

Ingenico ePayments

Planning Guide

October 2018



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

© 2018 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 Unpublished rights reserved under the copyright laws of the United States.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 6

About This Guide 7

Audience 7

Purpose 7

Conventions 7

Note, Important, and Warning Statements 7

Text and Command Conventions 8

Related Documents 8

Customer Support 8

Chapter 1 **Payment Types** 9

Direct Debits 9

Bank Cards 10

Global Bank Cards 10

Regional and Country-Specific Bank Cards 11

Risk Types 12

Compliance 12

Merchant Account Descriptor Requirements 12

Excessive Credit Card Chargebacks and Excessive Direct Debit Returned Items 13

Merchant Remittance Funding 13

Dormant and Closed Accounts 13

Chapter 2 **Business Implementation** 14

Countries and Currencies 14

Selecting Countries 14

Selecting Currencies 14

Planning Your Business Implementation	15
Contacting Your Account Representative	15
Providing Company Information	15
Signing the Merchant Agreement	15
Creating a Reserve Account	16
Opening Your CyberSource Account and Completing the Intake Process	16
Closing Your CyberSource Account	17

Chapter 3	Transaction Life Cycle	18
	Transactions and Events	18
	Transaction Life Cycle	19
	Order Tracking	20
	Merchant Reference Code	20
	Transaction Reference Number (Reconciliation ID)	20
	Request ID	20
	Forwarding the Transaction to the Processor	21
	Fulfilling the Order	21
	Expected Payment Receipt Times	22
	Exceptions	23
	Funding	23
	Timing of Funding	24
	Funding Exceptions	24
	Request IDs and Request Tokens	24
	Financial Reconciliation	25
	Financial Reports	25
	Collection Report	25
	Remittance Report	26
	Report Schedule	26
	Order Reconciliation	27
	Payment Submission Detail Report	27
	Payment Events Report	28

Chapter 4	Technical Implementation	30
	Guidelines for Displaying Bank Information	30
	Testing	30

Chapter 5	Direct Debits and Direct Debit Refunds	32
	Direct Debits	32
	Flow of Identifiers for Order Tracking for Direct Debits	33
	Payment Confirmation and Shipping Goods	34
	Direct Debit Reversals	35
	Using Chargebacks and Banking Reversal Codes for Reconciliation	35
	Design Considerations	37
	Web Site Modifications	37
	Direct Debit Refunds	38
	Types of Refunds	38
	Requesting a Follow-on Refund	38
	Flow of Identifiers for Order Tracking for Direct Debit Refunds	38
	Transaction Status Changes	40
	Reconciling a Refund	40

Chapter 6	Bank Cards	41
	Bank Card Types	41
	Online and Offline Processing	42
	Online Bank Card Flow	42
	Offline Bank Card Flow	43
	Reconciliation	45
	Bank Card Refunds	45
	Web Site Modifications	45
	API for Bank Card Implementation	45

Appendix A	Reason Codes	46
	Reason Codes for the Simple Order API	46

Index	48
--------------	-----------

Recent Revisions to This Document

Release	Changes
October 2018	Removed information about bank transfers and real-time bank transfers. CyberSource has developed a next generation Alternative Payments solution that replaces the Ingenico ePayments bank transfer and real-time bank transfer functionality. The Alternative Payments solution supports multiple kinds of bank transfer payment methods. Contact your account representative for details about using the platform.
September 2018	Changed the name of <i>Carte Bleue</i> to <i>Cartes Bancaires</i> .
May 2016	Renamed document to <i>Ingenico ePayments Planning Guide</i> .
April 2016	Renamed <i>Global Collect</i> to <i>Ingenico ePayments</i> . Moved Boleto Bancario information to the Boleto Bancario Processing Implementation Guide .
December 2014	Removed requirement to send request token fields with direct debit refunds. See the following sections: <ul style="list-style-type: none"> ■ "Requesting a Follow-on Refund," page 38 ■ "Flow of Identifiers for Order Tracking for Direct Debit Refunds," page 38

About This Guide

Audience

This guide is written for merchants who want to use the Ingenico ePayments processor to offer direct debit services and bank card processing to customers.

Purpose

This guide describes the business and technical implementations a merchant must complete in order to make direct debits and direct debit refunds.

Conventions

Note, Important, and Warning Statements



Note

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



Important

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



Warning

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

Text and Command Conventions

Convention	Usage
bold	<ul style="list-style-type: none"> Field and service names in text; for example: Include the ics_applications field. Items that you are instructed to act upon; for example: Click Save.
screen text	<ul style="list-style-type: none"> XML elements. Code examples and samples. Text that you enter in an API environment; for example: Set the davService_run field to <code>true</code>.

Related Documents

- The *Global Payment Service Developer Guide* ([PDF](#) | [HTML](#)) describes the tasks a merchant must complete in order to make direct debits and direct debit refunds.
- *Credit Card Services Using the Simple Order API* ([PDF](#) | [HTML](#)) describes the tasks you must complete to integrate the credit card services into your existing management system.
- *Credit Card Services Using the SCMP API* ([PDF](#) | [HTML](#)) describes the tasks you must complete to integrate the credit card services into your existing order management system.
- *Getting Started with CyberSource Advanced for the Simple Order API* ([PDF](#) | [HTML](#)) describes how to get started using the Simple Order API.
- *Getting Started with CyberSource Advanced for the SCMP API* ([PDF](#) | [HTML](#)) describes how to get started using the SCMP API.
- The *Classic Reporting Developer Guide* ([PDF](#) | [HTML](#)) describes how to download reports.

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>

Payment Types

Direct Debits

Customers provide their bank account information and authorize you to transfer money out of their accounts. Direct debits are used for domestic fund transfers only, so CyberSource provides you with a local bank account. When the local account receives payment, CyberSource funds your merchant bank account. Direct debits are similar to electronic checks used in the U.S.

CyberSource supports direct debits in Austria, Germany, the Netherlands, and Spain.

**Note**

Direct debit is a general term for the payment type and is used throughout the documentation. Direct debits have other names, depending on the country. For example, in Germany, one of the large direct debit systems is called *ELV*, which stands for *Elektronisches Lastschriftverfahren* and means electronic debit method.

A mandate is a signature or another form of permission that you obtain in order to transfer funds from a customer's account. In some countries the customer's bank requires a mandate in order to process a direct debit. Other banks may require a mandate if you want to dispute reversals. Contact CyberSource Customer Support for more information about mandate requirements in countries that support direct debits.

Direct debits are subject to extensive dispute rights and high dispute fees. You should research the rules as a part of your due diligence process because rules differ in each country.

Direct debit payments are also a fraud risk because identification and authentication requirements are weak. These payments are also a customer credit risk because no initial authorization verifies whether the bank account has sufficient funds. It is customary to delay shipping until you receive payment confirmation.

For more information about direct debits, see [Chapter 5, "Direct Debits and Direct Debit Refunds," on page 32.](#)

Bank Cards

Each bank card transaction is classified as either online or offline. See [Table 1, page 10](#). Bank cards can be either global or local.

- **Online**—when you submit an order, you receive an immediate confirmation of the availability of funds. Most common global bank cards are processed online. For online payment types, you typically start the process of order fulfillment soon after you receive confirmation of the order.
- **Offline**—when you submit an order you do not receive immediate confirmation of payment. You should not ship the goods until you receive this payment confirmation. Offline bank cards typically take five days longer than online cards to process and for you to receive payment confirmation. For direct debits, the processing time is typically two or three days.

Table 1 Online and Offline Payment Types

Online Payment Types	Offline Payment Types
American Express	Diners Club
Carta Si—Italian Visa-branded or Mastercard branded in-country bank card	Direct Debit
Cartes Bancaires—French Visa-branded or Mastercard-branded in-country bank card; for this card your capture requests must be for 0.99 euros or more	
Dankort—Danish Visa-branded in-country bank card	
Delta—U.K. Visa debit card	
Electron—European Visa debit card	
Eurocard—Regional brand of Mastercard	
JCB	
Laser Irish Visa-branded in-country bank card	
Mastercard	
Maestro U.K. in-country bank card	
Visa	

Global Bank Cards

Global bank cards are accepted worldwide:

- American Express
- Diners Club
- JCB

- Mastercard
- Visa

You might have already implemented processing for one of these global bank cards through a different payment processor that might not have multi-currency processing for supporting international payments. Consider supporting these cards through Ingenico ePayments for these reasons:

- Multi-currency processing: customers can pay in their local currency. Contact your CyberSource Customer Support representative to learn which currencies are supported.
- Single set of reports for all transaction activities originating in each country.

You do not have to move your existing domestic bank card processing away from your current processor. However, if you want to use Ingenico ePayments and are already processing international payments through another processor, you must have those transactions processed through Ingenico ePayments.

Except for Diners Club, global bank cards are authorized and settled online, resulting in low credit risk to you. Because Diners Club is an offline card outside of the U.S., you do not receive an immediate online authorization and bear significant credit risk for this card. For information about offline processing, see ["Bank Cards," page 10](#), and ["Offline Bank Card Flow," page 43](#).

With the global bank cards, customers have limited dispute rights. You bear fraud risk for global bank cards with the exception of Visa and Mastercard transactions that are covered by payer authentication.

For information about global bank cards, see [Chapter 6, "Bank Cards," on page 41](#).

Regional and Country-Specific Bank Cards

Although global bank cards are used extensively in Australia, Canada, and the U.S., many European customers prefer instead to use regional or country-specific bank cards. Even though customers can choose to pay with a global bank card, by showing that you support local bank cards, you can improve your store presence and sales. These regional cards use payment networks other than those of global bank cards, but processing is similar to global card processing.

Ingenico ePayments enables you to accept the following country-specific and regional bank cards:

- Cartes Bancaires—French Visa branded or Mastercard branded bank card. Using this card your capture requests must be for 0.99 euros or more
- Carta Si—Italian Visa branded or Mastercard-branded in-country bank card

- Dankort—Danish Visa branded in-country bank card
- Delta—U.K. Visa debit card
- Electron—European Visa debit card
- Eurocard—Regional brand of Mastercard
- Laser—Irish Visa-branded bank card
- Maestro—U.K. bank card

Country-specific bank cards are subject to chargeback rules, and you bear fraud risk. Because consumer dispute rules differ by country, you should thoroughly research the rules as a part of your due diligence.

Risk Types

With each type of payment comes a certain amount and type of risk:

- Credit risk—the customer does not have the required funds in the account to cover the payment. To avoid credit risk, do not ship the goods until the payment has been confirmed.
- Fraud risk—an unauthorized person is using the bank account or bank card.
- Consumer dispute rights—the customer disputes a charge against the bank account or bank card. You may be required to return the amount of the disputed charge to the customer's account. Disputes can create both administrative and financial costs for you.

Compliance

Accepting payments from a country other than your own requires that you observe the processing rules and practices of the payment systems in those countries. The following two sections outline specific areas of compliance. Other sections in this guide describe operational requirements that you must follow in order to be compliant.

Merchant Account Descriptor Requirements

The merchant account descriptor is a fixed text field that is associated with either a merchant credit card account or merchant direct debit services. The purpose of the descriptor is to communicate merchant name information to the customer to remind them of the circumstances that triggered the payment. Clearly stated, merchant descriptors

reduce the possibility of a credit card chargeback or a returned direct debit, which is similar to a credit card chargeback. Accordingly, the merchant descriptor displayed on the customer's statement should closely match the name on your web site. It is not good practice to consolidate multiple web sites into a single direct debit account or credit card account and use a generic descriptor that may or may not cover all offerings.

Excessive Credit Card Chargebacks and Excessive Direct Debit Returned Items

You are responsible for maintaining good customer support, rapid problem resolution, a high level of customer satisfaction, and a transaction management system that minimizes fraudulent transactions. Fulfilling these responsibilities prevents an excessive number of returned direct debits. Credit card chargebacks or direct debit returned items become excessive, CyberSource may require you to undertake business process changes to reduce their numbers. If chargebacks or returned items are not reduced to a satisfactory level, CyberSource may terminate the account.

Merchant Remittance Funding

In conjunction with the processing of direct debit transactions, you can request that CyberSource convert transaction proceeds to a another currency for funding into an operating account. The foreign exchange rate may be explicitly stated as a rate or implicitly stated as a transaction amount and a funded amount. The foreign exchange rate may also include an increase cover the foreign exchange risk, sales commissions, and handling costs.

Dormant and Closed Accounts

If a refund, credit, chargeback or direct debit return exceeds the available balance in your account, CyberSource may terminate your ability to process any further transactions.

Business Implementation

Countries and Currencies

Selecting Countries

You can process direct debits in many countries. Contact your CyberSource account representative for the current list. If you want to add any payment types, contact your CyberSource Technical Account Manager. CyberSource will provide you with pricing information and may need to collect additional information from you.

Selecting Currencies

Payments such as direct debits have currency restrictions:

- All the payments that originate from a particular country must be funded with a single currency and into a single bank account.
- During the intake process, you must inform CyberSource of the funding currency that you want to use for each processing currency.
- You will have a separate bank account for each funding currency, and you must provide CyberSource with detailed information of each funding bank account you use.

Planning Your Business Implementation

Contacting Your Account Representative

Contact your account representative to discuss your basic business needs:

- Payment types you want to accept
- Countries where you want to do business
- Currencies that you want to use to process payments and receive funds

CyberSource can recommend payment types to accept based on your business model and the countries where you want to do business. Based on this information, CyberSource quotes a price for services.

Providing Company Information

When you accept the quote you must provide information about your company, the company's financial status, and your projected transaction volumes by payment type and country.

Based on this information CyberSource assesses the risk of underwriting your account. The assessment takes approximately 2 weeks to complete. In this relationship CyberSource is the merchant account provider and bears the ultimate risk of any chargebacks, reversals, or returns.

Signing the Merchant Agreement

If CyberSource accepts the risk of underwriting your account, CyberSource supplies a merchant agreement. All business arrangements, including the terms and conditions relating to the reserve account, are identified in the agreement. The agreement is organized according to the payment types and the countries involved. As part of the agreement you are required to read this guide so that you understand the implications and requirements of the payment types and countries.

Creating a Reserve Account

As part of the agreement, you might be required to create a reserve account that covers chargebacks and credits in the event that your organization is unable to meet these obligations. The amount and type of reserve can vary depending on the payment type and other variables:

- A rolling 6-month reserve—each month CyberSource typically collects 5% to 15% of your sales activity for that month. At the end of the seventh month, CyberSource returns to you what was collected during the first month, and so on. This type of reserve takes into account the seasonal nature of your business.
- A prepaid reserve that you provide.
- A flat reserve that is a percentage of your volume, with a maximum amount.

If you plan to process bank cards, CyberSource typically requires a rolling reserve. If you plan to process direct debits, CyberSource typically requires a prepaid or flat reserve.

CyberSource is entitled to review and adjust the amount of the reserve regularly during the term of the agreement on the basis of actual risk and monetary volume associated with your CyberSource account.

Opening Your CyberSource Account and Completing the Intake Process

After the merchant agreement is endorsed, CyberSource opens and configures your account. CyberSource processes any required forms necessary to open your local bank account. In some circumstances CyberSource opens new terminal IDs and merchant IDs for online and offline card acceptance.



Important

When opening your account you must inform CyberSource if you plan to use multiple CyberSource merchant IDs. For example, you may have separate business units within your company each with a CyberSource merchant ID. You must have a separate processor merchant ID for each CyberSource merchant ID.

Your CyberSource account manager will work with you so that CyberSource has all the information it needs about the countries, currencies, payment types, and bank accounts that you will be using. CyberSource informs you when the local bank accounts are ready to receive funds from customers.

Closing Your CyberSource Account

To stop accepting payment types in a particular country or to close your CyberSource account, contact your CyberSource Technical Account Manager.

Transaction Life Cycle



Important

Bank card processing with Ingenico ePayments is similar to domestic bank card processing. Global bank card processing is not discussed at length here. CyberSource assumes that you already have a system for processing bank cards.

Transactions and Events

A *transaction* occurs when you request that CyberSource move money in the form of a payment or a refund. You initiate transactions.

An *event* is related to a transaction that you have submitted. You do not initiate events; banks initiate events.

For example, you submit a transaction to CyberSource for a direct debit. Later, a payment *event* occurs indicating that the bank has received the customer's payment.

CyberSource supplies two reports to help you keep track of your transactions and events:

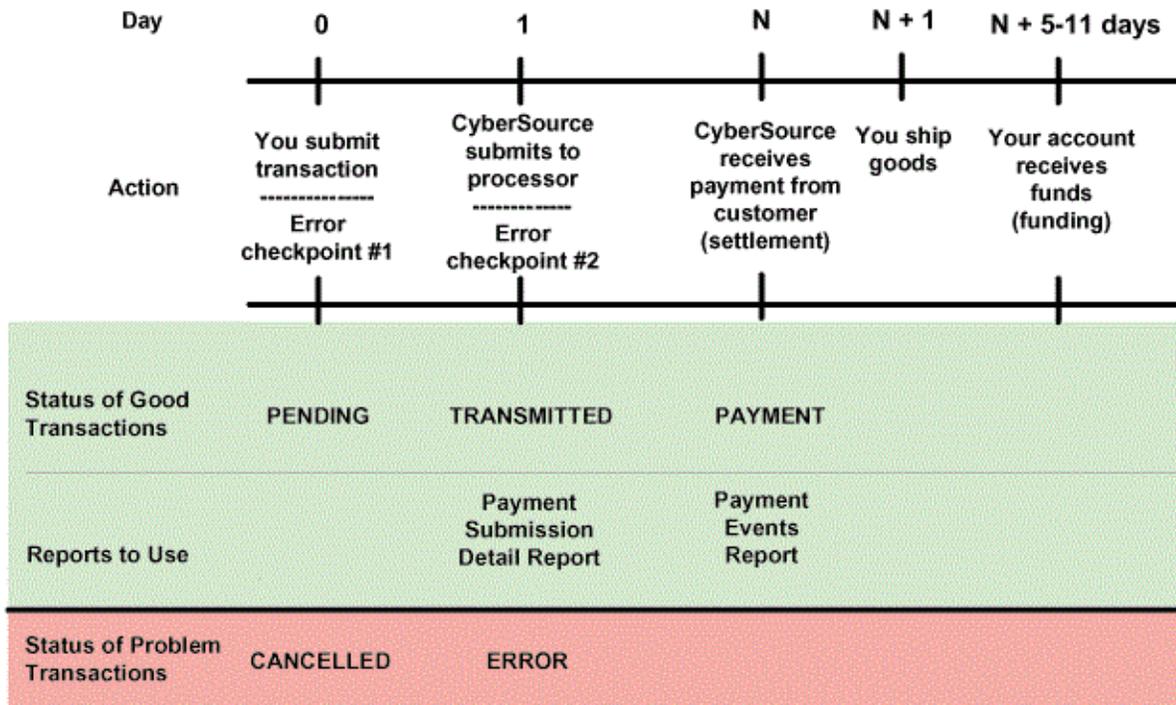
- Payment Submission Detail Report—for transactions
- Payment Events Report—for events

For more information see "[Order Reconciliation](#)," page 27.

Transaction Life Cycle

This section focuses on direct debits and their associated refunds. CyberSource provides several tools that help you keep track of your transactions and that indicate when to fulfill and reconcile your orders.

Figure 1 Transaction Life Cycle



When you submit the transaction to CyberSource, it immediately goes through error checkpoint #1. CyberSource ensures that the request has all the required fields and no invalid data. If the request has an error, CyberSource rejects it and you immediately receive notification in the reply. The transaction's status is set to CANCELLED.

If the request has no errors, the transaction's status changes to PENDING.

Search for the transaction in the Business Center. The Transaction Search Details page displays a transaction's status. You can search for one or more transactions using specific criteria. Basic information and current status of the transaction are displayed.

Order Tracking

After you submit your transaction, several identifiers become associated with it. You can use these identifiers to keep track of the transaction in the CyberSource reports and the Transaction Search Details screens in the Business Center:

- Merchant reference code (merchant reference number)
- Transaction reference number (reconciliation ID)
- Request ID
- Request token

Merchant Reference Code

You generate the merchant reference code and include it in the request. This field is a string and can contain a combination of data, such as your order ID and customer ID. The merchant reference code appears on all CyberSource daily reports. You can use it to search for the transaction in the [Business Center](#).

CyberSource recommends that you use a unique value for each order and that you use the same value for all requests that you send to CyberSource related to an order. For example, if you request a direct debit refund use the same merchant reference code for the direct debit refund that you used for the direct debit. This practice helps you track the order in your system and CyberSource's system.

Transaction Reference Number (Reconciliation ID)

CyberSource generates the transaction reference number (reconciliation ID) and returns it to you in the reply. CyberSource uses this number to track transactions with the payment processor. The value is guaranteed to be unique, and it appears in various reports.

**Note**

You can reconcile your orders with their corresponding payments by using either the merchant reference code or the transaction reference number.

Request ID

CyberSource generates a unique request ID for each request that you send and returns the ID in the reply. The request ID is useful if you need to discuss a specific request with CyberSource Customer Support.

You can use the request ID from the original request to request a refund. You include the request ID of the payment, and CyberSource uses that value to find information about the payment.

Forwarding the Transaction to the Processor

How a transaction gets processed depends on the transaction type and the processor. The following table describes the status of each transaction type.

Table 2 Transaction Processing

Type of Transaction	Payment Status
Direct Debit or Direct Debit Refund	<ul style="list-style-type: none"> ■ Transaction bypasses error checkpoint #2. ■ Transaction is sent to the processor. ■ Status changes to TRANSMITTED. ■ Transaction appears in the Payment Submission Detail Report.

All transactions that you submit before 12:00 a.m. Pacific time are reported in the next day's Payment Submission Detail Report. The report is usually available for download by 6.00 a.m. Pacific time. For more information, see "[Payment Submission Detail Report](#)," [page 27](#).

Fulfilling the Order

For offline payment methods such as direct debits or offline bank cards, you should ship the goods after you receive the payment confirmation. If a transaction status is ERROR or ON HOLD, do not ship the goods until the error is resolved and the customer's payment is received. Inform customers when they place their orders that you do not ship until you receive payment confirmation.

Use the Payment Events Report to determine when the customer's payment is received. When the payment is received, CyberSource changes the transaction's status to PAYMENT. The Payment Events Report will contain a line item for that transaction with the event type set to *Payment*. For all payment methods except direct debits, this status indicates that you can ship the goods.

For direct debits you should wait an additional 3 to 4 business days before shipping the goods. During this time, monitor the Payment Events Report to ensure that the direct debit has not been reversed.

The payment receipt times vary depending on the payment method and other variables. Monitor the Payment Events Report daily to keep track of incoming payments for orders that need to be fulfilled. For information about when to expect payment for each payment

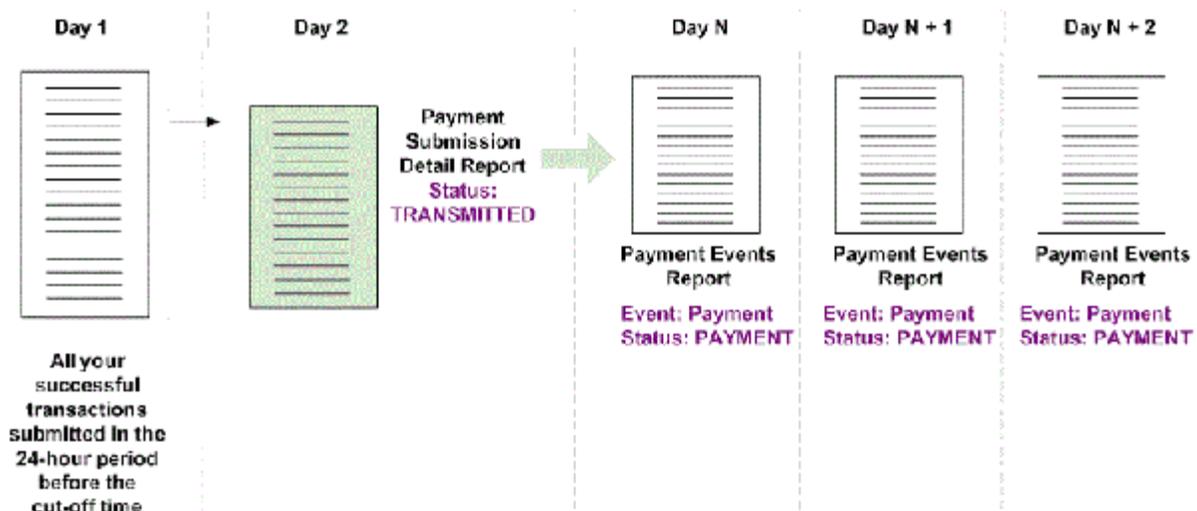
type, see ["Expected Payment Receipt Times," page 22](#). For more information about the Payment Events Report, see ["Payment Events Report," page 28](#).



Note

For all countries the Ingenico ePayments settlement processing does not occur on Saturday or Sunday. A Payment Events Report that you download on Sunday or Monday generally does not contain any payment events for Ingenico ePayments.

Figure 2 Fulfilling the Order



Refunds go through the same process as described previously. You can view refunds being settled with the customer by monitoring the Payment Events Report. When CyberSource receives notification from the processor that the refund has been processed, CyberSource changes the refund transaction's status to REFUND. The next day's Payment Events Report contains a line item for that refund transaction with the event type set to *Refund*.

Expected Payment Receipt Times

Direct debit payments and online bank card payments are processed through the customer's bank in 2 or 3 business days. Offline bank card payments are processed in 5 business days.

Exceptions

After a transaction is settled, which is when the customer's payment is received, several exceptions can occur. They are displayed in the Payment Events Report:

- Direct debits—a reversal occurs when the customer claims that the money was taken in error or without permission, or when there are insufficient funds in the customer's account. The event in the Payment Events Report is *Reversal*. For more information see "[Direct Debit Reversals](#)," page 35.
- If a chargeback occurs for a bank card, the event in the Payment Events Report is *Chargeback*. Before a chargeback occurs, a Request For Information (RFI) occurs. This is the first step in the chargeback process. It occurs when the customer's bank contacts the payment processor requesting information about the merchant and the transaction. CyberSource Customer Support sends you a notification email when an RFI occurs.

You should monitor the Payment Events Report daily for these events and update your systems accordingly. In the Business Center, a table at the bottom of the Transaction Search Details screen for the original transaction lists the history of events. To request an inquiry for a transaction, go to the [CyberSource Support Center](#).

Funding

When a transaction's status is PAYMENT or REFUND, the next step is funding. During this process your bank account receives the funds due to you. During funding any reserves, reversals and refunds that you owe are subtracted from the funding amount.

Funding and settlement are separate occurrences for direct debits. For bank cards, funding and settlement are the same thing. When the customer's bank pays (settlement), the money transfers directly to your bank account (funding). For direct debits, settlement occurs when the customer's payment is received in a local account that CyberSource sets up for you. Funding occurs weekly and CyberSource deposits all your payments for the week minus any reserves, reversals, or refunds.

When a transaction is funded, it's status does not change from its current state of PAYMENT or REFUND. When funding happens, no event appears in the Payment Events Report. Instead, you can assume that the transaction will be funded 4-11 days after its status changes to PAYMENT or REFUND. You can see the status of the transaction in the Transaction Search Details screen.

Timing of Funding

For the Ingenico ePayments, funding occurs weekly. If you have a high order volume you might be eligible to fund twice a week. Depending on the country, funding can occur at different times during the week.

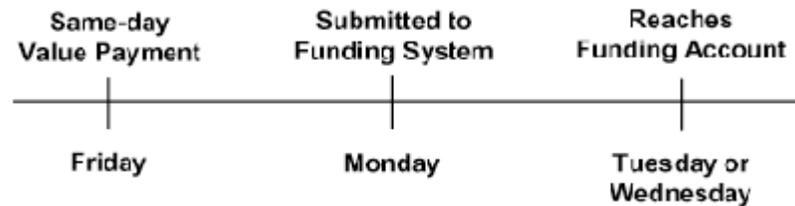


Note

Funding does not occur on weekends and holidays. All days listed are business days.

The Ingenico ePayments processor starts the funding process on Friday of each week. Your merchant bank account is funded with a same-day-value transaction that is initiated on Tuesday of the following week. You should receive funds on Tuesday or Wednesday.

Figure 3 Ingenico ePayments Funding Process



Funding Exceptions

If the net amount to be funded in the weekly period is less than 100 euros or equivalent, the funding is delayed and processed when the funding amount reaches 100 euros. If a failure occurs during the funding cycle, CyberSource contacts you. CyberSource funds those transactions in the next funding cycle.

If CyberSource detects transactions that are suspicious, your funding can be put on hold until CyberSource can discuss the transactions with you.

Request IDs and Request Tokens

Request IDs and request tokens are identifiers that CyberSource includes in the replies for all services. You must store the contents of the request ID and request token fields because you need these values when you send a request for a follow-on service.



Important

Although the names of the request ID and request token fields that you receive are the same in each reply, the contents of the fields are different.

Financial Reconciliation

Financial reconciliation is the process of verifying that the funds CyberSource deposited into your bank account have been received by your bank.

Financial Reports

For financial reconciliation for transactions performed with the Ingenico ePayments processor, you receive two reports in PDF format: the Collection Report and the Remittance Report. Each report describes the movement of funds into your funding accounts. These reports are available in the [Business Center](#).

Collection Report

The Collection Report describes the total amount of the payments you received in each foreign currency, the amount for each foreign currency, and the exchange rates used.

[Figure 4](#) shows an example of a Collection Report with activity in eight foreign currencies. The report number lists the contract number just to the right of the year. The term *contract number* is synonymous with *account number* or *merchant agreement number*. The report example is for account number 1935.

Figure 4 Collection Report Example

Collection Report

Report number:	2003 - 1935 - 017			
Report date:	24-04-2003			
Report period:	18-04-2003 to 24-04-2003			
Description		Exch. rate	Curr	Amount
Reported payments in CHF	3,424.00	0.593981	USD	2,033.79
Reported payments in CZK	3,680.92	0.027876	USD	102.61
Reported payments in DKK	2,175.00	0.117595	USD	255.77
Reported payments in EUR	6,019.85	0.873193	USD	5,256.49
Reported payments in FRF	1,272.00-	0.133011	USD	169.19-
Reported payments in GBP	626.00	1.414872	USD	885.71
Reported payments in NOK	4,710.00	0.112921	USD	531.86
Reported payments in SEK	1,710.00	0.095655	USD	163.57
Total USD				9,060.61

Remittance Report

The Remittance Report, [Figure 5](#), describes the total amount of the payment transfer made to your merchant bank account. The information in the Remittance Report example is consistent with the Collection Report example.

Figure 5 Remittance Report Example

Remittance Report					
Date: 24-04-2003					
	Contract	Description	Currency	Amount	
Collection Reports					
20031935-017-USD	1935	18-04-2003 24-04-2003	USD	9,060.61	
				9,060.61	
R0004100			Total USD	9,060.61	
The amount in USD will be transferred to your account 3016163416, First Fidelity Bank, Newark					

Report Schedule

The availability of the Collection Report and Remittance Report depends on whether your settlement period is on a weekly schedule or a twice-weekly schedule.

Table 3 Schedule for Collection Report and Remittance Report

Schedule	Settlement Period	Collection Report Available	Remittance Report Available
Weekly	Saturday to Friday	Monday	Tuesday
Twice-weekly	Wednesday to Friday	Monday	Tuesday
	Saturday to Tuesday	Wednesday	Thursday

Order Reconciliation

Order reconciliation is the process of verifying that all successful orders that you have initiated with CyberSource are settled, shipped, and funded. In general, your transactions are split into the categories in the table below. CyberSource provides you with various tools to help you determine when a transaction is in a particular category or point in its life cycle. These tools include:

- Payment Submission Detail Report
- Payment Events Report

These reports are described in the following sections.

Table 4 Reconciliation Reports

Transaction Categories	Status	Available Tools to Identify Transactions in the Category
Awaiting payment	PENDING or TRANSMITTED	Payment Submission Detail Report: The presence of the transaction in the report indicates the status is TRANSMITTED. PENDING transactions do not appear in this report.
Received payment Note Your own system must monitor whether the goods have been shipped. For direct debits, you must wait 3 or 4 days to ensure that there is no reversal.	PAYMENT	Payment Events Report: Look for a Payment event.

The Payment Submission Detail Report and the Payment Events Report are daily reports detailing transactions that had a status change in the past 24 hours. If you use these reports you must monitor them daily.

Payment Submission Detail Report

This daily report includes all transactions that you submitted to CyberSource in the past 24 hours without any errors. See "[Forwarding the Transaction to the Processor](#)," page 21, for more information. For Ingenico ePayments the report includes:

- Bank card captures and credits
- Direct debits and direct debit refunds

You can use the report to:

- Confirm the orders that you have submitted and that will be processed
- Trigger order fulfillment for online payment types—online bank cards
- Estimate settlement amounts and revenue

The report contains transactions that you submit from 12:00 a.m. to 12:00 a.m. Pacific time. The report is typically available for download by 6:00 a.m. Pacific time the next day.



Note

If you use CyberSource services for any payment services other than Ingenico ePayments, including all credit card and check processing, those transactions also appear in this report.

Each transaction entry in the report includes:

- Request ID
- Merchant reference code
- Transaction reference number (reconciliation ID)
- Payment type
- Currency code
- Amount
- CyberSource service that was called
- Payment processor

For information about the format of the report and how to download it, see the [Classic Reporting Developer Guide](#).

Payment Events Report

This report describes events that occurred for your transactions in the past 24 hours. You can use this report:

- Trigger order fulfillment for offline payment types—direct debits and offline bank cards
- Reconcile confirmed payments and refunds to orders for all of the Ingenico ePayments payment types



Note

If you use CyberSource for specific payment service, such as TeleCheck electronic checks, those transactions are also described in this report.

The Payment Events report is available for download by 6:00 a.m. Pacific time the next day.

Each event that occurs has a separate record in the report. The types of events listed in the report are:

- Payments
- Refunds
- Chargebacks
- Reversals
- Corrections
- Any unanticipated events reported by the payment processor

Each record includes the request ID, merchant reference code, transaction reference number (reconciliation ID), type and date of the event, and other event details.

For information about the format of the report and how to download it, see the [Classic Reporting Developer Guide](#).

Important Notes about Payment Events Report Generation

The report is generated each day that CyberSource receives a data file from the processor before CyberSource's cut-off time. Because CyberSource does not receive a data file from the processor on weekends or holidays, the report that you download on Mondays will contain information for multiple days of processing. Ensure that your implementation can handle reports that span multiple processing days.

If the generation of the report is delayed on a particular day, you are notified. Because a report generated after a delay can span more than one day, ensure that you can track the delayed reports.

CyberSource regenerates the entire report, not just the selected transactions that need to be regenerated. You are notified as soon as the new version of the report is available. Ensure that your implementation can recognize and process only the transactions that were modified or added to the report.

Technical Implementation

**Note**

For API information for direct debits and their associated refunds, see the *Global Payment Service Developer Guide*.

For API information for the various types of bank cards, see *Credit Card Services Using the Simple Order API* or *Credit Card Services Using the SCMP API*.

Guidelines for Displaying Bank Information

When you implement direct debits you must display bank account information to customers or request it from them. The representation of the account information varies from country to country. To minimize delays or errors in transferring funds, CyberSource recommends that you pay attention to how the bank account information is displayed in each country. For example, some countries require only a bank account number, but other countries also require a special bank code.

Testing

CyberSource recommends that you test your implementation to ensure that you are sending direct debit requests to, and handling replies from, the CyberSource services correctly. CyberSource performs the same basic validation checks that are performed for production transactions. Test transactions are *not* forwarded to the payment processor.

The requirements for test transactions are:

- Use your regular CyberSource merchant ID to perform testing.
- Match the country and currency information.
- When testing the Simple Order API, use the test URL:
<https://ics2wstest.ic3.com/commerce/1.x/transactionProcessor>
- When testing the SCMP API, use the CyberSource test server:
<https://ics2test.ic3.com>

Using specific amounts in your test transactions to trigger specific responses enables you to generate the responses that your system must process.

For information about amounts and decline (error) responses returned by the simulator for both the Simple Order API (reason code) and the SCMP API (rflag and rmsg description), see the [Global Payment Service Developer Guide](#).

Direct Debits and Direct Debit Refunds

Direct Debits

**Note**

Contact CyberSource Customer Support for a full list of supported countries.

For direct debits, customers provide their bank account information and authorize you to transfer money out of their accounts. Because direct debits are used only for in-country fund transfers, CyberSource provides you with local country bank accounts. When the account receives payment, CyberSource funds your merchant bank account. Direct debits are similar to electronic checks used in the U.S.

**Note**

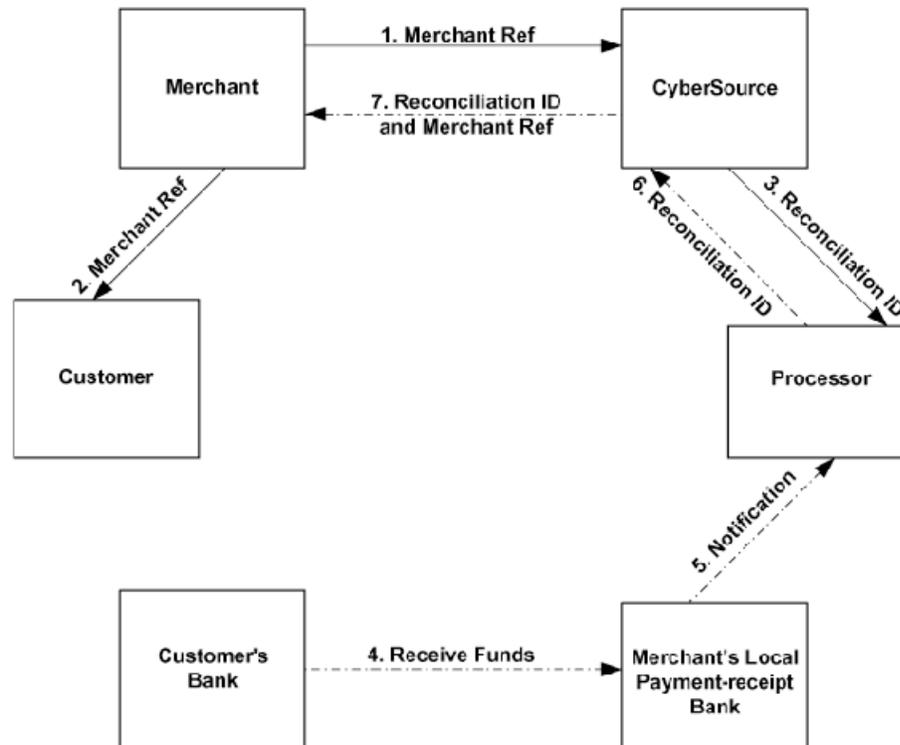
Depending on the country, direct debits can be called by other names. For example, in Germany, one of the large direct debit systems is called *ELV*, which stands for *Elektronisches Lastschriftverfahren*, and which means electronic debit method.

When the customer's payment is received, CyberSource matches the payment to the customer's order and communicates the payment information to you in the Payment Events Report.

Flow of Identifiers for Order Tracking for Direct Debits

The following figure shows the flow of information and identifiers that occurs for a direct debit.

Figure 6 Direct Debit Identifier Flow



In the figure, solid lines (steps 1-3) indicate actions that happen during the purchase process. Dashed lines (steps 4-7) indicate actions that happen during payment and reconciliation.

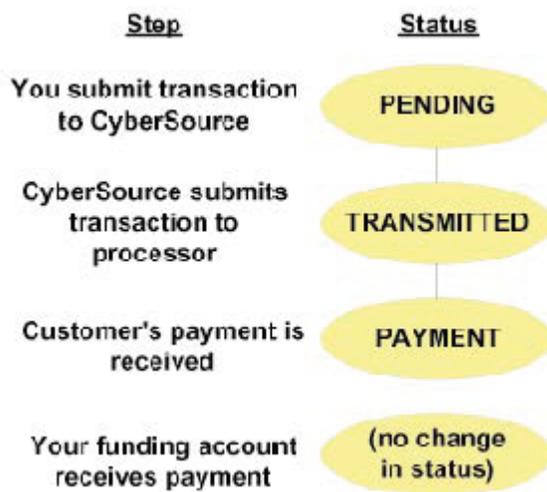
For definitions of identifiers, see ["Order Tracking," page 20](#).

- 1** The customer chooses to pay by direct debit. You gather the bank information and send it with your merchant reference code in a request to CyberSource.
- 2** You send a confirmation to the customer along with the merchant reference code.
- 3** CyberSource generates a transaction reference number, or reconciliation ID, and sends it and the request to the payment processor.
- 4** Your local bank receives payment from the customer's bank.
- 5** The processor processes the settlement transaction.

- 6 The processor notifies CyberSource of the payment. CyberSource updates the transaction status in the CyberSource system as shown in [Figure 7](#), and the payment is matched to its original order.
- 7 You receive confirmation of the payment in the Payment Events Report, and you update your corresponding pending orders based on the report's information. The report includes the transaction reference number, or reconciliation ID, and your merchant reference code for the payment.

The following figure shows the possible transaction statuses for a direct debit.

Figure 7 Direct Debit Transaction Statuses



You can view a transaction's status in the Transaction Search Details screen. The status is listed as the "Action" in the small table in the top right corner of the screen.

Payment Confirmation and Shipping Goods

Use the Payment Events Report to determine when a direct debit payment has been received so that you can ship the goods. Look for an event type of Payment. For more information about the report, see ["Fulfilling the Order," page 21](#).

You can reconcile your orders with their corresponding payments by using either the CyberSource-generated transaction reference number, or reconciliation ID, or your own merchant reference code. If you plan to use the merchant reference code, make sure it is a unique value when you send it in the request.

Direct Debit Reversals

Customers can reverse direct debits if they believe the money was taken in error or without permission. A direct debit can also be reversed when there are insufficient funds in the customer's account.

When a direct debit is reversed, you receive notice in the Payment Events Report. Look for events labeled Reversal. The Processor Message field provides information about why the direct debit was reversed. The funds are automatically removed from your account, and the status of the direct debit changes to REVERSAL.

Using Chargebacks and Banking Reversal Codes for Reconciliation

You can use the daily Payment Events Report to reconcile your weekly or twice-weekly funding. The process is similar to reconciling a bank statement. Customer payments, such as credit card charges and direct debits credit your account, and credit card chargebacks and direct debit reversals debit your account. When your account is debited you are not getting paid for the goods or services you provided.

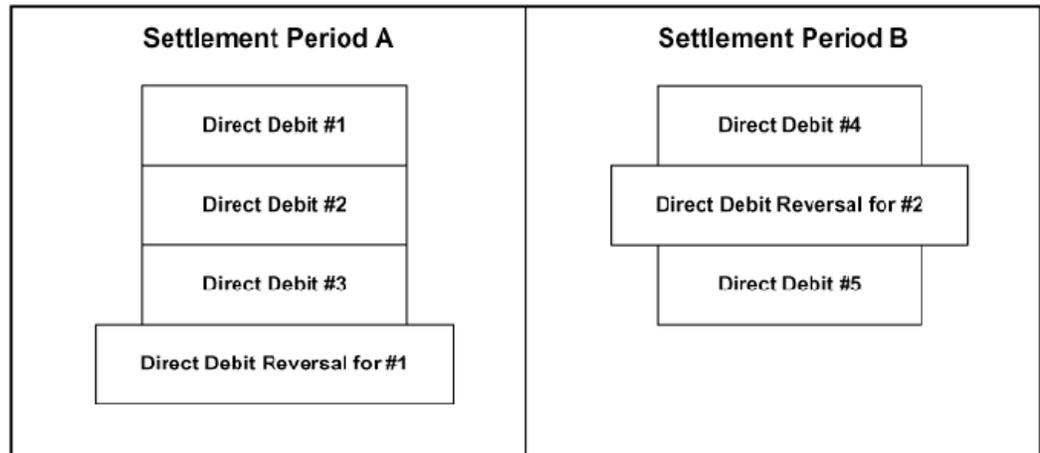
From an accounting perspective, credit card charges—even when the payment is later reversed—always credit your account, and chargebacks always debit the account. The sum of all credit card chargebacks is shown as a negative entry on the weekly or twice-weekly Remittance Report. See "[Remittance Report](#)," page 26.

Direct debit reversals occur two ways:

- If a direct debit reversal is received by the processor in the same settlement period as the direct debit it reverses, funds are neither credited nor debited in the Remittance Report. Instead, the transactions are internally reversed and are displayed as a notational entry in the Payment Events Report with an "X" prepended to the banking reversal code. See the appendix about banking reversal codes in the [Classic Reporting Developer Guide](#), which is available on the Support Center.
- If a direct debit reversal is received by the processor after the settlement period for the direct debit it reverses, then funds are debited. All debited funds are added together and are displayed as a single debit entry in the Remittance Report. The individual reversal is displayed as a regular entry in the Payment Events Report.

[Figure 8, page 36](#), illustrates the two types of direct debit reversals.

Figure 8 Direct Debit Reversals



The reversal for direct debit #1 occurs in the same settlement period as the direct debit it reverses. These transactions do not affect the Remittance Report. The reversal is in the Payment Events Report with an X banking reversal code.

Direct debit #2 is credited to your account in settlement period A. The reversal for direct debit #2 occurs in the following settlement period. The reversal is on the Remittance Report for settlement period B and is included in the sum of deductions. The reversal is in the Payment Events Report with a regular (no X) banking reversal code.

Settlement period A and settlement period B could be in the same or different funding cycles.

Design Considerations

Consider these factors when designing your system:

- With direct debits, you should not ship the goods until you receive confirmation of the customer's payment. Therefore, consider informing customers that shipment will not occur until you receive payment. For more information, see ["Fulfilling the Order," page 21](#).
- Depending on the country in which the direct debit takes place, you might be required to obtain and store mandates. Contact CyberSource Customer Support for country-specific requirements.
- Direct debits are subject to dispute rights. For example, a customer can claim that you did not have permission to remove funds from the account. Therefore, be prepared to handle disputes.
- You might be required to inform the customer before you collect a direct debit payment. Contact CyberSource Customer Support for country-specific requirements.
- To avoid providing a refund to customers who reverse a direct debit, CyberSource recommends that instead of issuing refunds for direct debits, you ask customers to reverse the direct debits.

Web Site Modifications

To accept direct debits, make the following modifications to your web site:

- Offer direct debit as a payment option if the customer resides in one of the supported countries.
- Provide the necessary procedure for obtaining a mandate. Contact CyberSource Customer Support for country-specific requirements.
- Display the appropriate bank information fields for the customer to complete. These fields and their local language labels depend on the country in which the direct debit occurs. For guidelines on the bank account number structures used in various countries, see the [Global Payment Service Developer Guide](#).

Direct Debit Refunds

You can submit a request to refund up to 100% of a direct debit. You can also request multiple partial refunds of a direct debit. The sum of the partial refunds cannot exceed 100% of the original direct debit. CyberSource recommends that before giving the refund you confirm that you have already received the direct debit payment.

When designing your system and your return policy for direct debit refunds, consider the fact that customers can reverse direct debits. The time interval during which customers can do so varies by country. Contact CyberSource Customer Support for country-specific requirements.

Types of Refunds

There are two types of direct debit refunds: follow-on refunds and stand-alone refunds. A follow-on refund uses information from a previous direct debit. A stand-alone refund does not depend on a previous transaction.

A follow-on refund must occur within a limited number of days after the request for the direct debit. If you are using the API to make these transactions, a follow-on refund must occur within 60 days of the direct debit request. If you are using the Business Center to make these transactions, a follow-on refund must occur within 180 days of the direct debit request.

After the time limit for a follow-on refund has passed, the only kind of refund you can make is a stand-alone refund.

Requesting a Follow-on Refund

A request for a follow-on direct debit refund must include the Request ID that was returned in the reply for the direct debit.

Flow of Identifiers for Order Tracking for Direct Debit Refunds

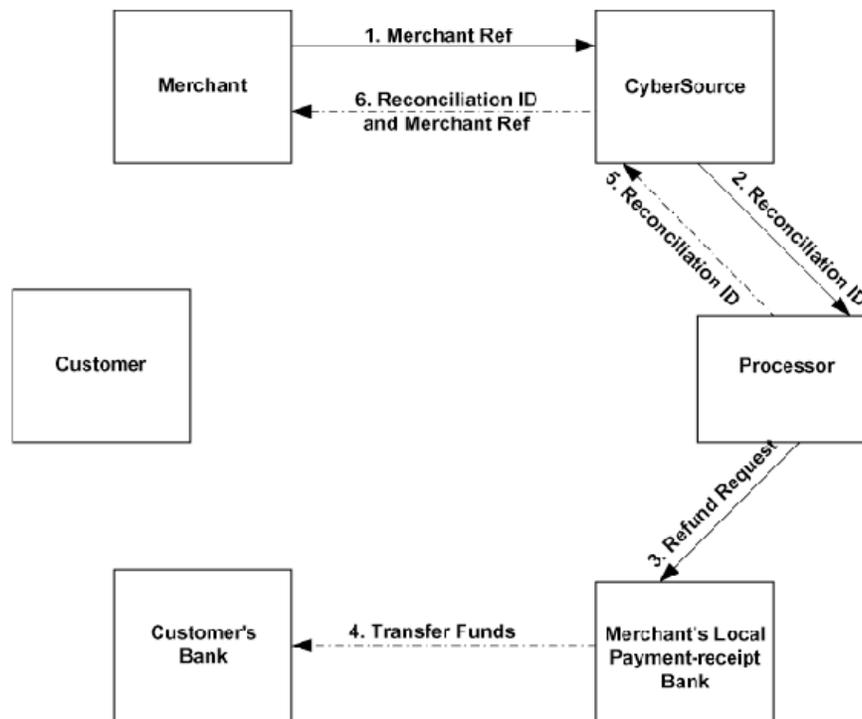
To perform a direct debit refund, you must obtain the customer's bank account information and supply it as part of the request to CyberSource. You must also link the refund to the direct debit by providing particular information from the direct debit in your refund request. For more details about the API fields, see information about direct debit refunds in the [Global Payment Service Developer Guide](#).

CyberSource recommends that when you request a refund, you use the same merchant reference code that you used for the direct debit. Using the same code makes it easier for

you to link the refund to the original direct debit in your own system and in CyberSource reports and Transaction Search screens.

Figure 9, page 39, shows the flow of information and identifiers that occurs for a direct debit refund.

Figure 9 Direct Debit Refund Identifier Flow



In the figure, solid lines (Steps 1-3) indicate actions that happen during the refund initiation process. Dashed lines (Steps 4-6) indicate actions that happen during payment and reconciliation. For definitions of the identifiers, see "[Order Tracking](#)," page 20.

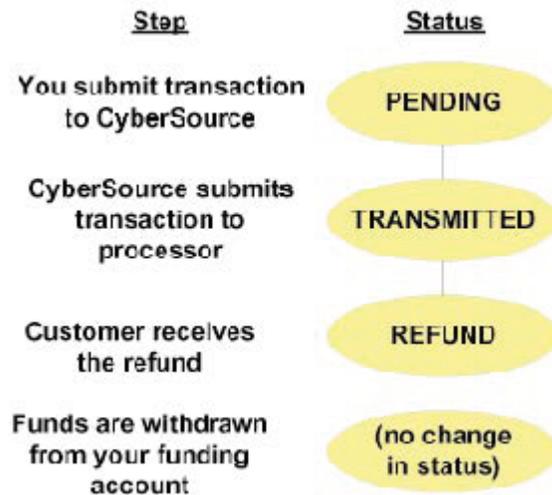
- 1 You collect the customer's bank information and send it along with the merchant reference code from the original direct debit in a request to CyberSource. To request a follow-on refund, send the following additional field (not shown in the figure): Request ID of the original direct debit.
- 2 CyberSource sends the refund request to the payment processor.
- 3 The payment processor sends the refund request to your local bank.
- 4 Your local bank transfers the money to the customer's bank and notifies the processor.
- 5 The payment processor notifies CyberSource that the refund is complete, and CyberSource updates the transaction status.

- 6 You download the Payment Events Report and update your system based on the report's information. The report contains the merchant reference code and the refund transaction reference number. Depending on which processor you are using, these numbers might not be the same as the direct debit number.

Transaction Status Changes

The following figure shows the different transaction statuses for a direct debit refund.

Figure 10 Direct Debit Refund Transaction Status Changes



You can view a transaction's status in the Transaction Search Details screen. The status is listed as the Action in the small table in the top right corner of the screen.

You can confirm that a refund has been given to the customer by looking at the Payment Events Report. Look for a Refund event for the refund.

Reconciling a Refund

Reconciliation for a refund is the same as reconciliation for direct debits. Use the Payment Events Report to get the confirmation that the refund has been processed by the payment processor. See "[Payment Events Report](#)," page 28. The report contains the transaction reference number (reconciliation ID) and the merchant reference code (merchant reference number) for the refund. The transaction reference numbers that you receive for all of the refunds will be the same as the number for the direct debit.

Bank Cards

Bank Card Types

There are two general types of bank cards you can accept through Ingenico ePayments:

- Global bank cards
- Regional or country-specific bank cards

For more information, see ["Bank Cards," page 10](#).

The global bank cards include:

- American Express
- Diners Club
- JCB
- Mastercard
- Visa

The regional or country-specific bank cards include:

- Cartes Bancaires (French bank card; for this card your capture requests must be 0.99 euros or more)
- Carta Si (Italian Visa or Mastercard bank card)
- Dankort (Danish Visa bank card)
- Delta (U.K. Visa debit card)
- Electron (European Visa debit card)
- Eurocard (Regional brand of Mastercard)
- Laser (Irish Visa bank card)
- Switch (U.K. bank card)

Online and Offline Processing

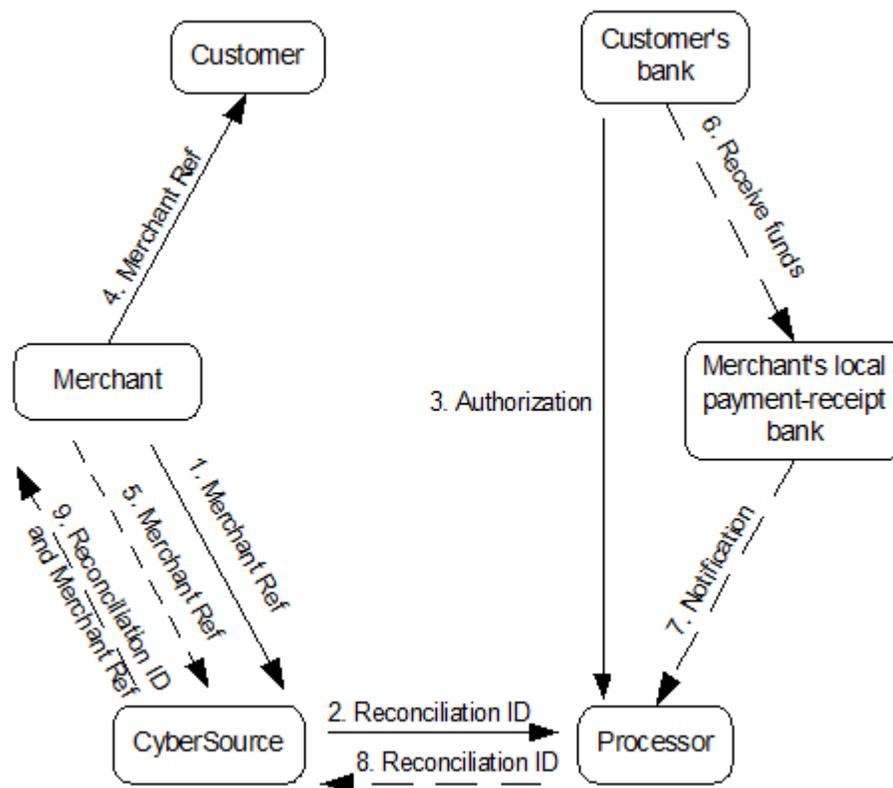
On Ingenico ePayments, each bank card is classified as *online* or *offline*.

Online Bank Card Flow

Online means that when you submit an authorization request to CyberSource, you receive an immediate confirmation from the customer's bank that the funds are available. For online bank cards, you typically start fulfilling the order when you receive confirmation.

Figure 11 shows the flow of information and identifiers for an online bank card.

Figure 11 Online Bank Card Identifier Flow



In the figure, solid lines (Steps 1-4) indicate actions that happen during the purchase process. Dashed lines (Steps 5-9) indicate actions that happen during payment and reconciliation.

See "Order Tracking," page 20, for definitions of the identifiers.

- 1 The customer chooses to pay by online bank card, and you send a request for authorization to CyberSource with the merchant reference code.

- 2 CyberSource generates a transaction reference number (reconciliation ID) and sends it and the authorization request to the payment processor.
- 3 The customer's bank authorizes the transaction in near real time, returning an authorization code.
- 4 You send confirmation to the customer with the merchant reference code.
- 5 When you are ready to bill the customer, you send a capture request to CyberSource with the same merchant reference code that you used in [Step 4](#).

**Note**

For Cartes Bancaires, your capture request must be at least 0.99 euros.

- 6 The customer's bank settles the order with your local bank.
- 7 The processor processes the settlement transaction and matches it to the original order.
- 8 The processor notifies CyberSource of the payment. CyberSource updates the transaction status in the CyberSource system.
- 9 Download the Payment Events Report using the merchant reference code and the transaction reference number (reconciliation ID) for the payment, and you can update the pending orders based on the report's information.

Offline Bank Card Flow

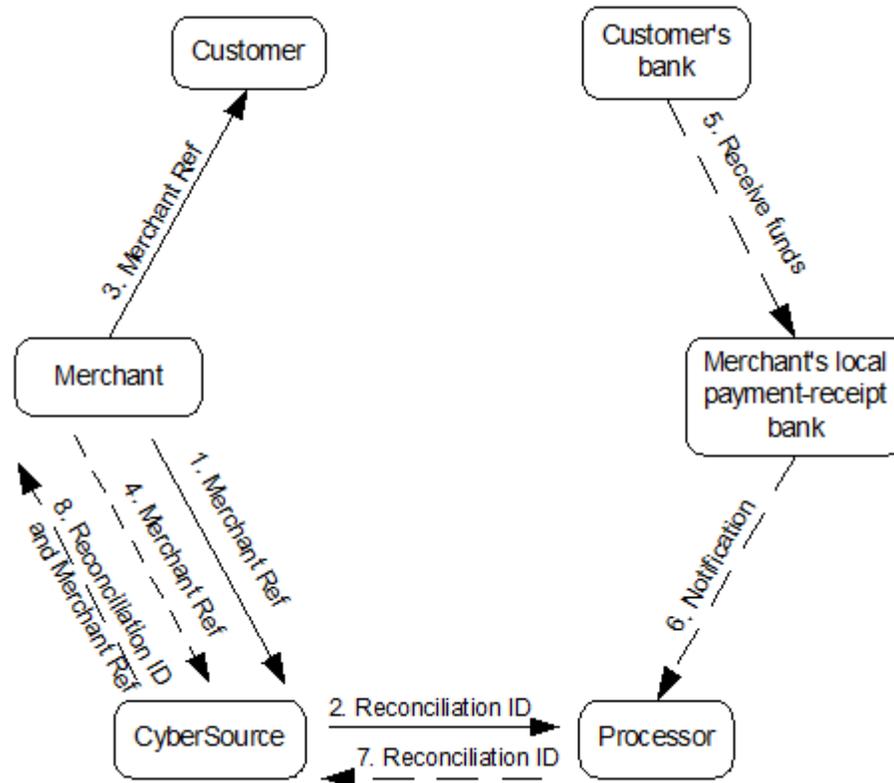
For offline cards, you do not receive immediate authorization from the customer's bank indicating that the funds are available. You will not know that funds are available until you receive confirmation of payment.

If you sell physical goods, you typically do not ship them until you receive payment confirmation.

Offline bank cards typically require 5 more days to confirm payment than online cards do.

[Figure 12](#) shows the flow of information and identifiers for an offline bank card.

Figure 12 Offline Bank Card Identifier Flow



In the figure, solid lines (steps 1-3) indicate actions that happen during the purchase process. Dashed lines (steps 4-8) indicate actions that happen during payment and reconciliation.

See "Order Tracking," page 20, for definitions of identifiers.

- 1 The customer chooses to pay by offline bank card, and you send a request for authorization to CyberSource with the merchant reference code.
- 2 CyberSource generates a transaction reference number (reconciliation ID) and sends it and the request to the payment processor. Because there is no online authorization, you receive an authorization code of Offline.
- 3 You send a confirmation to the customer with the merchant reference code. Funds availability cannot be predicted, however.
- 4 When you are ready to bill the customer, you send a capture request to CyberSource with the same merchant reference code that you used in Step 3. Note that an alternative is to eliminate this step and instead request both authorization and capture together in Step 1.
- 5 The customer's bank settles the order with your local bank.
- 6 The processor processes the settlement transaction and matches it to the original order.

- 7 The processor notifies CyberSource of the payment. CyberSource updates the transaction status in the CyberSource system.
- 8 Download the Payment Events Report using the merchant reference code and the transaction reference number (reconciliation ID) for the payment, and you can update the pending orders based on the report's information.

Reconciliation

Reconciliation enables you to determine when the bank card payment is received. Use the Payment Events Report for confirmation of payments or refunds for all types of bank cards. For more information about the report, see "[Payment Events Report](#)," page 28.

You can reconcile your orders to their corresponding payments using either the CyberSource-generated transaction reference number (reconciliation ID) or your own merchant reference code. If you plan to use the merchant reference code to reconcile orders, make sure it is a unique value such as the merchant order number.

Bank Card Refunds

You can perform follow-on credits for bank cards. You can also perform multiple partial credits against an original charge. Note that for bank cards processed with Ingenico ePayments, you can perform only one partial credit per day for a particular charge.

Web Site Modifications

You must modify your web site to offer your customers the option to pay using the bank cards appropriate for their country.

API for Bank Card Implementation

You use the same API for processing bank cards on Ingenico ePayments that you use for credit cards processed with CyberSource through other processors. You can find API information in [Credit Card Services Using the Simple Order API](#) or [Credit Card Services Using the SCMP API](#).

Reason Codes

Reason Codes for the Simple Order API

These reason codes apply only to Simple Order API. The reason code appears in the reply that you receive immediately after you request the service. See [Getting Started with CyberSource Advanced for the Simple Order API](#) for a discussion of replies, decisions, and reason codes.



Note

CyberSource reserves the right to add new reason codes at any time. If your error handler receives a reason code that it does not recognize, it should use the **decision** field to obtain the result.

Table 5 Reason Codes for the Simple Order API

Reason Code	Description
100	Successful transaction.
101	The request is missing one or more required fields. Optional action: See the reply fields missingField_0...N . Resend the request with the complete information. See the information about missing and invalid fields in Getting Started with CyberSource Advanced for the Simple Order API .
102	One or more fields in the request contain invalid data. Optional action: See the reply fields invalidField_0...N . Resend the request with the correct information. See the information about missing and invalid fields in Getting Started with CyberSource Advanced for the Simple Order API .
150	Error: General system failure. See the documentation for your CyberSource client for information on handling retries in the case of system errors.
151	Error: The request was received, but a server time-out occurred. This error does not include time-outs between the client and the server. Optional action: To avoid duplicating the transaction, do not resend the request until you review the transaction status in the Business Center. See the documentation for your CyberSource client for information about resending requests when errors occur.

Table 5 Reason Codes for the Simple Order API (Continued)

Reason Code	Description
152	<p>Error: The request was received, but a service timed out.</p> <p>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center. See the documentation for your CyberSource client for information about resending requests when errors occur.</p>
231	<p>Invalid account number.</p> <p>Optional action: Request a different form of payment.</p>
233	<p>General decline by the processor.</p> <p>Possible action: Request a different form of payment.</p>
234	<p>A problem exists with your CyberSource merchant configuration.</p> <p>Optional action: Do not resend the request. Contact Customer Support to correct the configuration problem.</p>
236	<p>Processor failure.</p> <p>Optional action: Wait a few minutes and resend the request.</p>
239	<p>The requested transaction amount must match the previous transaction amount.</p> <p>Optional action: Correct the amount and resend the request.</p>
241	<p>The request ID is invalid.</p> <p>Optional action: Verify that the request ID is correct.</p>
244	<p>The bank account number failed the validation.</p> <p>Optional action: Verify with the customer that the account number is correct; if it is incorrect, request the service again with the corrected information.</p>
250	<p>Error: The request was received, but a time-out occurred with the payment processor.</p> <p>Optional action: To avoid duplicating the transaction, do not resend the request until you review the transaction status in the Business Center.</p>
254	<p>Your CyberSource account is prohibited from processing stand-alone refunds.</p> <p>Optional action: In the refund request, provide the requestID of the payment to create a follow-on refund. If you want to process stand-alone refunds, contact your CyberSource account representative.</p>
255	<p>Your CyberSource account is not configured to process the service in the country you specified.</p> <p>Optional action: For a direct debit, verify that the bankInfo_country value is set to the correct country. To process the service in a country for which you are not configured, contact your CyberSource account representative.</p>

Index

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

A

accounts [16](#)
American Express [41](#)

B

bank cards
 country-specific [41](#)
 described [41](#)
 online and offline [42](#)
 reconciliation [45](#)
 worldwide [41](#)
bank information, displaying [30](#)

C

Carta Si [41](#)
Cartes Bancaires [41](#)
chargebacks
 in reports [29](#)
 providing company information [15](#)
Collection Report [25](#)
country-specific bank cards [41](#)
currencies [14](#)
customer support [23](#)

D

Dankort [41](#)
Diners Club [41](#)
direct debit refunds [38](#)

direct debits
 described [32](#)
 expected payment times [22](#)
 overview [9](#)
 reconciliation [34](#)
 reversals [35](#)
 Web site modifications [37](#)

E

Electron [41](#)
ELV [32](#)
Eurocard [41](#)
events [18](#)
exceptions [23](#)

F

financial reports [25](#)
follow-on refunds for direct debits [38](#)
fulfillment policies [21](#)

I

implementation [14, 18](#)

J

JCB [41](#)

L

Laser [41](#)

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

M

Mastercard [41](#)
 merchant agreements [15](#)
 merchant reference codes [20](#)

O

offline and online payment types [42](#)
 offline bank cards
 expected payment times [22](#)
 payment flow [43](#)
 online bank cards
 expected payment times [22](#)
 payment flow [42](#)
 order tracking
 for direct debit refunds [38](#)
 for direct debits [33](#)
 overview [20](#)

P

Payment Events Report
 described [28](#)
 direct debit refunds in [40](#)
 direct debit reversals in [35](#)
 direct debits in [34](#)
 exceptions in [23](#)
 for order reconciliation [27](#)
 for payment confirmation [21](#)
 refunds in [22](#)
 Payment Status Report, for order reconciliation [27](#)
 Payment Submission Detail Report
 described [27](#)
 for order reconciliation [27](#)

R

reason codes [46](#)
 reconciliation
 bank cards [45](#)
 for direct debit funding [35](#)
 for direct debit refunds [40](#)
 for direct debits [34](#)
 reconciliation IDs [20](#)
 refunds for direct debits [38](#)
 Remittance Report [25](#)
 reports
 and settlement periods [26](#)
 Collection Report [25](#)
 financial reports [25](#)
 Payment Events Report [28](#)
 Payment Submission Detail Report [27](#)
 Remittance Report [25](#)
 schedules for [26](#)
 request tokens [24](#)
 reserve accounts [16](#)
 reversals [35](#)

S

settlement periods
 and direct debit reversals [35](#)
 and reports [26](#)
 shipping [21](#)
 stand-alone refunds for direct debits [38](#)
 Switch [41](#)

T

tracking orders [20](#)
 trans ref nos [20](#)
 Transaction Exception Detail Report, for order reconciliation [27](#)
 transaction reference numbers [20](#)

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

U

underwriting assessments **15**

V

Visa **41**

W

worldwide bank cards **41**