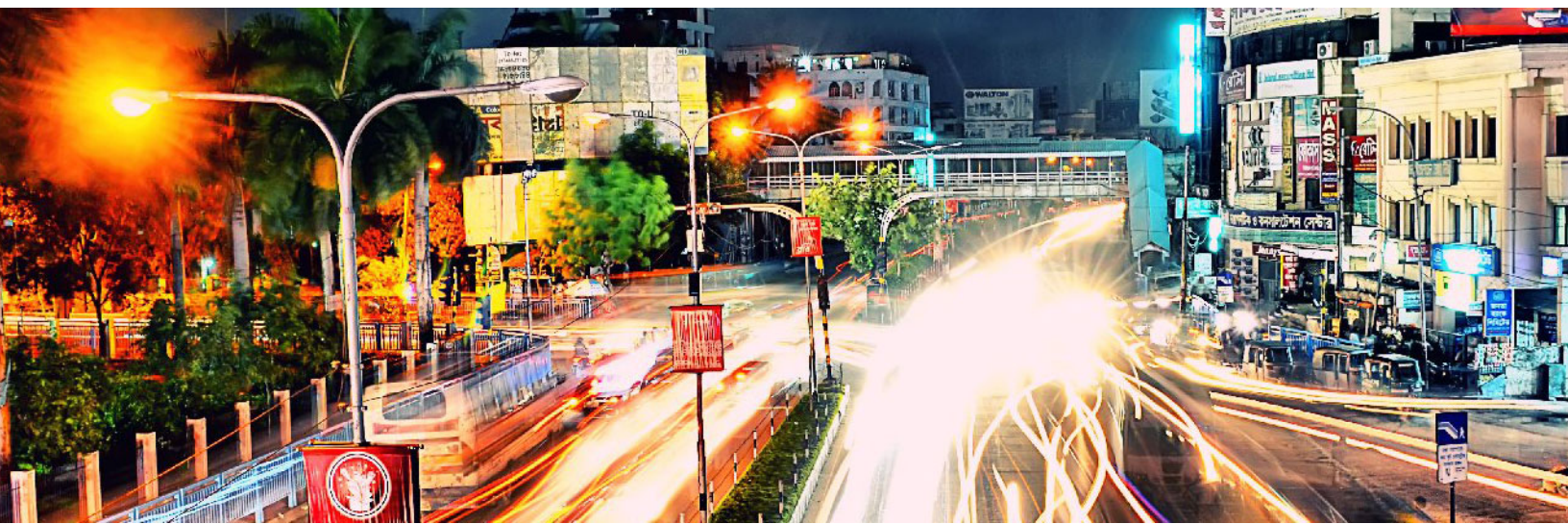# Card-Present Processing for Cybersource through VisaNet Using the SCMP API

Supplement to Credit Card Services for CyberSource through VisaNet Using the SCMP API
and
PIN Debit Processing for CyberSource through VisaNet Using the SCMP API

CyberSource®
A Visa Solution

Contents

Recent Revisions to This Document

Release	Changes
December 2020	Changed *Cybersource through VisaNet* to *Cybersource through VisaNet*.
	Updated the description for the **emv_request_combined_tags**. See "EMV Request-Level Fields," page 19.
July 2020	Updated the requirements for the following fields. See "General Card-Present Request-Level Fields," page 24.
	■ jpo_jcca_terminal_id
	■ sales_slip_number
	■ transaction_local_date_time
March 2020	Added support for mass transit transactions:
	■ Added "Mass Transit Transactions," page 12.
	■ Added the following fields to "General Card-Present Request-Level Fields," page 24:
	● aggregated_auth_indicator
	● auth_capture_date
	● auth_deferred_auth_indicator
	● debt_recovery_indicator
	● transportation_mode
	■ Updated the description for the **industry_datatype** field in "General Card-Present Request-Level Fields," page 24.
November 2019	Updated link to documentation about payment network tokens. See "Authorizations with Payment Network Tokens," page 10.
	Updated the description for the **emv_request_repeat** field. See "EMV Request-Level Fields," page 19.
	Updated the descriptions for the following reply fields in "Reply Fields," page 42:
	■ emv_reply_chip_validation_results
	■ emv_reply_chip_validation_type
	■ issuer_pin_request

Release	Changes
October 2019	Added the **emv_request_repeat** field. For details, see "EMV Request-Level Fields," page 19.
	Added the **issuer_pin_request** field. For details, see "Reply Fields," page 42.
September 2019	Created new examples. See Appendix B, "Examples," on page 45.
	Updated the description for the **terminal_capability** field in "General Card-Present Request-Level Fields," page 24.
	Updated descriptions for the following fields in "Reply Fields," page 42:
	■ emv_reply_chip_validation_results
	■ emv_reply_chip_validation_type
	Corrected the data types for the following fields in "General Card-Present Request-Level Fields," page 24:
	■ cashback_amount
	■ grand_total_amount
	■ gratuity_amount
	Deleted the following fields because they are not supported on Cybersource through VisaNet. See "General Card-Present Request-Level Fields," page 24.
	■ All bill-to fields except **bill_zip**
	■ All ship-to fields except **ship_to_zip**
	Removed "Beta" from the cover because the Cybersource through VisaNet card-present functionality is not considered beta.

About This Guide

Audience and Purpose

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

Implementing the 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.

Information in this guide about Europay, Mastercard, and Visa (EMV) applies to payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.

Conventions

The following special statement is used in this document:

⚠	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 1   Text Conventions

Convention	Meaning
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.

■ The CyberSource API Versions page provides information about the API versions.

■ *Credit Card Services for CyberSource through VisaNet Using the SCMP API* describes how to integrate payment processing services into your business. To obtain this document, contact customer support.

■ *PIN Debit Processing for CyberSource through VisaNet Using the SCMP API* describes how to integrate payment processing services into your business. To obtain this document, contact customer support.

Refer to the Support Center for complete technical documentation:

https://www.cybersource.com/en-us/support/technical-documentation.html

Customer Support

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

http://www.cybersource.com/support

Introduction to Card-Present Transactions

This supplement to *Credit Card Services for CyberSource through VisaNet Using the SCMP API* describes card-present processing.

Information in this guide about Europay, Mastercard, and Visa (EMV) applies to payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.

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 customer support whether you must have a separate Cybersource merchant ID for your card-present transactions.

■ Contact customer support to have your account configured to process card-present transactions.

■ Make sure that you are familiar with the SCMP API for processing e-commerce and mail order/telephone order (MOTO) transactions as described in *Credit Card Services for CyberSource through VisaNet Using the SCMP API*. Use the fields in this guide in addition to the fields in *Credit Card Services for CyberSource through VisaNet Using the SCMP API*.

Optional Features

Authorizations with Payment Network Tokens

You can request a payment card authorization with a payment network token instead of a primary account number (PAN). For information about adding this functionality to an order management system that already uses credit card services, see *Authorizations with Payment Network Tokens Using the SCMP API*.

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 payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.

Services:

- Authorization
- Authorization reversal
- Capture
- Credit
- PIN debit credit
- PIN debit purchase
- PIN debit reversal

Card Types for Contact EMV Transactions:

- American Express

- Mastercard

- Visa

Card Types for Contactless EMV Transactions:

- American Express ExpressPay

- Mastercard PayPass

- Visa payWave

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, which 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.

EMV Cards and Cardholder Verification Methods (CVMs)

Most EMV cards are chip-and-PIN cards. For these cards, a PIN is the preferred CVM. 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.

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 19. The following fields and values are specifically for EMV:

- Request fields: see "EMV Request-Level Fields," page 19.

- Reply fields: see "Reply Fields," page 42

- 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).

- Values for **terminal_capability**:
  - `4`: Terminal can read chip cards.
  - `5`: Terminal can read contactless chip cards.

Mass Transit Transactions

Service:

- Authorization

Card types:

- Mastercard
- Visa

The following transaction types are supported for mass transit transactions (MTTs):

- Contactless zero amount authorizations
- Contactless deferred authorizations
- Cardholder-initiated MOTO and e-commerce debt recovery
- Merchant-initiated MOTO debt recovery

For an MTT, you can capture a declined authorization when the amount is less than the regional chargeback threshold.

Create an authorization request for an MTT:

Step 1   Include the **industry_datatype** field in the authorization request. Set the value for this field to `transit`.

Step 2   Include fields required for an authorization request.

Step 3   Include any of the following optional MTT request fields:

- aggregated_auth_indicator
- auth_capture_date
- auth_deferred_auth_indicator
- debt_recovery_indicator
- transportation_mode

For descriptions of these fields, see "General Card-Present Request-Level Fields," page 24.

PCI P2P Encryption with Bluefin

Services:

- Authorization
- Stand-alone credit

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 need to 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 API field for the billing street address in your request.

Overview

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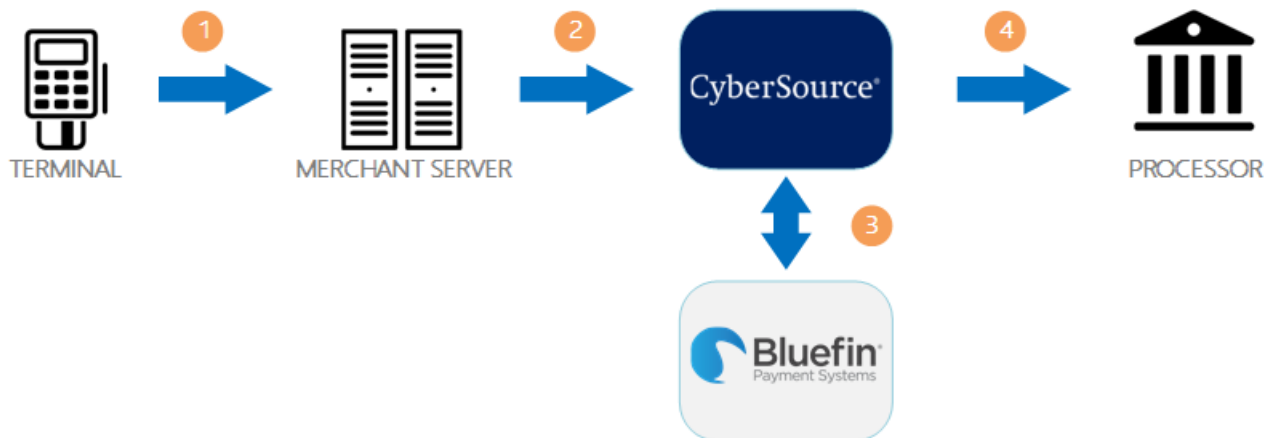
1   When a customer swipes a card through the Bluefin device, the device encrypts the card details at the hardware level and in accordance with PCI P2PE standards. The device sends the encrypted payload to your order management system.

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.

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 55.

Step 1   Include the following fields in the request:

- encrypted_payment_data
- encrypted_payment_descriptor

These fields are described in "P2PE Request Fields," page 41.

Step 2   Include general card-present request fields in the request as needed. See "General Card-Present Request-Level Fields," page 24, and "General Card-Present Offer-Level Fields," page 39.

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

> ⚠️ 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.

POS Transactions in Brazil

Services:

- Authorization
- Capture
- Credit

The **merchant_descriptor_postal_code** field is required for POS transactions in Brazil. For a description of this field, see the information about merchant descriptors in *Merchant Descriptors Using the SCMP API*.

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

> This guide is a supplement to the credit card guide and PIN debit guide. This supplement provides information about features and fields that are used in addition to the information that is in the credit card guide and PIN debit guide.
>
> When you send a request that includes card-present data, you must include the basic fields required for every credit card or PIN debit request. For information about these basic fields, see *Credit Card Services for CyberSource through VisaNet Using the SCMP API* and *PIN Debit Processing for CyberSource through VisaNet Using the SCMP API*.

Formatting Restrictions

Unless otherwise noted, all fields are order and case insensitive and the fields accept special characters such as @, #, and %.

> 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

For more information about these data types, see the World Wide Web Consortium (W3C) XML Schema Part 2: Datatypes Second Edition.

Table 2   Data Type Definitions

Data Type	Description
Date and time	Format is YYYY-MM-DDThhmmssZ, where: ■ T separates the date and the time ■ Z indicates Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT) **Example** 2020-01-11T224757Z equals January 11, 2020, at 22:47:57 (10:47:57 p.m.)
Decimal	Number that includes a decimal point **Example** 23.45, -0.1, 4.0, 90809.0468
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
Nonnegative integer	Whole number greater than or equal to zero {0, 1, 2, 3, ...}
Positive integer	Whole number greater than zero {1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

EMV Request-Level Fields

Table 3   EMV Request-Level Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 10. Information in this guide about EMV applies to payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.	ics_auth (O) ics_pin_debit_credit (O) ics_pin_debit_purchase (O)	String with numbers only (3)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Table 3   EMV Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
emv_request_ combined_tags	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 "Europay, Mastercard, Visa (EMV)," page 10. For information about the individual tags, see the "Application Specification" section in the *EMV 4.3 Specifications*: http://emvco.com **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 Information in this guide about EMV applies to payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.	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)	In Japan: 199 bytes In other countries: String (252)

continued on next page...

Table 3   EMV Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
emvRequest_ combinedTags (*continued*)	***Cybersource through VisaNet*** Include the following tag for better interchange rates: ■ 84: Dedicated file name The value for Tag 84 corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP02 TCR0 ■ Position: 118-149 ■ Field: Dedicated File Name - Application ID (AID)		
emv_request_repeat	Indicates that this is a duplicate authorization request. When you receive the **issuer_pin_ request** field in an authorization reply message, you must respond with the customer's PIN in a duplicate authorization request. Possible value: ■ 1: This is a duplicate authorization request. This field is supported only for Mastercard transactions.	ics_auth (R for a duplicate authorization request; otherwise, O.)	String (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Table 3   EMV Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
pos_environment	Operating environment. Possible values for all card types except Mastercard: ▪ 0: No terminal used or unknown environment. ▪ 1: On merchant premises, attended. ▪ 2: On merchant premises, unattended. Examples: oil, kiosks, self-checkout, mobile telephone, personal digital assistant (PDA). ▪ 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: ▪ 2: On merchant premises, unattended, or cardholder terminal. Examples: oil, kiosks, self-checkout, home computer, mobile telephone, personal digital assistant (PDA). Cardholder terminal is supported only for Mastercard transactions. ▪ 4: Off merchant premises, unattended, or cardholder terminal. Examples: vending machines, home computer, mobile telephone, PDA. Cardholder terminal is supported only for Mastercard transactions.	ics_auth (O)	String (1)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Clear Text Request-Level Fields

Table 4   Clear Text Request-Level Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
pos_service_code	Mastercard service code that is included in the track data. You can extract the service code from the track data and provide it in this API field. This field is supported only for Mastercard.	ics_auth (O)	String (3)
track_data	Card's track 1 and 2 data. This value consists of one of the following: ■ Track 1 data ■ Track 2 data ■ Data for both tracks 1 and 2 **Example** %B4111111111111111^SMITH/JOHN ^1612101976110000868000000?;4111111111111111=16121019761186800000?	ics_auth (R when **pos_entry_mode** is `contact`, `contactless`, `msd`, or `swiped`; otherwise, not used.)	String (119)

General Card-Present Request-Level Fields

Table 5   General Card-Present Request-Level Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
aggregated_auth_ indicator	Flag for a mass transit transaction that indicates whether the authorization is aggregated. Possible values: ■ Y: Aggregated ■ N: Not aggregated The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR7 ■ Position: 150-151 ■ Field: Transit Transaction Type Indicator This field is supported only for mass transit transactions. See "Mass Transit Transactions," page 12.	ics_auth (O)	String (1)
auth_capture_date	Date on which the customer initiated a contactless transit transaction. Format: MMDD This field is supported only for mass transit transactions. See "Mass Transit Transactions," page 12.	ics_auth (O)	String (4)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2   This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length

auth_deferred_auth_ indicator	Indicates whether the authorization request was delayed because connectivity was interrupted. Possible values:
	
	■ Y: Deferred authorization
	
	■ N (default): Not a deferred authorization
	
	The value for this field corresponds to the following two data items in the TC 33 capture file[1]:
	
	■ First data item:
	  ● Record: CP01 TCR0
	  ● Position: 160-163
	  ● Field: Message Reason Code
	
	■ Second data item:
	  ● Record: CP01 TCR7
	  ● Position: 150-151
	  ● Field: Transit Transaction Type Indicator
	
	This field is supported only for mass transit transactions.
	
	See "Mass Transit Transactions," page 12.
		ics_auth (O)	String (1)

bill_zip	Postal code for billing address. Postal code must consist of 5 to 9 digits. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] **Example** A1B 2C3	ics_auth (O)	String (10)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
card_encrypted_data	Payment card data that was encrypted by the POS terminal. The encrypted data can be track data or keyed data and is in tag-length-value (TLV) format. A data set consists of encrypted data and the encryption attributes that are associated with the encrypted data. This field can contain multiple data sets. See Appendix D, "Encrypted Data," on page 59.	ics_auth (O) ics_credit (O for stand-alone credits)	String (255)
card_present	Indicates whether the card is present at the time of the transaction. Possible values: ■ N: Card is not present. ■ Y: Card is present.	ics_auth (R)	String (1)
card_type	Type of card to authorize. Possible values: ■ 001: Visa ■ 002: Mastercard ■ 003: American Express ■ 004: Discover ■ 005: Diners Club ■ 007: JCB	ics_auth (R for JCB. O for other card types.) **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.	String (3)
cashback_amount	Cashback amount in the acquirer's currency.	ics_auth (O) ics_auth_reversal (O)	Decimal (9)
cat_level	Type of cardholder-activated terminal. Possible values: ■ 1: Automated dispensing machine ■ 2: Self-service terminal ■ 3: Limited amount terminal ■ 4: In-flight commerce (IFC) terminal ■ 5: Radio frequency device ■ 6: Mobile acceptance terminal Some acquirers do not support all six values.	ics_auth (O)	Nonnegative integer (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5 General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
currency	Currency used for order. For possible values, see the *ISO Standard Currency Codes*.	ics_auth (R)	String (5)
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 payment card is illegible. ■ 9: CVN not imprinted on payment card.	ics_auth (O)	Nonnegative integer (1)
customer_cc_cv_ number	CVN. See the CVN information in *Credit Card Services for CyberSource through VisaNet Using the SCMP API*.	ics_auth (O)	Nonnegative integer (4)
customer_cc_expmo	Two-digit month in which payment card expires. Format: MM. Possible values: 01 through 12. Leading 0 is required.	ics_auth (R when keyed.)[2]	String (2)
customer_cc_expyr	Four-digit year in which payment card expires. Format: YYYY.	ics_auth (R when keyed.)[2]	Nonnegative integer (4)
customer_cc_number	Payment card number.	ics_auth (R when keyed.)	Nonnegative integer (20)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
debt_recovery_indicator	Flag for a mass transit transaction that indicates whether the purpose of the authorization is to recover debt. Possible values: ■ Y: Debt recovery transaction ■ N: Not a debt recovery transaction The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR7 ■ Position: 150-151 ■ Field: Transit Transaction Type Indicator This field is supported only for mass transit transactions. See "Mass Transit Transactions," page 12.	ics_auth (O)	String (1)
e_commerce_indicator	Type of transaction. For a card-present transaction, you must set this field to retail.	ics_auth (R)	String (13)
extended_credit_total_count	Number of months over which the cardholder can pay for the purchase. You can use this field when offering extended credit to a cardholder at a retail location. The cardholder provides this value. The issuer pays you for the purchase in one payment, and then the cardholder pays the issuer in the number of monthly payments specified by this value. This field is supported only on Cybersource through VisaNet for acquirers in South Africa.	ics_auth (O)	String (2)
grand_total_amount	Grand total for the order. You must include either this field or **offer0** and the offer-level field **amount**. For information about offers and grand totals, see *Getting Started with CyberSource Advanced for the SCMP API*.	ics_auth (See description)	Decimal (15)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2   This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
gratuity_amount	Gratuity or tip amount for restaurants when the card is present. Allowed only when **industry_datatype** is `restaurant`. When your customer uses a debit card or prepaid card, and you receive a partial authorization, the payment networks recommend that you do not submit a capture amount that is higher than the authorized amount. When the capture amount exceeds the partial amount that was approved, the issuer has chargeback rights for the excess amount. For information about partial authorizations, see *Credit Card Services for CyberSource through VisaNet Using the SCMP API*.	ics_bill (O)	Decimal (12)
ics_applications	Cybersource services to process for the request.	ics_auth (R)	String (255)
industry_datatype	***Mass Transit Transactions*** Indicates whether the transaction includes mass transit transaction (MTT) data. You must set this field to `transit` in order for MTT data to be sent to the processor. When this field is not set to `transit` or is not included in the request, Cybersource does not send MTT data to the processor. See "Mass Transit Transactions," page 12. ***Restaurant Transactions*** Indicates whether the transaction includes restaurant data. You must set this field to `restaurant` in order for restaurant data to be sent to the processor. When this field is not set to `restaurant` or is not included in the request, Cybersource does not send restaurant data to the processor.	ics_auth (R for MTT transactions.) ics_bill (R for restaurant transactions.)	String (10)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
jpo_jcca_terminal_id	Unique Japan Credit Card Association (JCCA) terminal identifier that is provided by Cybersource. The difference between this field and the **terminal_id** field is that you can define **terminal_id**, but **jpo_jcca_terminal_id** is defined by the JCCA and is used only in Japan. The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR9 ■ Position: 130-142 ■ Field: Terminal Identification Number	ics_auth (R when the terminal ID number is not recorded in your account. Otherwise, O.) ics_credit (R for stand-alone credits. O for follow-on credits.)	Integer (13)
jpo_jis2_track_data	Japanese Industrial Standard Type 2 (JIS2) track data from the front of the card.	ics_auth (O) ics_credit (O)	String (69)
merchandise_code	Identifier for the merchandise. This value must be right justified. In Japan, this value is called a *goods code*.	ics_auth (O)	Integer (7)
merchant_id	Your Cybersource merchant ID.	ics_auth (R)	String (30)
merchant_ref_number	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*.	ics_auth (R)	String (50)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
mobile_remote_ payment_type	Type of payment initiated from a cardholder's mobile device. Possible values:	ics_auth (O)	String (1)

■ 1: Customer-initiated remote purchase, face-to-face

■ 2: Customer-initiated remote purchase, e-commerce

■ 3: Customer-initiated remote purchase, mail order / telephone order

■ 4: Customer-initiated bill pay

■ 5: Customer-initiated top up

■ 6: Customer-initiated cash out

■ 7: ATM-triggered or agent-initiated cash out

■ 8: Merchant-initiated remote purchase, face-to-face

■ 9: Merchant-initiated remote purchase, e-commerce

This field is supported only for Mastercard transactions.

Cybersource through VisaNet
The value for this field corresponds to the following data in the TC 33 capture file[1]:

■ Record: CP01 TCR6

■ Position: 94

■ Field: Mastercard Mobile Remote Payment Program Indicator

---

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2   This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
mpos_device_type	Type of mPOS device. Possible values: ■ 0: Dongle ■ 1: Phone or tablet The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR6 ■ Position: 141 ■ Field: Mastercard mPOS Transaction This field is supported only for Mastercard transactions.	ics_auth (O)	String (1)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2   This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5 **General Card-Present Request-Level Fields (Continued)**

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payment_initiation_ channel	Mastercard-defined code that indicates how the account information was obtained. Possible values: ■ `00` (default): Card ■ `01`: Removable secure element that is personalized for use with a mobile phone and controlled by the wireless service provider; examples: subscriber identity module (SIM), universal integrated circuit card (UICC) ■ `02`: Key fob ■ `03`: Watch ■ `04`: Mobile tag ■ `05`: Wristband ■ `06`: Mobile phone case or sleeve ■ `07`: Mobile phone with a non-removable, secure element that is controlled by the wireless service provider ■ `08`: Removable secure element that is personalized for use with a mobile phone and not controlled by the wireless service provider; example: memory card ■ `09`: Mobile phone with a non-removable, secure element that is not controlled by the wireless service provider ■ `10`: Removable secure element that is personalized for use with a tablet or e-book and is controlled by the wireless service provider; examples: subscriber identity module (SIM), universal integrated circuit card (UICC) ■ `11`: Tablet or e-book with a non-removable, secure element that is controlled by the wireless service provider	ics_auth (O)	String (2)

continued on next page...

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payment_initiation_ channel (*continued*)	■ `12`: Removable secure element that is personalized for use with a tablet or e-book and is not controlled by the wireless service provider ■ `13`: Tablet or e-book with a non-removable, secure element that is not controlled by the wireless service provider This field is supported only for Mastercard.		
pos_entry_mode	Method of entering payment card information into the POS terminal. Possible values: ■ `contact`: Read from direct contact with chip card. ■ `contactless`: Read from a contactless interface using chip data. ■ `keyed`: Manually keyed into POS terminal. ■ `msd`: Read from a contactless interface using magnetic stripe data (MSD). ■ `swiped`: Read from payment card magnetic stripe. The `contact`, `contactless`, and `msd` values are supported only for EMV transactions. See "Europay, Mastercard, Visa (EMV)," page 10.	ics_auth (R)	String (11)
sales_slip_number	Transaction identifier that you generate. In Argentina, the value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR9 ■ Position: 8-15 ■ Field: Field Purchase Receipt Number In Japan, the value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR9 ■ Position: 143-147 ■ Field: Sales Slip Number	ics_auth: ■ R in Argentina. ■ R in Japan. ■ Otherwise, not used. ics_credit: ■ R for follow-on credits and stand-alone credits in Argentina. ■ R for stand-alone credits in Japan. ■ Otherwise, not used.	In Argentina: Integer (8) In Japan: Integer (5)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.
2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_zip	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] **Example** 12345-6789 When the shipping country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] **Example** A1B 2C3	ics_auth (R when shipping address information is included in the request and shipping to the U.S. or Canada; otherwise, O.)	String (10)
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; cannot use contact to read chip cards. For an EMV transaction, the value of this field must be 4 or 5. See "Europay, Mastercard, Visa (EMV)," page 10.	ics_auth (O)	Integer (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length

terminal_compliance	Flag that indicates whether the terminal is compliant with standards mandated by the Reserve Bank of India for card-present domestic transactions in India. Format:
	
	■ First character indicates whether the terminal supports terminal line encryption (TLE). Possible values:
	   ● `1`: Not certified
	   ● `2`: Certified
	
	■ Second character indicates whether the terminal supports Unique Key Per Transaction (UKPT) and Derived Unique Key Per Transaction (DUKPT). Possible values:
	   ● `1`: Not certified
	   ● `2`: Certified
	
	Example `21` indicates that the terminal supports TLE but does not support UKPT/DUKPT.
	
	You and the terminal vendors are responsible for terminal certification. If you have questions, contact your acquirer.
	
	This field is supported only for Mastercard transactions.
	
	Cybersource through VisaNet
	The value for this field corresponds to the following data in the TC 33 capture file[1]:
	■ Record: CP01 TCR6
	■ Position: 92-93
	■ Field: Mastercard Terminal Compliance Indicator
		ics_auth (R for card-present transactions in India. Otherwise, not used.)	Integer (2)

---

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5 **General Card-Present Request-Level Fields (Continued)**

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
terminal_id	Identifier for the terminal at your retail location. A list of all possible values is stored in your Cybersource account. When terminal ID validation is enabled for your Cybersource account, the value you send for this field is validated against the list each time you include the field in a request. To enable or disable terminal ID validation, contact Cybersource Customer Support. When you do not include this field in a request, Cybersource uses the default value that is defined in your Cybersource account.	ics_auth (O)	String (8)
transaction_local_date_time	Date and time at your physical location. Format: YYYYMMDDhhmmss, where: YYYY = year MM = month DD = day hh = hour mm = minutes ss = seconds The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR9 ■ Position: 16-21 ■ Field: Local Date In Argentina: ■ When you do not include this field, the value for this field is generated based on the time zone recorded in your account. ■ When you do not include this field, and no time zone is recorded in your account, the value for this field is generated based on GMT when the request is received.	ics_auth (R in Argentina when the time zone is not recorded in your account. Otherwise, O.)	String (14)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2 This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 5   General Card-Present Request-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length

transportation_mode	Mode of transportation or type of transportation-related payment. Possible values:
	
	■ 00: Use this value for:
	  ● Debt recovery
	  ● More than one transportation mode
	  ● Unknown transportation mode
	■ 01: Urban bus
	■ 02: Interurban bus
	■ 03: Light train mass transit
	■ 04: Train
	■ 05: Commuter train
	■ 06: Water-borne vehicle
	■ 07: Toll
	■ 08: Parking
	■ 09: Taxi
	■ 10: High-speed train
	■ 11: Rural bus
	■ 12: Express commuter train
	■ 13: Paratransit
	■ 14: Self-driving vehicle
	■ 15: Coach
	■ 16: Locomotive
	■ 17: Powered motor coach
	■ 18: Trailer
	■ 19: Regional train
	■ 20: Inter-city transportation
	■ 21: Funicular train
	■ 22: Cable car
	
	This field is supported only for mass transit transactions.
	
	See "Mass Transit Transactions," page 12.
	
	The value for this field corresponds to the following data in the TC 33 capture file[1]:
	
	■ Record: CP01 TCR7
	■ Position: 153-154
	■ Field: Transportation Mode Indicator
		ics_auth (O)	String (2)

---

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

2   This field is optional when your Cybersource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 16. **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 6   General Card-Present Offer-Level Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
amount	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.	ics_auth (See description)	Decimal (15)
merchant_product_ sku	Product identifier code.	ics_auth (R when **product_code** is not `default` or one of the values related to shipping and/or handling.)	String (15)
product_code	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 for CyberSource through VisaNet 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*.	ics_auth (O)	String (30)
product_name	Name of product.	ics_auth (R when **product_code** is not `default` or one of the values related to shipping and/or handling.)	String (30)

Table 6   General Card-Present Offer-Level Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
quantity	Default is `1`.	ics_auth (R when **product_code** is not `default` or one of the values related to shipping and/or handling.)	Nonnegative integer (10)

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.
		ics_auth (O)	Decimal (15)

P2PE Request Fields

Table 7   P2PE Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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 13.	ics_auth (R for authorizations that use Bluefin PCI P2PE) ics_credit (R for stand-alone credits that use Bluefin PCI P2PE)	String (3072)
encrypted_payment_descriptor	Format of the encrypted payment data. The value for Bluefin PCI P2PE is Ymx1ZWZpbg==. See "PCI P2P Encryption with Bluefin," page 13.	ics_auth (R for authorizations that use Bluefin PCI P2PE) ics_credit (R for stand-alone credits that use Bluefin PCI P2PE)	String (128)

Reply Fields

Table 8   Reply Fields

Field	Description	Returned By	Data Type & Length
emv_reply_chip_validation_results	Cryptogram validation results returned by the entity or service specified in **emv_reply_chip_validation_type**. Possible values: ■ `A`: Application cryptogram is valid, but the application transaction counter (ATC) is outside the allowed range. (A large increase in ATC values can indicate data copying or other fraud.) ■ `C`: Chip validation was completed successfully. ■ `E`: Application cryptogram is valid, but the ATC indicates possible replay fraud. ■ `F`: Format error in the chip data. ■ `G`: Application cryptogram is valid but is not a valid authorization request cryptogram (ARQC). ■ `I`: Application cryptogram is invalid. ■ `T`: Application cryptogram is valid, but terminal verification results (TVR) or card verification results (CVR) are invalid. ■ `U`: Application cryptogram could not be validated because of a technical error. This field is returned only for Mastercard near field communication (NFC) authorizations that use payment network tokens on Cybersource through VisaNet.	ics_auth	String (1)

1   The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Table 8   Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
emv_reply_chip_ validation_type	Entity or service that provided the validation results returned in the **emv_reply_chip_ validation_results** field. Possible values: ■ `02`: Mastercard pre-validation service. The Mastercard authorization platform validated the cryptogram before the issuer received the authorization request. ■ `03`: Mastercard stand-in service. The Mastercard authorization platform validated the cryptogram because the issuer was not available. ■ `50`: Issuer. ■ `90`: Chip fall-back transaction downgrade process. The chip could not be read. This field is returned only for Mastercard near field communication (NFC) authorizations that use payment network tokens on Cybersource through VisaNet.	ics_auth	String (2)
emv_reply_ combined_tags	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 "Europay, Mastercard, Visa (EMV)," page 10. For information about the individual tags, see the "Application Specification" section in the *EMV 4.3 Specifications*: http://emvco.com Information in this guide about EMV applies to payment card processing and PIN debit processing. All other information in this guide applies only to payment card processing.	ics_auth ics_auth_reversal ics_pin_debit_credit ics_pin_debit_purchase ics_pin_debit_reversal	String (252)
encrypted_ payment_error_code	Error code returned by Bluefin when the decryption fails. See Appendix C, "Bluefin PCI P2PE Error Codes," on page 58.	ics_auth ics_credit	String (4)
encrypted_ payment_reference_ id	Unique transaction identifier returned by Bluefin. You can use this value for tracking and reporting. See "PCI P2P Encryption with Bluefin," page 13.	ics_auth ics_credit	Integer (25)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Table 8   Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
issuer_pin_request	Value of `1` in this field indicates that the issuer requires a PIN. When you request an authorization for a card-present transaction but do not include a PIN in the request, the issuer can require the PIN. To complete the authorization: 1 Request a PIN from the customer. 2 Send a duplicate authorization request that includes the PIN and the **emv_request_ repeat** field. This field is supported only for Mastercard transactions.	ics_auth	String (1)
payment_account_ reference	Visa-generated reference number that identifies a card-present transaction for which you provided one of the following: ▪ Visa primary account number (PAN) ▪ Visa-generated token for a PAN This reference number serves as a link to the cardholder account and to all transactions for that account. ***Cybersource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ▪ Record: CP01 TCR8 ▪ Position: 79-110 ▪ Field: Payment Account Reference	ics_auth ics_auth_reversal	String (32)
sales_slip_number	Transaction identifier. 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.	ics_auth	Integer (5)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. Cybersource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment networks.

Examples

Authorization and Capture Using Swiped Track Data

Example 1   Request Message: Authorization Using Swiped Track Data

```
merchant_id=Merchant123
merchant_ref_number=ABC123
currency=usd
grand_total_amount=150.00
pos_entry_mode=swiped
card_present=Y
terminal_capability=2
track_data=%B4111111111111111^SMITH/BETTY^1312101976110000868000000?
card_type=001
ics_applications=ics_auth
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
third_party_certification_number=123456789012
merchant_transaction_identifier=1234265133532AB
```

Example 2   Reply Message: Authorization 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=150.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_time=2020-04-12T19:45:25Z
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=016153570198200
auth_card_category=A
auth_card_group=0
receipt_number=260371
```

Example 3   Request Message: Capture of Authorization That Used Swiped Track Data

```
merchant_id=Merchant123
merchant_ref_number=ABC123
currency=usd
grand_total_amount=150.00
ics_applications=ics_bill
auth_request_id=0305782650000167905080
third_party_certification_number=123456789012
```

Example 4   Reply Message: Capture of Authorization That Used Swiped Track Data

```
merchant_ref_number=ABC123
request_id=3342599254000176056442<
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_request_time=2020-04-13T17:16:15Z
bill_bill_amount=150.00
bill_trans_ref_no=3341645177430176056470
```

Sale Using Swiped Track Data

Example 5   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=16121200XXXX00000000?*
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
merchant_transaction_identifier=1234265133532AB
```

Example 6   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_time=2020-08-10T224757Z
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 7   Request Message: Sale Using Keyed Data

```
merchant_id=JanesPlants
merchant_ref_number=ABC123
bill_zip=123456789
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=2020
card_type=001
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
ignore_avs=yes
ignore_bad_cv=yes
merchant_transaction_identifier=1234265133532AB
```

Example 8   Reply Message: Sale Using Keyed 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_time=2020-08-10T224757Z
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 with Balance Inquiry

Example 9   **Request Message: Sale Using Keyed Data with Balance Inquiry**

```
merchant_id=Merchant123
merchant_ref_number=ABC123
bill_zip=481042201
currency=usd
grand_total_amount=140.00
pos_entry_mode=keyed
card_present=Y
terminal_capability=2
customer_cc_number=6011111111111111
customer_cc_expmo=12
customer_cc_expyr=2020
card_type=004
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
auth_partial_auth_indicator=true
ignore_avs=yes
ignore_bad_cv=yes
third_party_certification_number=123456789012
merchant_transaction_identifier=123456789012345
```

Example 10   Reply Message: Sale Using Keyed Data with Balance Inquiry

```
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=140.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_time=2020-04-12T19:45:25Z
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=016153570198200
auth_account_balance=45.65
auth_card_category=DI
auth_account_balance_currency=usd
auth_account_balance_sign=positive
auth_card_group=0
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_request_time=2020-04-12T19:45:27Z
bill_bill_amount=140.00
bill_trans_ref_no=1094820975023470
receipt_number=260371
```

Sale Using EMV Technology with a Contact Read

Example 11   **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=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
    ***?*;4111111111111111=16121200XXXX00000000?*
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
emv_request_combined_tags=9F33032040009505000000000009F3704518823719F100
    706011103A000009F26081E1756ED0E2134E29F36020015820200009C01009F1A020
    8409A030006219F02060000000020005F2A0208409F0306000000000000
emv_request_card_sequence_number=001
merchant_transaction_identifier=1234265133532AB
```

Example 12   Reply Message: Sale 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_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_time=2020-08-10T224757Z
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
    706011103A000009F26081E1756ED0E2134E29F36020015820200009C01009F1A020
    8409A030006219F02060000000020005F2A0208409F0306000000000000
```

Sale Using EMV Technology with a Contactless Read

Example 13   **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=%B4111111111111111^SMITH/BETTY^16121200123456789012**XXX***
    ***?*;4111111111111111=16121200XXXX00000000?*
ics_applications=ics_auth,ics_bill
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
emv_request_combined_tags=9F330320400095050000000009F3704518823719F100
    706011103A000009F26081E1756ED0E2134E29F36020015820200009C01009F1A020
    8409A030006219F02060000000020005F2A0208409F0306000000000000
emv_request_card_sequence_number=001
auth_capture_date=0823
merchant_transaction_identifier=1234265133532AB
```

Example 14   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_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_time=2020-08-10T224757Z
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=852734
emv_reply_combined_tags=9F33032040009505000000000009F3704518823719F100
    706011103A000009F26081E1756ED0E2134E29F36020015820200009C01009F1A020
    8409A030006219F02060000000020005F2A0208409F0306000000000000
```

Authorization Using Bluefin PCI P2PE

Example 15   Request Message: Authorization Using Bluefin PCI P2PE

```
merchant_id=demomerchant
merchant_ref_number=demorefnum
bill_zip=123456789
currency=usd
grand_total_amount=75.00
pos_entry_mode=keyed
card_present=y
terminal_capability=2
encrypted_payment_data=02d700801f3c20008383252a363031312a2a2a2a2a2a2a2
a303030395e46444d532020202020202020202020202020202020202020202020205e323231
322a2a2a2a2a2a2a2a3f2a3b363031312a2a2a2a2a2a2a303030393d323231322a2a2a
a2a2a2a2a2a3f2a7a75ad15d25217290c54b3d9d1c3868602136c68d339d52d98423391
f3e631511d548fff08b414feac9ff6c6dede8fb09bae870e4e32f6f462d6a75fa0a178c
3bd18d0d3ade21bc7a0ea687a2eef64551751e502d97cb98dc53ea55162cdfa39543132
343932383030376299490100001a000731a8003
encryptedPayment_descriptor=Ymx1ZWZpbg==
ics_applications=ics_auth
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
ignore_avs=yes
ignore_bad_cv=yes
merchant_transaction_identifier=1234265133532AB
```

Example 16   Reply Message: Authorization Using Bluefin PCI P2PE

```
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_auth_amount=75.00
auth_auth_code=831000
auth_auth_avs=1
auth_auth_time=2020-08-10T224757Z
auth_auth_response=100
auth_trans_ref_no=1094820975023470
encrypted_payment_reference_id=120160922122091013107861
```

Restaurant Authorization and Capture with Gratuity

Example 17   Request Message: Restaurant Authorization

```
merchant_id=Merchant123
merchant_ref_number=ABC123
currency=usd
grand_total_amount=125.00
pos_entry_mode=swiped
card_present=Y
terminal_capability=2
track_data=%B4111111111111111^SMITHY/BRAD ^13121019761100008680000000?
card_type=001
ics_applications=ics_auth
e_commerce_indicator=retail
auth_partial_auth_indicator=Y
third_party_certification_number=123456789012
merchant_transaction_identifier=1234265133532AB
```

Example 18   Reply Message: Restaurant Authorization

```
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=125.00
auth_auth_code=831000
auth_auth_avs=2
auth_auth_time=2020-04-12T19:45:25Z
auth_auth_response=00
auth_trans_ref_no=1094820975023470
auth_payment_network_transaction_id=016153570198200
auth_card_category=A
auth_card_group=0
receipt_number=260371
```

Example 19   Request Message: Restaurant Capture with Gratuity

```
merchant_id=Merchant123
merchant_ref_number=ABC123
currency=usd
grand_total_amount=136.50
ics_applications=ics_bill
auth_request_id=0305782650000167905080
industry_datatype=restaurant
gratuity_amount=11.50
third_party_certification_number=123456789012
```

Example 20   Reply Message: Restaurant Capture with Gratuity

```
merchant_ref_number=ABC123
request_id=0305782650000167905080
ics_rcode=100
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
currency=usd
bill_rcode=100
bill_rflag=SOK
bill_rmsg=Request was processed successfully.
bill_bill_request_time=2020-04-13T17:16:15Z
bill_bill_amount=136.50
bill_trans_ref_no=3341645177430176056470
```

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 13. When an encryption error occurs:

■ The reply flag is set 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.

■ The value for the **encrypted_payment_error_code** field is set to the Bluefin PCI P2PE error code.

Table 9   Bluefin PCI P2PE Error Codes

Error Code	Description
1001	Generic or unknown error code.
1101 1102 1103 1104 1105	Internal system configuration setup error
1202	Device not found or device not recognized.
1203	Device not active.
1204	Invalid firmware version.
1303	All decryptions failed.
1404	Decryption failed for some other reason.
1406	Decrypted result did not include payment card information.

Encrypted Data

Use the **card_encrypted_data** field to include encrypted card data in your request. The encrypted data can be track data or keyed data and is in tag-length-value (TLV) format. A data set consists of encrypted data and the encryption attributes that are associated with the encrypted data. The **card_encrypted_data** field can contain multiple data sets. PIN data is optional because some networks no longer require the PIN, thereby making the **card_encrypted_data** field optional.

Format: Data set ID + Length of TLV sequence in bytes + [TLV, TLV, TLV, …]

2 characters (1 byte)	4 characters (2 bytes)	Variable length
Data set ID	Length of TLV sequence in bytes	TLV sequence

Example   01001F0101050205100073608103050002100001040103 1F1F08D65E
6B2922F58C63

Data Set ID (1 byte)	Length of TLV Sequence (2 bytes)	TLV Sequence (31 bytes)
01	001F	010105 02051000736081 03050002100001 040103 1F1F08D65E6B2922F58C63

Table 10   Tags for Encrypted Data

Tag	Description	Length in Characters
01	Key management scheme for the encryption data in this data set. Possible value: ■ 01: Acquirer working key (AWK) ■ 05: Derived unique key per transaction (DUKPT).	2
02	Key set identifier that identifies the key used for encryption.	6 to 11
03	Device ID and transaction counter. This value consists of a 19-bit device ID and 21-bit transaction counter.	10
04	Identifier for the encryption algorithm that is used to encipher either the encrypted data elements in this data set or the keys in the associated key management data element. Possible value: ■ 03	2
1F1F	Encrypted PIN data. This value is a PIN or numeric password, encrypted and formatted as a block of 16 hexadecimal digits. This tag contains the PIN data, which is optional because some networks no longer require the PIN. Your agreement with the debit networks determines whether the customer must provide a PIN.	16