Cashflows

Remote API Integration Guide

Version 2.7 – October 2020

Table of contents

About this guide

Welcome to the Cashflows Remote API Integration Guide. This document is designed to provide you details on how to integrate your business to the Cashflows payment processing system and optionally take advantage of our m-commerce voice signature technology.

This document assumes a working knowledge of HTML, HTTP(S) and some programming skills like, Java, PHP, ASP or .Net.

If you are taking card payments, you will also need to be PCI DSS compliant as you will need to securely collect and store cards details. For further information about PCI DSS and your security requirements, please visit http://support.cashflows.com/pcidss/

In addition to this guide we have a team of specialists providing technical support during your integration with Cashflows. To receive support please visit our website - http://support.cashflows.com

The latest version of this guide is always available from:
http://support.cashflows.com/kb/remote_api_integration_guide.pdf

Introduction

Cashflows delivers a range of merchant services designed to help businesses manage and maximise their cash flow. Cashflows Merchant Services enables businesses to offer their customers a full range of payment channels including, online, mobile and mail & telephone orders.

How does Cashflows work?

1. A consumer selects a product or a service to purchase from your store.
2. The consumer's payment card details are entered via an online payment page or Virtual Terminal.
3. The payment card details are sent by us via the card schemes network to the consumer's card issuing bank for authorisation.
4. The card issuer checks the card details, that the cardholder's account has sufficient funds and that the card hasn't been reported lost or stolen. If everything is OK, the issuing bank authorise the amount requested and debits those funds from the consumer's payment card account.
5. The authorisation results are returned to you and your customer, the cardholder confirming the result of the transaction.
6. We receive the funds from the card schemes network and then remit them into your business bank account.

Cashflows Remote API

The Cashflows Remote API is a mechanism that allows you to collect cardholder and transaction details within your application or online store and to submit them directly to Cashflows for processing. This differs from the standard payment page integration where you submit the transaction details only to Cashflows and we collect the cardholder details.

Using the Cashflows Remote API would be applicable if you have an online store and you wish your shoppers to remain on your site for the whole duration of the transaction. If you take orders over the phone, then it would make sense to integrate your backend order processing application to Cashflows using the Remote API and avoid your operators having to enter credit card details into the Virtual Terminal.

Security Requirements

Using the Remote API model to send payment data means that you will be capturing, transmitting, and possibly storing card data. The Card Schemes, Visa Europe and MasterCard International, have never permitted the storage of sensitive data (track data and/or CVV2) post-authorisation, and it is prohibited under 'Requirement 3' of the Payment Card Industry Data Security Standard (PCI DSS). Merchants who store Sensitive Authentication Data (SAD) are being fined by the Card Schemes.

Consequently, if you use the Remote API model you will need to demonstrate that your systems can handle this data securely and that you are taking full responsibility for your PCI compliance. One part of this is the need for us to see a clean Vulnerability scan being made on your systems. To view a list of Approved Scanning Vendors, please go to https://www.pcisecuritystandards.org/qsa_asv/find_one.shtml.

For further information on PCI security standard, please visit http://support.cashflows.com/pcidss/ or https://www.pcisecuritystandards.org

Submitting a payment request

The payment request takes the form of a HTTPS **POST** request containing a description of the goods or services being purchased, the total cost, your Cashflows Profile ID and the credit card and cardholder details of the consumer. The **POST** request must be UTF-8 encoded and submitted to:

URL	Environment
https://secure-int.cashflows.com/gateway/remote	Integration
https://secure.cashflows.com/gateway/remote	Production

Please contact techsupport@cashflows.com if you require an integration account.

Warning: Our payment service does not have fixed IP addresses and are therefore subject to change. When sending payment requests you should always point to the DNS record of secure.cashflows.com instead.

Note: Before you can send payment requests you will be required to provide our support team with the IP address(es) of your payment server, so that we can correctly configure your profile.

If the purchase consists of more than one item, your shopping cart system must total all the items into a single description and total cost and submit a single combined payment request.

Payment Request parameters

The following table lists the parameters that can be passed to the Remote API to request a payment authorisation.

Note: All payment request parameters are mandatory unless specified.

Parameter	Description
auth_id	Your Profile ID
auth_pass	Authentication password
card_num	Customer's card number. (Must be numeric only with no separators.)
card_cvv	Card security code.
card_start	Card start date. Format is MMYY. (Optional)
card_issue	Card issue number. (Optional)
card_expiry	Card expiry date, format is MMYY
cust_name	Customer's name
cust_address	Customer's address (Multiple lines can be separated using the new line break character (ASCII code 10))
cust_postcode	Customer's post/zip/area code
cust_country	Customer's country (ISO3166 2-character code)
cust_ip	Customer's IP address (IPV4 Format only)
cust_email	Customer's email address
cust_tel	Customer's telephone number

tran_ref	Your transaction reference (e.g. cart ID)
tran_desc	Your transaction description (Max of 99 characters) (Optional)
tran_amount	Transaction amount to 2 decimal places, e.g. 24.99. (The currency symbol must not be included.)
tran_currency	Transaction currency, 3-character code.
tran_testmode	Transaction test mode. 0=Live, 1=Test
tran_type	Transaction type = sale
tran_class	Transaction class = “ecom” or “moto”
tran_recurrence	To be used to override default MID settings. • **sing** = Single transaction with no recurrence • **subs** = Transaction in recurring subscription • **inst** = Transaction in recurring instalment • **unsc** = Unscheduled transaction with a stored card • **card** = Cardholder initiated transaction with a stored card (Optional)
sca_exemption_indicator	Indication of why the transaction may be exempt from SCA, possible values: • **lowvalue** = Applicable to transactions where amount is less than €30 or currency equivalent) (Optional)
descriptor	A soft descriptor that is added to your Company Name when displayed on the Cardholders statement. (Max of 12 characters) (Optional)
Additional fields for 3d Secure Transactions	
VERSION 1:	
acs_3dsversion	The version of 3DS being used for authentication (Optional, when not supplied version **1.0.2** is assumed)
acs_eci	The response from the Access Control Server, stating the 3DS method and result: • **5** = VbyV **-** Full Authentication • **6** = VbyV **-** Attempted Authentication • **7** = VbyV - No Authentication • **2** = MasterCard SecureCode **-** Full Authentication • **1 =** MasterCard SecureCode **-** Attempted Authentication • **0** = MasterCard SecureCode **-** No Authentication
acs_cavv	The Cardholder Authentication Verification Value from the Access Control Server, 28 characters.
acs_xid	The unique **Authentication** Id for transaction from the Access Control Server, 28 characters.
VERSION 2:	
acs_3dsversion	The version of 3DS being used for authentication (Optional - when not supplied version 1 is assumed) otherwise **2.1.0** or **2.2.0** should be set
acs_eci	The response from the 3DS server. • **5** = VbyV **-** Full Authentication • **6** = VbyV **-** Attempted Authentication • **7** = VbyV - No Authentication • **2** = MasterCard SecureCode **-** Full Authentication • **1 =** MasterCard SecureCode **-** Attempted Authentication • **0** = MasterCard SecureCode **-** No Authentication
acs_cavv	The Cardholder Authentication Verification Value from the Access Control Server, 28 characters.
acs_dstransid	The unique **Authentication** Id for transaction from the Access Control Server, 28 characters.
Additional fields for merchants with the MCC 6012, 6051 or 7299 (Financial Institutions)	

primary_recipient_dob	Customer's Date of Birth. Format is YYYYMMDD (8 numeric characters)
primary_recipient_surname	Customer's Surname or Last name (2-64-characters alpha characters, including –)
primary_recipient_postcode	Customer's Postcode (2 to 16-characters alpha characters, including spaces)
primary_recipient_account_number	Customer's Account Number (1 to 32 alpha numeric characters, including /-) For PAN Numbers: First 6 and Last 4 (Never include full PAN in primary_recipient_account_number field.)

Example of a Payment Request

You can submit a **POST** request using a range of different programming languages, below is an example of how to submit a payment request using PHP and CURL:

```
<?php
$PaymentUrl = "https://secure.cashflows.com/gateway/remote";
$PostString="auth_id=1234&auth_pass=Password&card_num=4000000000000002&card_cvv=123&card_expiry=0116&cust_name=Testing&cust_address=My%20house%0AMy%20street%0AMy%20Town&cust_postcode=CB22%205LD&cust_country=GB&cust_ip=123.45.67.89&cust_email=test@test.com&tran_ref=abc123&tran_amount=9.99&tran_currency=GBP&tran_testmode=0&tran_type=sale&tran_class=ecom";
$ch = curl_init($PaymentUrl);
curl_setopt($ch, CURLOPT_POST,1);
curl_setopt($ch, CURLOPT_POSTFIELDS, $PostString);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$result = curl_exec($ch);
curl_close($ch);
?>
```

The above example **POST** request will send the following payment details to the Remote API for authorisation.

```
auth_id=1234&auth_pass=Password&card_num=4000000000000002&card_cvv=123&card_expiry=0116&cust_name=Testing&cust_address=My%20house%0AMy%20street%0AMy%20Town&cust_postcode=CB22%205LD&cust_country=GB&cust_ip=123.45.67.89&cust_email=test@test.com&tran_ref=abc123&tran_amount=9.99&tran_currency=GBP&tran_testmode=0&tran_type=sale&tran_class=ecom
```

Remote administration

Void and Refunds

To Void or Refund a transaction you can either use the administration system or send a request to the Remote API. A Void/Refund request takes the form of a HTTPS **POST** request containing the transaction details that you wish to void or refund. The **POST** request must be UTF-8 encoded and submitted to: *https://secure.cashflows.com/gateway/remote*

To void a transaction you will need to enter all of the transaction details including the full amount of the original transaction and send the Void value in the *trans_type*. Using the Remote API, you can also fully or partially refund a transaction by entering the amount that you wish to refund into the *trans_amount*.

Note: You cannot refund more than the original transaction's value. You are also unable to complete a full or partial refund on the same day that the transaction was made as the funds are yet to be cleared.

Void/Refund Request parameters

The following table lists the parameters that can be passed to the Remote API:

Parameter	Description
auth_id	Must be set to the Profile ID
auth_pass	Authentication password
tran_amount	Transaction amount to 2 decimal places, e.g. 24.99. (The currency symbol must not be included.)
tran_currency	Transaction currency, 3-character code.
tran_testmode	Transaction test mode. 0=Live, 1=Test
tran_type	Transaction type = "**refund**" or "**void**"
tran_class	Transaction class = must match the original transaction class
tran_orig_id	Original transaction ID to be refunded or voided
descriptor	A soft descriptor that is added to your Company Name when displayed on the Cardholders statement. (Max of 12 characters) (Optional)

Example of a Void Request

Example of the **POST** string sent in the Void request to the Remote API for administration.
auth_id=1234&auth_pass=Password&tran_amount=9.99&tran_currency=GBP&tran_testmode=0&tran_type=void&tran_class=ecom&tran_orig_id=01S0001

Example of a Refund Request

Example of the **POST** string sent in the Refund request to the Remote API for administration.
auth_id=1234&auth_pass=Password&tran_amount=2.99&tran_currency=GBP&tran_testmode=0&tran_type=refund&tran_class=ecom&tran_orig_id=01S0001

Credit Transfers

If you have the appropriate 7995 MCC and have Credit Transfers enabled, you can use the Remote API to

make a credit transfer request. The credit transfer request takes the form of a HTTPS **POST** containing the amount that you wish to credit a customer who made the original transaction. The **POST** request must be UTF-8 encoded and submitted to: *https://secure.cashflows.com/gateway/remote*

Credit Transfer Request parameters

The following table lists the parameters that can be passed to the API:

Parameter	Description
auth_id	Must be set to the Profile ID
auth_pass	Authentication password
tran_amount	Credit Transfer amount to 2 decimal places, e.g. 24.99. (The currency symbol must not be included.)
tran_currency	Transaction currency, 3-character code.
tran_ref	Your transaction reference (e.g. cart ID)
tran_testmode	Transaction test mode. 0=Live 1=Test
tran_type	Transaction type = credit
tran_class	Transaction class = cred
tran_orig_id	Original transaction Id to which the credit will be applied to.
security_hash	A security Hash value used to ensure that no-one has tampered with the credit transfer request.
descriptor	A soft descriptor that is added to your Company Name when displayed on the Cardholders statement. (Max of 12 characters) (Optional)

Example of a Credit Transfer

Example of the **POST** string sent in the Credit Transfer request to the API for administration.
auth_id=1234&auth_pass=Password&tran_amount=2.99&tran_currency=GBP&tran_ref=Payout1234tran_testmode=0&tran_type=credit&tran_class=cred&tran_orig_id=01S0001&security_hash=e5446ea59340d867af9fed6ba92f267e17d0119c7d972d7d84c0ab31ee4b1708

To protect the Credit Transfer from being tampered with whilst being transferred you **must** include a cryptographic hash digital signature. The digital signature or 'message digest' needs to be created by your own server side scripting using the SHA256 algorithm method and contain the following values:
tran_type:tran_amount:tran_currency:tran_orig_id:tran_ref:[secret key]

Each section of data is separated using a '**:**' (colon) character, and the data must be organised in the exact sequence shown.

The 'message digest' is then be included into your credit transfer request using the *security_hash* parameter. Cashflows compares the 'message digest' against its own 'message digest' created from your credit transfer details supplied. As only you and the Cashflows know the secret key element of the 'message digest', the credit transfer will only be processed if the two 'message digest' match.

Warning: At no time should the actual pre-set secret key be included in any FORM or web page that is held on your server.

Note: Please contact your account manager to confirm if Credit Transfers have been enabled on your account.

Credit transactions are only supported for the following MCC's:
7995 - Gambling
7994 - Game of skill
6010 - Financial Institutions – Manual Cash Disbursements
6011 - Financial Institutions – Automated Cash Disbursements
6012 - Financial Institutions – Merchandise, Services, and Debt Repayment
6300 - Insurance Sales, Underwriting, and Premiums
6399 - Insurance, Not Elsewhere Classified
8999 - Professional Services (Not Elsewhere Classified)
5262 - Marketplaces

Recurring payments

To take recurring payments from a cardholder you will need to create a Recurring Payment Agreement & Schedule, where you inform the cardholder the exact details of the agreement including:
The amount of the Recurring Payment
Whether the amount is fixed or variable
The Schedules date(s) of the Recurring Payment
Whether the Schedules date(s) are fixed or variable
Upon the cardholder's express consent, you can submit recurring payment requests via the Remote API, using an approach called continuous authority. To submit a recurring payment, you will first require getting an initial account verification of a consumer's card details including the card's CVV. This account verification request is then checked and if successful, authorised. We then store the card details securely on our PCI approved system and send you a request response containing an account verification Id. When sending a continuous (recurring) payment request you must include this account verification Id to enable us to use the initially stored card details to send the payment for authorisation.

Note: Any changes to a cardholder's Recurring Agreement must be communicated at least seven working days prior to the next payment being taken. You must communicate to the cardholder in any of the following situations:
More than six months have elapsed since the last payment
A trial period, introductory offer or promotional activity has expired
There are changes to the Recurring Agreement: - any change to the amount of the Recurring Payment *and/or* - any change to the date of the Recurring Payment

Account Verification Request parameters

The following table lists the account verification request parameters that must be passed to the Remote API:

Note: All request parameters are mandatory unless specified.

Parameter	Description
auth_id	Must be set to the Profile ID
auth_pass	Authentication password
card_num	Customer's card number. Must be numeric only with no separators.
card_cvv	Card security code.
card_start	Card start date. Format is MMYY. (Optional)
card_issue	Card issue number. (Optional)
card_expiry	Card expiry date, format is MMYY
cust_name	Customer's name
cust_address	Customer's address. (Multiple lines can be separated using the new line break character (ASCII code 10))
cust_postcode	Customer's post/zip/area code
cust_country	Customer's country, ISO3166 2-character code.
cust_ip	Customer's IP address (IPV4 Format only)
cust_email	Customer's email address

cust_tel	Customer's telephone number
tran_ref	Your transaction reference (e.g. cart ID)
tran_desc	Your transaction description (Optional)
tran_currency	Transaction currency, 3-character code (For a list of currencies code you can use / accept, please contact support@cashflows.com)
tran_testmode	Transaction test mode. 0=Live, 1=Test
tran_type	Transaction type = verify
tran_class	Transaction class = "ecom" or "moto"
descriptor	A soft descriptor that is added to your Company Name when displayed on the Cardholders statement. (Max of 12 characters) (Optional)

Additional fields for 3d Secure Transactions	
VERSION 1:	
acs_3dsversion	The version of 3DS being used for authentication (Optional, when not supplied version **1.0.2** is assumed)
acs_eci	The response from the Access Control Server, stating the 3DS method and result: • **5** = VbyV **-** Full Authentication • **6** = VbyV **-** Attempted Authentication • **7** = VbyV - No Authentication • **2** = MasterCard SecureCode **-** Full Authentication • **1 =** MasterCard SecureCode **-** Attempted Authentication • **0** = MasterCard SecureCode **-** No Authentication
acs_cavv	The Cardholder Authentication Verification Value from the Access Control Server, 28 characters.
acs_xid	The unique **Authentication** Id for transaction from the Access Control Server, 28 characters.
VERSION 2:	
acs_3dsversion	The version of 3DS being used for authentication (Optional - when not supplied version 1 is assumed) otherwise **2.1.0** or **2.2.0** should be set
acs_eci	The response from the 3DS server. • **5** = VbyV **-** Full Authentication • **6** = VbyV **-** Attempted Authentication • **7** = VbyV - No Authentication • **2** = MasterCard SecureCode **-** Full Authentication • **1 =** MasterCard SecureCode **-** Attempted Authentication • **0** = MasterCard SecureCode **-** No Authentication
acs_cavv	The Cardholder Authentication Verification Value from the Access Control Server, 28 characters.
acs_dstransid	The unique **Authentication** Id for transaction from the Access Control Server, 28 characters.
Additional fields for merchants with the MCC 6012, 6051 or 7299 (Financial Institutions)	
primary_recipient_dob	Customer's Date of Birth. Format is YYYYMMDD (8 numeric characters)
primary_recipient_surname	Customer's Surname or Last name (2-64-characters alpha characters, including –)
primary_recipient_postcode	Customer's Postcode (2 to 16-characters alpha characters, including spaces)
primary_recipient_account_number	Customer's Account Number (1 to 32 alpha numeric characters, including /-) For PAN Numbers: First 6 and Last 4 (Never include full PAN in primary_recipient_account_number field.)

Example of an Account Verification Request

Example of the **POST** string sent in the account verification request to the Remote API for authorisation.

auth_id=1234&auth_pass=Password&card_num=4000000000000002&card_cvv=123&card_expiry=0116&cust_name=Testing&cust_address=My%20house%0AMy%20street%0AMy%20Town&cust_postcode=CB22%205LD&cust_country=GB&cust_ip=123.45.67.89&cust_email=test@test.com&tran_ref=abc123&tran_currency=GBP&tran_testmode=0&tran_type=verify&tran_class=ecom

Note: An Account Verification request checks if the account is valid, it will not perform a check for available funds on the account and is not an authorisation of a sale.

Example of an Account Verification Response

Example of the account verification response sent to you after submitting an account verification request:

Example Response	Meaning
A|01P00001724|232|031971|Authorised	Authorised: A Account Verification Id: 01P00001724 CVV/AVS:232 Authorisation code: 031971

This includes the account verification Id denoted with a 01P prefix and the CVV/AVS check response. A continuous authorised payment request can only be performed where the CVV comparison check has been returned as a MATCH (i.e. the first check value must be a 2), irrespective of the authorisation status of the Account Verification.

For more information about request responses, please refer to: Authorisation Request Response.

Continuous Payment Request parameters

To send a continuous payment request you must **exclude** *card_num*, *card_expiry* & *card_cvv* parameter, and include the *tran_orig_id* which has the value of the *Account Verification Id.* The following table lists the continuous payment request parameters that must be passed to the Remote API:

Note: All request parameters are mandatory unless specified.

Parameter	Description
auth_id	Must be set to the Profile ID
auth_pass	Authentication password
cust_name	Customer's name
cust_address	Customer's address. (Multiple lines can be separated using the new line break character (ASCII code 10))
cust_postcode	Customer's post/zip/area code
cust_country	Customer's country, ISO3166 2-character code.
cust_ip	Customer's IP address (IPV4 Format only)
cust_email	Customer's email address
cust_tel	Customer's telephone number

tran_ref	Your transaction reference (e.g. cart ID)
tran_desc	Your transaction description (Optional)
tran_amount	Transaction amount to 2 decimal places, e.g. 24.99. (The currency symbol must not be included.)
tran_currency	Transaction currency, 3-character code.
tran_testmode	Transaction test mode. 0=Live, 1=Test
tran_type	Transaction type = sale
tran_class	Transaction class = cont
tran_orig_id	Account Verification or ECOM transaction ID
tran_recurrence	To be used to override default MID settings. • **sing** = Single transaction with no recurrence • **subs** = Transaction in recurring subscription • **inst** = Transaction in recurring instalment • **unsc** = Unscheduled transaction with a stored card • **card** = Cardholder initiated transaction with a stored card (Optional)
sca_exemption_indicator	Indication of why the transaction may be exempt from SCA, possible values: • **recurring** = Applicable to transactions where recurrence type = '**subs'** or '**inst'** • **merchantinitiated** = Applicable to merchant-initiated transactions where recurrence type = '**sing'** or '**unsc'** (Optional)
descriptor	A soft descriptor that is added to your Company Name when displayed on the Cardholders statement. (Max of 12 characters) (Optional)
Additional fields for merchants with the MCC 6012, 6051 or 7299 (Financial Institutions)	
primary_recipient_dob	Customer's Date of Birth. Format is YYYYMMDD (8 numeric characters)
primary_recipient_surname	Customer's Surname or Last name (2-64 characters alpha characters, including –)
primary_recipient_postcode	Customer's Postcode (2 to 16 -characters alpha characters, including spaces)
primary_recipient_account_number	Customer's Account Number (1 to 32 alpha numeric characters, including /-) For PAN Numbers: First 6 and Last 4 (Never include full PAN in primary_recipient_account_number field.)

Example of a Continuous Payment Request

Example of the **POST** string sent in the continuous payment request to the Remote API for authorisation.

auth_id=1234&auth_pass=Password&cust_name=Testing&cust_address=My%20house%0AMy%20street%0AMy%20Town&cust_postcode=CB22%205LD&cust_country=GB&cust_ip=123.45.67.89&cust_email=test@test.com&tran_ref=abc123&tran_amount=9.99&tran_currency=GBP&tran_testmode=0&tran_type=sale&tran_class=cont&tran_orig_id=01P00001724

Authorisation request response

The response consists of the authorisation status code, transaction ID, CVV/AVS result, authorisation code and authorisation message. These fields are separated using the vertical bar character. An authorisation status of 'A' indicates that the transaction was authorised, anything else indicates that it was not.

Example Response	Meaning
A|01S00001724|232|031971|Authorised	Authorised: A Transaction Id: 01S00001724 CVV/AVS:232 Authorisation code: 031971
D|01S00001723|400|D102|Not Authorised	Not authorised: D Transaction Id: 01S00001723 CVV/AVS:400
V|01S00001722|000|V226|Invalid request	Invalid request: V Transaction Id: 01S00001722 CVV/AVS:000 (please refer to Appendix A for further information.)
B|01S00632BE2|000|D090|Not authorised	Blocked: D Transaction Id: 01S00632BE2 CVV/AVS:000 (please refer to Appendix A for further information.)

CVV/AVS check values

The CVV/AVS result is a 3-digit value, each digit representing a different check.
The first value is the CVV check, the second is the address and the third is the postcode.
The possible values for each digit are as follows:

Value	Meaning
0	Not Checked
1	Check was not available
2	Full match
3	Partial match
4	Not matched
5	Error

A partial match is only possible for the address or postcode data, not for CVV check.
Not all acquirers or issuers support all of these checks, in which case the results will be either 0 or 1.

Example Response	CVV	Address	Postcode
232	Full match	Partial match	Full match
400	Not matched	Not checked	Not checked

Testing your integration

You can test your integration to our Remote API by setting your **POST** request to test mode. To send a test payment request you will need to set *tran_testmode=1* and enter a valid Visa test card number as show below:

Card Number	Expiry Date	CVV
4000000000000002 (VISA)	Any valid expiry date (MMYY)	123
4462030000000000 (VISA prepaid)	Any valid expiry date (MMYY)	444
5555555555554444 (MasterCard)	Any valid expiry date (MMYY)	321
5597507644910558 (MasterCard prepaid)	Any valid expiry date (MMYY)	888

Warning: Test card numbers will only work when the payment request is in test mode, if used in live mode the test will be subject to a payment authorisation charge.

Appendix a: payment system response codes

Status 'A' is authorised, anything else is not. The auth code and auth message for authorised transactions cannot be predicted (as they can change from one bank/issuer to the next).

'V' is a validation error (e.g. invalid card number)
'D' is a decline
'R' is a referral (has to be treated as a decline)
'B' is a blocked transaction
'C' is a cancelled transaction (e.g. user pressed cancel on payment page)
'S' is a system error

These will be followed by a 3-digit code, the first digit is an internal code which can be ignored. The second two digits are the actual error code for the given status. Attached is a list of the current error codes. (Please note this list is subject to change).

The list is given as, for example, Vx01 which means it is the result for V101, V201, V301 etc.

CODE	REASON
Vx01	Invalid merchant details
Vx02	Invalid expiry date
Vx03	Invalid start date
Vx04	Invalid issue number
Vx05	Invalid CVV
Vx06	Invalid card number
Vx07	Card holder name not set
Vx08	Insufficient address details
Vx09	Invalid country code
Vx10	Invalid cart ID
Vx11	Invalid email address
Vx12	Invalid phone number
Vx13	Invalid amount
Vx14	Invalid currency code
Vx15	Invalid customer IP
Vx16	Original trans not found
Vx17	Invalid merchant IP
Vx18	Unknown transaction type
Vx19	Card number changed
Vx20	Currency changed
Vx21	Original trans ref required
Vx22	Amount exceeds original
Vx23	Can not refund this type of transaction
Vx24	Amount changed
Vx25	User account details required
Vx26	Invalid request
Vx27	Original trans not pre-auth
Vx28	Transaction mode changed
Vx29	Card/Currency combination not supported
Vx30	Unknown card type
Vx31	Issue number required
Vx32	Issue number not required
Vx33	Duplicate transaction

Vx34	Unable to void transaction
Vx35	Original trans was not authorised
Vx36	Invalid PIN
Vx37	Unknown transaction class
Vx38	Original transaction type does not match
Vx39	Card expired
Vx40	CVV Required
Vx41	Original transaction already settled
Vx42	Original transaction already cancelled
Vx43	This card does not support the required transaction type
Vx44	Transaction details do not match original
Vx48	User Details not valid
Vx52	3DS Not Enabled
Vx53	3DS Data Invalid
Vx54	Concurrent Authorisations
Vx55	Invalid Funds Recipient Date (MCC 6012, 6051 or 7299 merchants)
Vx56	Terminal mismatch
Vx57	Transaction not allowed on this card
Vx58	Original transaction requires 3DS attempt/auth
Vx59	ECOM transactions require 3DS attempt/auth
Vx60	Verify for Amex card not supported
Vx61	Recurrence Flag usage invalid
Vx62	Initial Sale/Verify ARN missing for subsequent sale
Vx63	Initial Sale/Verify for subsequent sale not approved
Vx64	Initial transaction on card expired

Dx01	Non-specific decline
Dx02	Declined due to funds (insufficient/limit exceeded)
Dx03	Retain card response
Dx05	On our blacklist
Dx07	Live/test mismatch
Dx08	Refund: Insufficient merchant funds in account
Dx10	Card authorisation attempt limit reached
Dx11	Monthly Scheme Decline Rate limit reached
Dx40	Continuous Authority cancelled for the transaction
Dx41	Continuous Authorities cancelled for the merchant
Dx43	Continuous Authorities cancelled for the card
Dx49	Additional customer authentication required
Dx90	Pre-Authorisation anti-fraud block
Dx91	Post-Authorisation anti-fraud block

Rx01	Not Authorised

Ex01	Transaction error

Cx01	Transaction cancelled
Cx02	Transaction expired

Sx00	Invalid transaction Request
Sx01	Connection failure
Sx02	Invalid response

Sx03	Response timeout
Sx04	Server error
Sx05	Server error
Sx06	No response from issuer
Sx07	Service not available
Sx99	Unknown Error