
```

Card-Present Processing Using the SCMP API | June 2019 | 62
Appendix B  Examples

All Other Processors

Example 10  Request Message: Sale Using EMV Technology with a Contact Read

merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contact
card_present=Y
terminal_capability=4
track_data=3841111111111111\SMITH/BETTY\16121200123456789012**XXX**
**4111111111111111=16121200XXXX00000000*'
is_applications=ics_auth,ics_bill
e_commerce_indicator=retail
emv_request_combined_tags=9F33032040009505000000000009F3704518823719F100
7060111103A000009F26081E1756ED0E2134E29F360200158202000009C01009F1A020
8409A03006219F0206000000000000005F2A0208409F03060000000000
emv_request_card_sequence_number=001

Example 11  Reply Message: Sale Using EMV Technology with a Contact Read

merchant_ref_number=ABC123
request_id=030578265000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=0412MCCNYJPWY
auth_card_category=J1
auth_card_group=0
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=260371
emv_reply_combined_tags=9F33032040009505000000000009F3704518823719F100
7060111103A000009F26081E1756ED0E2134E29F360200158202000009C01009F1A020
8409A03006219F0206000000000000005F2A0208409F03060000000000
Sale Using EMV Technology with a Contactless Read

American Express Direct

Example 12  Request Message: Sale on American Express Direct Using EMV Technology with a Contactless Read

merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contactless
pos_device_id=123lkjdIOBK34981slviLI39bj
card_present=Y
terminal_capability=5
terminal_serial_number=01043191
terminal_input_capabilities_0=contact
terminal_input_capabilities_1=contactless
terminal_input_capabilities_2=keyed
terminal_input_capabilities_3=swiped
terminal_cvm_capabilities_0=pin
terminal_cvm_capabilities_1=signature
track_data=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
***?4111111111111111=16121200XXXX00000000?*
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
cardholder_verificationMethod=2
emv_request_combined_tags=9F330320400095050000000009F3704518823719F100
706011109030009P6E01E1756EC629F360201562000009C01009F1A20
8409A03006219P020600000000020005F2A0208409P030600000000000
emv_request_card_sequence_number=001
partner_original_transaction_id=510be4aeef907116acbc7d88388d803d
partner_sdk_version=2.18.0
Example 13  Reply Message: Sale on American Express Direct Using EMV Technology with a Contactless Read

```plaintext
merchant_ref_number=ABC123
request_id=030578265000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=852734
emv_reply_combined_tags=9F33032040009505000000000093704518823719F100
706011103AA00009F26D81E175ED90E2134E29F36020015820200009C01009F1A020
8409A030006219F0206000000020005F2A020849F030600000000000
acquirer_merchant_number=1234567890
issuer_response_code=721100
terminal_id=ABCD1234
```
Appendix B  Examples

Credit Mutuel-CIC, FDC Nashville Global, or SIX

Example 14  Request Message: Sale on Credit Mutuel-CIC, FDC Nashville Global, or SIX Using EMV Technology with a Contactless Read

merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contactless
pos_device_id1231kjd10B3498ls1vi3I39fbj
card_present=Y
terminal_capability=5
terminal_serial_number=01043191
terminal_input_capabilities_0=contact
terminal_input_capabilities_1=contactless
terminal_input_capabilities_2=keyed
terminal_input_capabilities_3=swiped
terminal_cvm_capabilities_0=pin
terminal_cvm_capabilities_1=signature
track_data=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
cardholder_verificationMethod=2
emv_request_combined_tags=9F330320400095050000000009F3704518823719F100
706011103A00009F26081E175E68E2134E29F3602001582000009C01009F1A02
849A03006219F020600000000000000000000000000000000000000
emv_request_card_sequence_number=001
partner_original_transaction_id=510be4ae09711e6abc7d88388d803d
partner_sdk_version=2.18.0
Example 15  Reply Message: Sale on Credit Mutuel-CIC, FDC Nashville Global, or SIX Using EMV Technology with a Contactless Read

```
merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_response=00
auth_trans_ref_no=1094820975023470
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=852734
emv_reply_combined_tags=9F33032040009505000000000009F3704518823719F100
706011103A0000000F26081E175EDE0E2134E29F3602001582000009C01009F1A020
8409A030006219F02060000000000200052F2A0208409F03060000000000
acquirer_merchant_number=1234567890
issuer_response_code=721100
terminal_id=ABCD1234
```

All Other Processors

Example 16  Request Message: Sale Using EMV Technology with a Contactless Read

```
merchant_id=JanesPlants
merchant_ref_number=ABC123
currency=usd
grand_total_amount=75.00
pos_entry_mode=contactless
card_present=Y
terminal_capability=5
track_data=4B411111111111111111**XXX***
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
emv_request_combined_tags=9F33032040009505000000000009F3704518823719F100
706011103A0000000F26081E175EDE0E2134E29F3602001582000009C01009F1A020
8409A030006219F02060000000000200052F2A0208409F03060000000000
emv_request_card_sequence_number=001
auth_capture_date=0823
```
Example 17  Reply Message: Sale Using EMV Technology with a Contactless Read

merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_amount=75.00
auth_code=831000
auth_avs=2
auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=0412MCCNYJPWY
auth_card_category=J1
auth_card_group=0
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_amount=75.00
bill_trans_ref_no=1094820975023470
receipt_number=852734
emv_reply_combined_tags=9F330320400095050000000009F3704518823719F100
706011103A000009F26081E1756ED0E2134E29F36020015820200009C01009F1A20
8409A03006219F0296600000002000SP2A0208409F035600000000000
Authorization Using Bluefin PCI P2PE

Example 18  Request Message: Authorization Using Bluefin PCI P2PE

```plaintext
merchant_id=demomerchant
merchant_ref_number=demorefnum
currency=usd
grand_total_amount=75.00
pos_entry_mode=keyed
card_present=y
terminal_capability=2
encrypted_payment_data=02d70081f3c20008383252a363031312a2a2a2a2a2a2
a303030395e46444d532020202020202020202020202020202020205e323232
2a2a2a2a2a2a2a2a3f2a3b363031312a2a2a2a2a2a303030393d3232323232a2a2
a2a2a2a2a2a75ad15d5217290c54b3d9d1c386862136c68d339f2d98323391
f3e63151d548ff80b414feac9ff6c6dede8fb09bae870e432ff64626a75faa178c
3bd18d63ade21bc7a0ea687a2eef64551751e502d97cb98d533a55126cda39543132
34932383030372994901000001a000731a8003
encryptedPayment_descriptor=Ymx1ZWZpbg==
ics_applications=ics_auth
e_commerce_indicator=retail
```

Example 19  Reply Message: Authorization Using Bluefin PCI P2PE

```plaintext
merchant_ref_number=demorefnum
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
auth_rcode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_amount=75.00
auth_auth_code=831000
auth_avs=1
auth_response=100
auth_trans_ref_no=104820975023470
encrypted_payment_reference_id=120160922212209101307861
```
Bluefin PCI P2PE Error Codes

The following table describes the error codes returned by Bluefin for Bluefin PCI P2PE transactions. For information about encrypted transactions, see "PCI P2P Encryption with Bluefin," page 17. When an encryption error occurs:

- CyberSource sets the reply flag field to `ESYSTEM` in the authorization or stand-alone credit reply message. This value indicates that a general system failure occurred and your authorization or stand-alone credit request was not processed.
- CyberSource sets the value for `encrypted_payment_error_code` to the Bluefin PCI P2PE error code.

Table 14 Bluefin PCI P2PE Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Generic or unknown error code.</td>
</tr>
<tr>
<td>1101</td>
<td>Internal system configuration setup error</td>
</tr>
<tr>
<td>1102</td>
<td></td>
</tr>
<tr>
<td>1103</td>
<td></td>
</tr>
<tr>
<td>1104</td>
<td></td>
</tr>
<tr>
<td>1105</td>
<td></td>
</tr>
<tr>
<td>1202</td>
<td>Device not found or device not recognized.</td>
</tr>
<tr>
<td>1203</td>
<td>Device not active.</td>
</tr>
<tr>
<td>1204</td>
<td>Invalid firmware version.</td>
</tr>
<tr>
<td>1303</td>
<td>All decryptions failed.</td>
</tr>
<tr>
<td>1404</td>
<td>Decryption failed for some other reason.</td>
</tr>
<tr>
<td>1406</td>
<td>Decrypted result did not include credit card information.</td>
</tr>
</tbody>
</table>
Card Types

Table 15 lists the values that are supported for the card_type field in requests and replies. Even though all of these card types are supported for card-not-present transactions, many of them are not supported for card-present transactions. Contact your processor if you have questions about which card types are supported for card-present transactions.

<table>
<thead>
<tr>
<th>Value</th>
<th>Card Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>Visa</td>
</tr>
<tr>
<td></td>
<td>For card-present transactions on all processors except SIX, the Visa Electron card type is processed the same way that the Visa debit card is processed. Use card type value 001 for Visa Electron.</td>
</tr>
<tr>
<td>002</td>
<td>Mastercard, Eurocard¹: European regional brand of Mastercard.</td>
</tr>
<tr>
<td>003</td>
<td>American Express</td>
</tr>
<tr>
<td>004</td>
<td>Discover</td>
</tr>
<tr>
<td>005</td>
<td>Diners Club</td>
</tr>
<tr>
<td>006</td>
<td>Carte Blanche¹</td>
</tr>
<tr>
<td>007</td>
<td>JCB¹</td>
</tr>
<tr>
<td>014</td>
<td>EnRoute¹</td>
</tr>
<tr>
<td>021</td>
<td>JAL¹</td>
</tr>
<tr>
<td>024</td>
<td>Maestro (UK Domestic)¹</td>
</tr>
<tr>
<td>033</td>
<td>Visa Electron¹</td>
</tr>
<tr>
<td></td>
<td>Use this value only for SIX. For other processors, use 001 for all Visa card types.</td>
</tr>
<tr>
<td>034</td>
<td>Dankort¹</td>
</tr>
<tr>
<td>036</td>
<td>Cartes Bancaires¹</td>
</tr>
</tbody>
</table>

¹ For this card type, you must include the card_type field in your request for an authorization or a stand-alone credit.
Table 15  Card Types (Continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Card Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>037</td>
<td>Carta Si¹</td>
</tr>
<tr>
<td>039</td>
<td>Encoded account number¹</td>
</tr>
<tr>
<td>040</td>
<td>UATP¹</td>
</tr>
<tr>
<td>042</td>
<td>Maestro (International)¹</td>
</tr>
<tr>
<td>050</td>
<td>Hipercard²</td>
</tr>
<tr>
<td>051</td>
<td>Aura</td>
</tr>
<tr>
<td>054</td>
<td>Elo</td>
</tr>
<tr>
<td>062</td>
<td>China UnionPay</td>
</tr>
</tbody>
</table>

¹ For this card type, you must include the `card_type` field in your request for an authorization or a stand-alone credit.