

TransactDirect with 3-D Secure

The UPG Guide for Secure Internet Transaction Delivery

For use with Transact.ashx and TransactACS.ashx



Introduction

Universal Payment Gateway (UPG)'s TransactDirect is an Internet-based real time card processing system that converts the traditional two-stage authorisation and payment processes into one convenient 'transaction' process.

TransactDirect is designed to be exceptionally easy to integrate into web sites, Internet-connected call centre systems and Internet-connected Electronic Point Of Sale (EPOS) terminals. It is flexible, robust and fast, normally returning authorisations within 3 seconds.

TransactDirect operates as a 'gateway' in the strictest sense in that it does not display any web pages during the transaction process nor does it require any software to be installed on the merchant's system. This makes it ideal for:

- Merchants that require customised Internet card payment solutions.
- Integration into Internet connected call centre systems.
- Integration into Internet connected EPOS terminals.
- Payment Service Providers (PSPs) who wish to build their own solution for their customers.

TransactDirect supports the latest UK banking industry initiatives including:

- Chip and PIN (Although it is technically possible to use TransactDirect for Chip and PIN transactions, we would recommend the direct use of UPG 2.1 format transaction submission via leased-line or private, point-to-point ADSL. If you intend to conduct Chip and PIN transactions, please contact UPG for additional guidelines.)
- Address Verification Service (AVS) and Card Verification Value / Check (CV2).
- Multi-currency.
- 3-D Secure for Verified by Visa and MasterCard SecureCode.

All TransactDirect merchants have secure access to their own private area of the TransactDirect Transaction Management System (TMS), providing merchants with the ability to view their Cardholder Not Present (CNP) and ecommerce transaction history, carry out settlement audits, conduct refunds and re-billing as well as set up AVS and CV2 response handling preferences.

It is recommended, however, that the processing of refunds, re-billing and the handling of referrals and communications failure be achieved directly through TransactDirect. Please note that these processes need the added protection of only being allowed if initiated from TransactDirect-registered static IP addresses and for refunds the submission of the ValidityID field becomes mandatory.

UPG's 3D Secure implementation for Visa's Verified by Visa and MasterCard/Europay's SecureCode initiatives is integrated directly into UPG's TransactDirect (Transact.ashx) creating a seamless, secure Internet card processing facility.

UPG's 3-D Secure implementation has the following features:

- Full compliance with Visa and MasterCard/Europay's 3-D Secure V1.02.
- Ease of integration using HTML form fields and browser client re-direction.
- Integrated directly into UPG's TransactDirect Transact.ashx internet card processing implementation.
- Transaction details are maintained by TransactDirect during the 3-D Secure process removing this liability from the merchants website.

Merchants wishing to use UPG's 3-D Secure implementation must have registered their requirement with UPG prior to sending live 3-D Secure requests. In addition, prior to going live, merchants must also undergo testing with UPG and/or their acquiring bank.

You can easily try out TransactDirect from within your own web site, call centre system or EPOS terminal to establish its speed, functionality and simplicity of integration.

Before you begin, you should be familiar with the use of HTML forms. Other areas of knowledge that would be useful but not essential are server-side scripting e.g. PERL, ASP, JSP, PHP etc. or programming languages such as C, C++, VB etc.

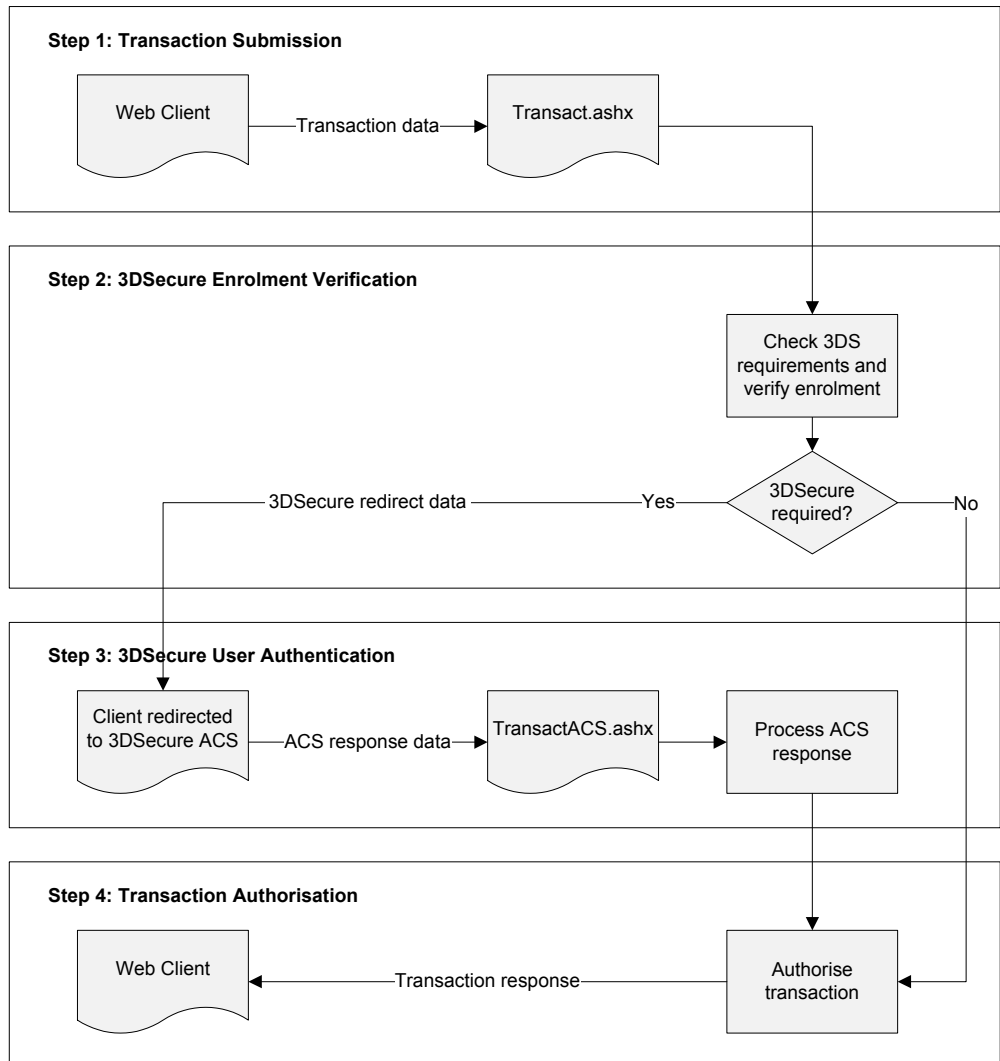
Note: For Internet merchants, although all transaction data is encrypted between a merchant and TransactDirect using TransactDirect's 128-bit Secure Socket Layer (SSL) environment, it is still recommended that Internet merchants obtain their own 128-bit SSL certificate. The use of 128-bit SSL is mandatory for merchants using web client re-direction of any kind in which card details are included. Merchants with their own 128-bit SSL certificate not only ensure in transit security of card details but help to ensure customer confidence by displaying an indication on their web client (browser) that the session is encrypted.

Table of Contents

Methods of Operation	5
Transaction Request.....	8
Mandatory Generic Transaction Request Fields.....	8
Card Keyed Transaction Request Fields.....	9
Swiped Transaction Request Fields.....	10
3-D Secure Transaction Request Fields.....	10
Generic Transaction Request Fields	11
Additional Form Fields.....	14
External 3-D Secure Authentication Request Fields	15
TransactDirect Message Types.....	16
Common Currency Codes.....	17
Example Field Names and Values for a Transaction Request.....	19
Example Using a Simple HTML Form.....	20
3-D Secure Transaction Response	22
3-D Secure ACS Response Fields	23
Web Client Call to Card Issuer's ACS	23
ACS Response Fields.....	24
Transaction Response	25
Default Response Following a Successful Transaction.....	26
Optional Responses Following Either a Successful or Unsuccessful Transaction.....	27
Additional Fields.....	34
Appendix 1: AVS / CV2 Primer	35
Appendix 2: How to implement a robust payment system for Internet Merchants.....	38
Appendix 3: Processing American Express and Diners Club Card Transactions	41
Appendix 4: Guide to handling referrals via TransactDirect.....	44
Appendix 5: Guide to handling deferred dispatch via TransactDirect	45
Appendix 6: Guide to handling continuous authority transactions via TransactDirect.....	47

Methods of Operation

The following is a typical sequence of events whereby transaction request data and transaction response data are passed securely over the Internet to TransactDirect. The term 'Web Client' will be used to indicate the party sending the transaction request data. Transact.ashx and TransactACS.ashx are the parties that receive the transaction request data and return the transaction responses to the Web Client.



Step 1: Web client sends transaction request data to TransactDirect

1. The web client (browser, Internet-aware application etc.) makes a secure TCP/IP socket connection (128-bit Secure Socket Layer version 3 or above – SSL – on port 443) to the TransactDirect web server at `https://www.universalpaymentgateway.com`.
2. Web client sends either an HTTP POST request (transaction information sent as form fields) or HTTP GET request (transaction information sent as query string attachments to: `https://www.universalpaymentgateway.com/secure/transact.ashx`

Step 2: 3-D Secure enrolment verification

If the request submitted in Step 1 requests 3-D Secure processing TransactDirect will validate the merchant's participation in 3-D Secure through UPG and then process a 3-D Secure enrolment request with Visa or MasterCard depending on the supplied card type.

TransactDirect will do one of three things dependent upon the result of the above steps:

1. If the merchant is not participating in 3-D Secure, 3-D Secure authentication was not requested, or the 3-D Secure enrolment verification process indicated that user authentication is not required then the transaction will immediately be passed for authorisation. Proceed to Step 4.
2. If the 3-D Secure enrolment verification process indicated that the user authentication is required then TransactDirect will return the details required to process user authentication in the format dependent upon the value of the `ThreeDSAction` request field:
 - a. If the `ThreeDSAction` field was set to `HTML` the response fields are sent to the client as a list of field names and values in the body of the HTTP response where the HTML is normally found e.g.

```
MD=<ENCODEDDATA>&PaReq=<ENCODEDDATA>&ACSURL=https%3a%2f%2fdropit.3dsecure.net%3a9443%2fPIT%2fACS
```

- b. If the `ThreeDSAction` field was set to `XML` the response fields are sent to the client as XML 1.0 formatted tags and values in the body of the HTTP where the HTML is normally found e.g.

```
<?xml version="1.0" encoding="UTF-8"?><veresponse><md>[ENCODEDDATA]</md><enrolled>Y</enrolled><pareq>[ENCODEDDATA]</pareq><acsurl>https://dropit.3dsecure.net:9443/PIT/ACS</acsurl></veresponse>
```

- c. If the `ThreeDSAction` field was set to `REDIRECT` TransactDirect issues a re-direct to the web client, redirecting it to the `Ret3DSAddress` with the response fields sent as query string attachments to the re-direct URL e.g.

```
http://www.myURL.com/3ds.asp?md=[ENCODEDDATA]&pareq=[ENCODEDDATA]&acsurl=https%3a%2f%2fdropit.3dsecure.net%3a9443%2fPIT%2fACS
```

- d. If the `ThreeDSAction` field was set to `ACSDIRECT` then TransactDirect will automatically redirect the client to the appropriate ACS URL for authentication. The ACS request will be configured to automatically redirect back to TransactDirect (`TransactACS.ashx`) on completion.

Note: This method provides for the simplest implementation of 3-D Secure and requires no additional coding or communication with the Web Client; however the ACS page will be displayed to the client in its original format.

- 3. If the TransactDirect is unable to continue with the process for any reason a standard error response will be returned dependent on the value of `ResponseAction` as detailed in Step 4.

Step 3: 3-D Secure user authentication

If 3-D Secure is used and cardholder authentication has been requested the cardholder will be directed to an Access Control Server (ACS). The ACS is managed by the issuing bank for the card being processed and will prompt the cardholder for information to verify their identity.

Once completed all fields returned from the ACS are passed to TransactDirect as an HTTP POST to:

<https://www.universalpaymentgateway.com/secure/transactacs.ashx>

Step 4: Authorisation and response

TransactDirect will authorise the provided transaction, including 3-D Secure details if processed and respond dependent upon the value of the `ResponseAction` request field:

- e. If the `ResponseAction` field was set to `HTML` the response fields are sent to the client as a list of field names and values in the body of the HTTP response e.g.

```
ResponseCode=00&Message=AUTHCODE:01223&CrossReference=03050711535801223303
```

- f. If the `ResponseAction` field was set to `XML` the response fields are sent to the client as XML 1.0 formatted tags and values in the body of the HTTP e.g.

```
<?xml version="1.0" encoding="UTF-8"?><transactionresponse><responsecode>00</responsecode><message>AUTHCODE:06166</message><crossreference>03050711584106166163</crossreference></transactionresponse>
```

- g. If the `ResponseAction` field was set to `REDIRECT` TransactDirect issues a re-direct to the web client, redirecting it to the `RetOKAddress` or `RetNotOKAddress` depending upon the transaction outcome, with the response fields sent as query string attachments to the re-direct URL e.g.

```
http://www.myURL.com/ReturnOKAddress.asp?ResponseCode=00&Message=AUTHCODE%3A01223&CrossReference=03050711535801223303
```

Transaction Request

The merchant will need a web page or some equivalent software e.g. call centre system or EPOS application, in order to collect the customer's card details and pass them, together with other transaction data, to TransactDirect. The passing of data to TransactDirect is accomplished using HTML form fields and/or query strings.

For a basic transaction, a form needs to be created that is set to POST its contents directly to the TransactDirect gateway:

```
<FORM METHOD="POST"
ACTION="https://www.universalpaymentgateway.com/secure/transact.ashx">
<!-- Insert form fields and other HTML code here -->
</FORM>
```

Note: If using the ResponseAction = REDIRECT option, once live transactions are being processed, it is not recommended to POST transaction data directly to the gateway. Please refer to Appendix 2 for further information.

The following tables detail the HTML form fields that are used to pass transaction data from the merchant's web client to TransactDirect. Every transaction that is passed to TransactDirect must include those fields listed in the 'Mandatory Generic Transaction Request Fields' table. Dependent upon the card details entry method, either chip/swipe or keyed, every transaction submitted must include the fields listed in 'Chip or Swiped Transaction Request Fields' or 'Card Keyed Transaction Request Fields' tables respectively. The fields from '3-D Secure Transaction Request Fields' are required in order to process 3-D Secure. A selection of optional fields are provided to allow access to further functionality

Mandatory Generic Transaction Request Fields

Field Name	Description	Req'd	Size	Type
Amount	The transaction amount, numeric, minor currency i.e. pence/cents etc. NO DECIMAL POINT e.g. £10.02 = 1002 (This is usually derived via an EPOS terminal, call centre system or Internet shopping application).	M	10 max.	N
CountryCode	ISO standard country code for merchant location. Use 826 for UK based merchants. Other options available on request. Although nominally mandatory, for backward compatibility defaults to 826 if not supplied.	M	3	N
CurrencyCode	ISO standard currency code of transaction. Use 826 for Sterling transactions. Other options available on request. Although nominally mandatory, for backward compatibility defaults to 826 if not supplied.	M	3	N

Dispatch	Used for deferred dispatch, options are NOW or LATER. Although nominally mandatory, for backward compatibility defaults to NOW if not supplied. If supplied as LATER, DispatchLaterAmount becomes mandatory.	M	5 max.	A
MerchantID	UPG merchant ID. Use 0000018 for testing.	M	7	N
MessageType	See later table for acceptable message types.	M	V	A
ResponseAction	Used to tell TransactDirect which method to use for the return of transaction response data. Options are: HTML XML REDIRECT	M	V	A

M = Mandatory, A = Alpha-Numeric, N = Numeric, V = Variable

Card Keyed Transaction Request Fields

Field Name	Description	Req'd	Size	Type
CardNumber	Card number.	M	20 max.	N
EMVTerminalType	Defined in EMV, contact UPG. Currently mandatory for E-Commerce transactions and optional for any other card keyed transaction. Use 32 for testing.	M/O	2	N
ExpMonth	Expiry month.	M	2	N
ExpYear	Expiry year.	M	2	N
IssueNumber	Issue number.	M/O*	2 max.	N
StartMonth	Start month.	M/O*	2	N
StartYear	Start year.	M/O*	2	N

M = Mandatory, O = Optional, N = Numeric, *Required for certain card types

Swiped Transaction Request Fields

Field Name	Description	Req'd	Size	Type
EMVTerminalType	Defined in EMV, please discuss with UPG. Use 32 for testing.	M	2	N
Track2Data	The unaltered track 2 equivalent data obtained from the chip or the unaltered track 2 read of a magnetic strip. Note: All track 2 reads of a magnetic strip must commence with the Start Sentinel character “;”, contain the “=” field separator, and finish with the End Sentinel character “?” and Longitudinal Redundancy Checksum (LRC) character.	M	40 max.	N

M = Mandatory, A = Alpha-Numeric, N = Numeric

Example of Track 2 Data Read From Magnetic Strip

```
;5301250070000191=04061010912345678901?<
```

3-D Secure Transaction Request Fields

Field Name	Description	Req'd	Size	Type
EchoThreeDSInformation	If set, passes back the card type used in the transaction as a two character code. Options are YES or NO. Defaults to NO if not supplied. If set to YES, the card type is returned as the additional response field CardType.	O	2 or 3	A
Ret3DSAddress	If ThreeDSAction = REDIRECT is used, this is the address (URL) to which the web client will be redirected with ACS information. The fields required to perform payer authentication are appended to this address as query string fields.	O	V	A
PurchaseDescription	Description of purchase. Useful when requesting a UPG 3-D Secure lookup.	O	255 max.	A
ThreeDSAction	Used to indicate requirement of 3-D Secure processing and to tell TransactDirect which method to use for the return of ACS data. Options are: NONE (or omitted) HTML XML REDIRECT ACSDIRECT	M	V	A

ThreeDSCAContinueOnFail	Options are YES or NO. Defaults to NO if not supplied. If set to YES, TransactDirect will allow a transaction to continue if the ACS response indicates that the cardholder failed verification .	O	2 or 3	A
ThreeDSPassword	The 3-D Secure password issued to each merchant by UPG.	M	8	A
ThreeDSTest	Options are YES or NO. Defaults to NO if not supplied. If set to YES, TransactDirect will process 3-D Secure traffic through the 3-D Secure test system.	M	2 or 3	A
ThreeDSVEContinueOnError	Options are YES or NO. Defaults to NO if not supplied. If set to YES, TransactDirect will allow a transaction to continue if an error occurred verifying card enrolment details .	O	2 or 3	A
TransactionId	A transaction identifier derived by merchant. Must be 20 digits long and unique for every transaction.	M	20	N

M = Mandatory, O = Optional, N = Numeric, *Required for certain card types

Generic Transaction Request Fields

Field Name	Description	Req'd	Size	Type
AuthorisationCode	To be sent when MessageType is prefixed with PAYMENT_ONLY_ (ignored if sent with any other MessageType) indicating that prior authorisation has been given by the merchant's acquiring bank e.g. following a referral when the merchant has contacted the bank's voice authorisation centre. If MessageType is prefixed with PAYMENT_ONLY_ and AuthorisationCode is not sent, TransactDirect will derive its own authorisation code for this transaction.	O	9 max.	A
AVSCV2Check	If set, passes back the result of the AVS/CV2 check. Options are YES or NO Defaults to NO if not supplied. If set to YES, the AVS and/or CV2 result is returned as the response field AVSCV2Check. Note: Regardless of using this field, accepting or rejecting a transaction based on the AVS/CV2 result is dependent on the AVS/CV2 configuration, as set in the TMS facility.	O	2 or 3	A

CrossReference	<p>This is sent in lieu of the card details (card number, track 2 data, expiry month and year, start month and year, issue number) and is used for completing transactions that were originally submitted as <code>Dispatch = LATER</code> or re-billing submitted with a <code>MessageType</code> of <code>SALE_CA</code>.</p> <p>Note: Merchants who wish to conduct transactions using Cross References must do so from a static IP address(es) that have been registered with TransactDirect.</p>	O	50 max.	A
CV2	<p>Card Verification Value normally printed after the card number on the card's magnetic strip (if applicable).</p> <p>Note: The CV2 value should not be stored under any circumstances – the value should be passed directly to TransactDirect. See also <code>AVSCV2Check</code> and <code>EchoAVSCV2ResponseCode</code>.</p>	O	3 or 4	N
DispatchLaterAmount	<p>The total amount of the transaction. Numeric, minor currency i.e. pence/cents etc. NO DECIMAL POINT e.g. £10.02 = 1002 (This is usually derived via an EPOS terminal, call centre system or Internet shopping application). Mandatory for transactions submitted as <code>DISPATCH=LATER</code>.</p>	M/O	10 Max	N
DuplicateDelay	<p>This delay helps to prevent duplicate transactions passing through the gateway e.g. in the circumstance that a user clicks a submission button more than once by accident. Supply the delay required in seconds e.g. 30 = 30 seconds. Supplying a value of 0 effectively disables the duplicate check. The default value is configurable by request, initially set to 300 (5 minutes).</p>	O	4 max.	N
EchoAmount	<p>If set, passes back the transaction amount following a successful authorisation. This option is normally used when a merchant wants to be absolutely sure that the amount has not been tampered with in transit. Options are <code>YES</code> or <code>NO</code>. Defaults to <code>NO</code> if not supplied. If set to <code>YES</code>, the amount is returned as the additional field <code>Amount</code>.</p>	O	2 or 3	A
EchoAVSCV2ResponseCode	<p>If set, passes back the raw AVS/CV2 result received from the acquiring bank as a six character code. Options are <code>YES</code> or <code>NO</code>. Defaults to <code>NO</code> if not supplied. If set to <code>YES</code>, the raw AVS/CV2 result is returned as the additional response field <code>AVSCV2ResponseCode</code>.</p> <p>Note: Regardless of using this field, accepting or rejecting a transaction based on the AVS/CV2 result is dependent on the AVS/CV2 configuration, as set in the TMS facility.</p>	O	6	N

EchoCardType	If set, passes back the card type used in the transaction as a two character code. Options are YES or NO. Defaults to NO if not supplied. If set to YES, the card type is returned as the additional response field CardType.	O	2 or 3	A
EchoReceiptInformation	Passes back all the information that a merchant needs to produce a customer's receipt. Options are YES or NO. Defaults to NO if not supplied. If set to YES, the receipt information is returned as the additional field ReceiptInformation.	O	2 or 3	A
EchoReferralTelephoneNumber	Passes back a referral telephone number from the acquirer/issuer, if provided, when the transaction is referred. Options are YES or NO. Defaults to NO if not supplied. If set to YES, the referral telephone number is returned as the additional response field ReferralTelephoneNumber.	O	2 or 3	A
QAName	Customer's name. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAName.	O	30 max.	A
QAAddress	Required for AVS check. Customer's address. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAAddress.	O	100 max.	A
QAPostcode	Required for AVS check. Customer's postcode. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAPostCode.	O	10 max.	A
QAEmailAddress	Customer's email address. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAEmailAddress.	O	50 max.	A
QAPhoneNumber	Customer's telephone number. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAPhoneNumber.	O	30 max.	A
QAProducts	Details of products or services purchased. Contents of this field are used to populate the TMS. If populated, the field is automatically returned as the additional response field QAProducts.	O	168 max.	A

RetNotOKAddress	If ResponseAction = REDIRECT is used, this is the address (URL) to which the web client will be redirected following an unsuccessful transaction. The TransactDirect response code, error message and if the transaction resulted in a referral or decline, the Cross Reference together with any other optional fields are appended to this address as query string fields. This address can be the same as RetOKAddress.	O	V	A
RetOKAddress	If ResponseAction = REDIRECT is used, this is the address (URL) to which the web client will be redirected following a successful transaction. The TransactDirect response code, authorisation message and Cross Reference together with any other optional fields are appended to this address as query string fields. This address can be the same as RetNotOKAddress.	O	V	A
TerminalType	The APACS Standard 30 terminal type. Defaults to 2004 for EPOS transactions and to 4081 for Internet delivered transactions. Contact UPG for alternative codes.	O	4	N
ValidityID	Is used by TransactDirect in conjunction with MerchantID to provide additional security. ValidityID will be issued by UPG for merchants with registered IP addresses set up to conduct refunds using TransactDirect. Mandatory for refunds. This field was originally known as MerchantPassword.	M/O	10 max.	A

O = Optional, A = Alpha-Numeric, N = Numeric

Additional Form Fields

Additional form or query string fields may be sent to TransactDirect as necessary and are returned unaltered.

Example

Custom Field Name	Description
BillingReferenceID	Additional form field or string.
AccountNumber	Additional form field or string.

Note: Please ensure that the names of any additional fields do not conflict with any that appear in this or related documents.

Note: If using the ResponseAction = REDIRECT option, and using a browser-based web client, there may be a browser-imposed limit of approximately 2000 characters for a query string. If you are going to submit or retrieve transaction data via a query string, be aware that the query string may be truncated if it exceeds this length or a client error may be created.

External 3-D Secure Authentication Request Fields

Where 3-D Secure is performed outside of the Transact.ashx system, for example using the original UPG 3-D Secure pages or a 3rd party 3-D Secure system, the 3-D Secure result fields can be still be supplied to Transact.ashx for processing.

Field Name	Description	Req'd	Size	Type
Authenticated	<p>"Y" for successfully authenticated with cardholder's issuing bank.</p> <p>"N" for unsuccessful authentication with cardholder's issuing bank.</p> <p>"U" for an unsuccessful authentication during which an error was raised.</p>	O	1	A
CAVV	Cardholder Authentication Value. Supplied by card issuer as part of a successful 3-D Secure authentication.	O	32 max	A
ECI	Electronic Commerce Indicator. Supplied by card issuer as part of a successful 3-D Secure authentication.	O	2	N
Enrolled	<p>"Y" for card enrolled for 3-D Secure as determined by the card scheme directory server.</p> <p>"N" for card not enrolled for 3-D Secure as determined by the card scheme directory server.</p> <p>"U" for an unsuccessful cardholder enrolment attempt during which an error was raised.</p>	O	1	A
TransactionID	A transaction identified derived by merchant. Must be unique for every transaction.	O	20	A

O = Optional, A = Alpha-Numeric, N = Numeric

TransactDirect Message Types

MessageType	Description
SALE_SWIPED	Sale transaction, card details read from magnetic strip at point of sale, equivalent to SALE_CARD without support for chip read. Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
SALE_KEYED	Sale transaction, card details keyed at point of sale (cardholder present). Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
SALE_CNP	Sale transaction, cardholder not present (typically from call-centre i.e. telephone, mail order, etc.). Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
SALE_CA	Sale transaction with continuous authority. Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
SALE_CASHBACK_SWIPED	Sale transaction with cash back, card details read from magnetic strip at point of sale, equivalent to SALE_CASHBACK_CARD without support for chip read. Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
SALE_CASHBACK_KEYED	Sale transaction with cash back, card details keyed at point of sale (cardholder present). Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
ESALE_SWIPED	E-Commerce (Internet) sale transaction, card swiped by cardholder (both merchant and cardholder not present). Equivalent to E-SALE_CARD without support for chip read. Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
ESALE_KEYED	E-Commerce (Internet) sale transaction, card keyed by cardholder (both merchant and cardholder not present). Note: Maybe prefixed with PAYMENT_ONLY_ see following note.
REFUND_SWIPED	Refund transaction, card details read from magnetic strip at point of sale, equivalent to REFUND_CARD without support for chip read.
REFUND_KEYED	Refund transaction, card details keyed at point of sale (cardholder present).
REFUND_CNP	Refund transaction, cardholder not present (typically from call-centre i.e. telephone, mail order, etc.).

Note:

- Transactions prefixed with `PAYMENT_ONLY_`, are not forwarded to the bank for authorisation. Such transactions are sent for settlement on the assumption that the merchant has obtained authorisation from some other source e.g. from a call to the bank's voice authorisation centre. `PAYMENT_ONLY_` transactions are typically used in situations where the original transaction resulted in a referral or when presenting transaction to TransactDirect following a period of communications failure. Transactions prefixed with `PAYMENT_ONLY_` are only acceptable if the source IP address has been registered with TransactDirect. Please contact UPG to register. The processing of referrals can also be carried out without IP registration using the TMS.

- Transactions conducted using the original transaction's Cross Reference in lieu of card details are only acceptable if the source IP address has been registered with TransactDirect. Please contact UPG to register.
- Refunds are only acceptable if the source IP address has been registered with TransactDirect. Please contact UPG to register.
The processing of refunds can also be carried out without IP registration using the TMS.
- Certain message types, for example, continuous authority (SALE_CA etc.) and sale with cash back (SALE_CASHBACK_SWIPED etc.) are only available by prior arrangement with the merchant's acquiring bank.
- Standard Internet-based sale transactions will usually be flagged as ESALE_KEYED.
- ESALE_KEYED should only be used in situations where the cardholder perceives the transaction to be Internet-based, such as purchasing from a web site/on-line store. If the Internet is used purely for the transport of information from the merchant directly to the gateway then the appropriate cardholder present or not present message type should be used rather than the 'E' equivalent.

Common Currency Codes

Currency	ISO-4217 Code (Numeric)
Australian Dollar	036
Canadian Dollar	124
Czech Koruna	203
Danish Krone	208
Hong Kong Dollars	344
Icelandic Krona	352
Japanese Yen	392
Norwegian Krone	578
Singapore Dollars	702
Swedish Krona	752
Swiss Franc	756
Pound Sterling	826
US Dollars	840
Euro	978

Note: Merchants must have obtained prior clearance from their UK acquiring bank (acquirer) before accepting multi-currency transactions. Certain acquirers will require separate merchant numbers to be issued. Not all acquirers accept all of these currencies whilst some accept many more. Multi-currency transactions must be identified by their numeric three-digit currency code, as per ISO-4217.

Example Field Names and Values for a Transaction Request

Example illustrating the basic information plus 3-D Secure fields sent in a transaction request:

Field Name	Example
Amount	1499
AVSCV2Check	YES
CardNumber	5301250070000191
CurrencyCode	826
CountryCode	826
CV2	419
Dispatch	NOW
EMVTerminalType	32
ExpMonth	06
ExpYear	08
MerchantID	0000018
MessageType	ESALE_KEYED
QAName	Martin Brewster
QAAddress	25 The Larches Narborough Leicestershire
QAPostcode	LE10 2RT
QAEmailAddress	m.brewster@longshot.com
QAPhoneNumber	+44 (0) 2084 235778
QAProducts	102293/D:Phone adapter
ResponseAction	REDIRECT
RetOKAddress	https://www.yourwebsite.com/shopping/ok.asp
RetNotOKAddress	https://www.yourwebsite.com/shopping/notok.asp
ThreeDSAction	XML
Authenticated	Y
ECI	05
CAVV	AAABAnMVNHgAAAAARU0AAAAA=
TransactionID	00000000000000000100

Example Using a Simple HTML Form

Below is an example of a simple HTML form containing the required code:

```
<form method="post"
action="https://www.universalpaymentgateway.com/secure/transact.ashx">
<input type="hidden" name="ResponseAction" value="HTML">
<input type="hidden" name="MerchantID" value="0000877">
<input type="hidden" name="MessageType" value="ESALE_KEYED">
<input type="hidden" name="Dispatch" value="NOW">
<input type="hidden" name="CountryCode" value="826">
<input type="hidden" name="CurrencyCode" value="826">
<input type="hidden" name="AVSCV2Check" value="YES">
<input type="hidden" name="ThreeDSTest" value="YES">
<input type="hidden" name="ThreeDSAction" value="ACSDIRECT">
<input type="hidden" name="ThreeDSPassword" value="NeTb3714">
<input type="hidden" name="TransactionID" value="00000000000000000210">
<table border="0" cellpadding="0" cellspacing="2">
<tr>
<td><b>Amount in minor currency</b><br><i>(normally provided
by<br>shopping trolley)</i></td>
<td><input type="text" name="Amount" size="10" maxlength="10"></td>
</tr>
<tr>
<td><b>Card Number</b></td>
<td><input type="text" name="CardNumber" maxlength="20"></td>
</tr>
<tr>
<td><b>Expiry Date (Month/Year)</b></td>
<td><input type="text" name="ExpMonth" size="2" maxlength="2"></input
type="text" name="ExpYear" size="2" maxlength="2"></td>
</tr>
<tr>
<td>Issue Number</td>
<td><input type="text" name="IssueNumber" size="2" maxlength="2">
<i>Maestro & Solo cards only</i></td>
</tr>
<tr>
<td>Start Date (Month/Year)</td>
<td><input type="text" name="StartMonth" size="2" maxlength="2"></input
type="text" name="StartYear" size="2" maxlength="2"> <i>if applicable</i></td>
</tr>
<tr>
<td><b>CV2 Value</b></td>
<td><input type="text" name="CV2" size="4" maxlength="4"></td>
</tr>
<tr>
<td>Name</td>
<td><input type="text" name="QAName" size="30" maxlength="30"></td>
</tr>
```

```

<tr>
  <td>Address</td>
  <td><textarea name="QAAddress" rows=3></textarea></td>
</tr>
<tr>
  <td>Postcode</td>
  <td><input type="text" name="QAPostcode" size="10" maxlength="10"></td>
</tr>
<tr>
  <td>Telephone Number</td>
  <td><input type="text" name="QAPhoneNumber" size="30"
maxlength="30"></td>
</tr>
<tr>
  <td>Email Address</td>
  <td><input type="text" name="QAEmailAddress" size="30"
maxlength="50"></td>
</tr>
<tr>
  <td>Products Ordered<br><i>(normally provided by<br>shopping
trolley)</i></td>
  <td><textarea name="QAProducts" rows=3></textarea></td>
</tr>
<tr>
  <td align="center" colspan="2"><br><input type="submit" value="Authorise
transaction"></td>
</tr>
</table>
</form>

```

Note:

- *In instances where the merchant carries out their own settlement, merchants may be set up for authorisation only rather than the default simultaneous authorisation and settlement. Please contact UPG for further information on implementation and billing.*
- *In instances where the merchant carries out their own authorisation or in instances in which an authorisation has been obtained by some other means e.g. via telephone following a referral or communications failure, merchants may instruct the gateway to perform settlement only rather than the default simultaneous authorisation and settlement. Please refer to the TransactDirect Message Types section.*

3-D Secure Transaction Response

If the `ThreeDSAction` field was set and the `Transact.ashx` has determined that user authentication is required then an appropriate 3-D Secure response will be returned. Otherwise a standard Transaction Response will be returned.

1. If the `ThreeDSAction` field was set to `HTML` the response fields are sent to the client as a list of field names and values in the body of the HTTP response where the HTML is normally found e.g.

```
MD=<ENCODEDDATA>&PaReq=<ENCODEDDATA>&ACSURL=https%3a%2f%2fdropit.3dsecure.net%3a9443%2fPIT%2fACS
```

2. If the `ThreeDSAction` field was set to `XML` the response fields are sent to the client as XML 1.0 formatted tags and values in the body of the HTTP where the HTML is normally found e.g.

```
<?xml version="1.0" encoding="UTF-8"?><veresponse><md>[ENCODEDDATA]</md>
<enrolled>Y</enrolled><pareq>[ENCODEDDATA]</pareq><acsurl>https://dropit.3dsecure.net:9443/PIT/ACS</acsurl></veresponse>
```

3. If the `ThreeDSAction` field was set to `REDIRECT` TransactDirect issues a re-direct to the web client, redirecting it to the `Ret3DSAddress` with the response fields sent as query string attachments to the re-direct URL e.g.

```
http://www.myURL.com/3ds.asp?md=[ENCODEDDATA]&pareq=[ENCODEDDATA]&acsurl=https%3a%2f%2fdropit.3dsecure.net%3a9443%2fPIT%2fACS
```

4. If the `ThreeDSAction` field was set to `ACSDIRECT` then TransactDirect will automatically redirect the client to the appropriate ACS URL for authentication. The ACS request will be configured to automatically redirect back to TransactDirect (`TransactACS.ashx`) on completion.

Note: This method provides for the simplest implementation of 3-D Secure and requires no additional coding or communication with the Web Client; however the ACS page will be displayed to the client in its original format.

3-D Secure ACS Response Fields

If the `ThreeDSAction` was set to `HTML`, `XML` or `REDIRECT` the response will include the following fields to allow the Web Client to handle the ACS redirection. For example if the Web Client needs to embed the ACS prompt within a branded web page.

Field Name	Description	Size	Type
ACSURL	Access Control Server URL. Used in redirecting the client browser to the card issuer's 3D Secure authentication host.	V	A
MD	Merchant Data. All merchant data is retained by the <code>Transact.ashx</code> page. The MD field is used to allow this data to be retrieved and must be included unaltered in the subsequent calls to the ACSURL and <code>TransactACS.ashx</code> .	V	A
PaReq	The full 3D Secure request as returned by the card scheme enrolment verification server. This should be passed in its entirety to the issuer's ACS.	V	A

Web Client Call to Card Issuer's ACS

The web client (browser, Internet-aware application etc.) makes a secure TCP/IP socket connection (128-bit Secure Socket Layer version 3 or above) to the card issuer's 3D Secure web server at ACSURL by sending an HTTP POST request (transaction information sent as form fields) to ACSURL.

Field Name	Description	Req'd	Size	Type
MD	Merchant Data. This field should be passed unaltered from the <code>Transact.ashx</code> response. <i>Note: The Web Client may opt to store this value locally rather than pass it to the ACS but it must be included in the call to <code>TransactACS.ashx</code>.</i>	O	V	A
PaReq	The full 3D Secure request. This field should be passed unaltered from the <code>Transact.ashx</code> response.	M	V	A
TermUrl	Termination URL. This is the address that the issuer's ACS will call after payer authentication is complete.	O	50 max.	A

The `TermUrl` field can be used to direct the ACS response back to the Web Client or directly to `TransactACS.ashx` to complete the transaction. If `TermUrl` is used to redirect back to `TransactACS.ashx` then MD becomes a mandatory field.

ACS Response Fields

If `TermUrl` is set to direct responses to the Web Client then the following fields will be returned. All fields should be forwarded in their entirety to `TransactACS.ashx` to complete the transaction.

Field Name	Description	Req'd	Size	Type
MD	Merchant Data. This field should be passed unaltered to <code>TransactACS.ashx</code> .	M	V	A
PaRes	The full 3D Secure response as returned by the cardholder's issuer. This field should be passed unaltered to <code>TransactACS.ashx</code> .	M	V	A

If `TermUrl` is set to direct to `TransactACS.ashx` then these fields will be passed automatically.

Transaction Response

If the `ResponseAction` field was set to `HTML` the response fields are sent to the client as a list of field names and values in the body of the HTTP response where you would normally expect to find the HTML e.g.

```
ResponseCode=00&Message=AUTHCODE:01223&CrossReference=03050711535801223303
```

If the `ResponseAction` field was set to `XML` the response fields are sent to the client as XML 1.0 formatted tags and values in the body of the HTTP response where you would normally expect to find the HTML e.g.

```
<?xml version="1.0" ?><transactionresponse><responsecode>00</responsecode><message>AUTHCODE:06166</message><crossreference>03050711584106166163</crossreference></transactionresponse>
```

If the `ResponseAction` field was set to `REDIRECT` TransactDirect issues a re-redirect to the web client, re-directing to the `ReturnOKAddress` or `ReturnNotOKAddress` depending upon the transaction outcome, with the response fields sent as query string attachments to the redirect URL e.g.

```
http://www.myURL.com/ReturnOKAddress.asp?ResponseCode=00&Message=AUTHCODE%3A01223&CrossReference=03050711535801223303
```

Transaction Outcome	Redirection URL
Successful transaction	RetOKAddress
Card referred	RetNotOKAddress
Card declined	RetNotOKAddress
Problem with card e.g. invalid card number, expired card etc	RetNotOKAddress
Processing error	RetNotOKAddress

Default Response Following a Successful Transaction

The result of the transaction is passed back in the following fields.

Field Name	Contents	Size	Type
ResponseCode	The TransactDirect response code. See table.	2	N
Message	The transaction message either as delivered by the bank or by TransactDirect. This is the message that should be displayed to the merchant on an EPOS system or call centre application and to the cardholder on an Internet web site implementation. Typical examples are: AUTHCODE:123456 CARD EXPIRED CARD REFERRED CARD DECLINED CARD DECLINED - KEEP CARD AVS CV2 DECLINED ERROR XXXX	80 max.	A
CrossReference	The unique character string supplied by TransactDirect to identify this transaction.	50 max.	A

O = Optional, A = Alpha-Numeric, N = Numeric

TransactDirect Response Code	Description
00	Transaction successful / authorised
02	Card referred
03	Retailer unknown
04	Keep card decline
05	Card declined
11	Invalid card details
12	Invalid request
30	Exception

Optional Responses Following Either a Successful or Unsuccessful Transaction

Echo Amount

Field Name	Description	Size
Amount	<p>Amount sent with transaction request to acquiring bank or, in the event of a payment only transaction, accepted by TransactDirect. Only returned if requested, and in minor currency value i.e. pence/cents etc.</p> <p>Returned if transaction request field <code>EchoAmount</code> was set to YES. Not returned if TransactDirect <code>ResponseCode</code> = 30</p>	10 max.

Echo AVS/CV2 Response Code

Field Name	Description	Size
AVSCV2ResponseCode	<p>The raw AVS/CV2 code returned by the acquiring bank – see following tables. Only sent back if requested.</p> <p>Returned if transaction request field <code>EchoAVSCV2ResponseCode</code> was set to YES. Not returned if TransactDirect <code>ResponseCode</code> = 30</p>	6

The AVS/CV2 Response Code is made up of six characters and is sent back in the raw form that is received from the acquiring bank.

Position 1 Value	Position 1 Value Description
0	No additional information available.
1	CV2 not checked.
2	CV2 matched.
4	CV2 not matched.
8	Reserved

Position 2 Value	Position 2 Value Description
0	No additional information available.
1	Postcode not checked.
2	Postcode matched.
4	Postcode not matched.
8	Postcode partially matched.

Position 3 Value	Position 3 Value Description
0	No additional information available.
1	Address numeric not checked.
2	Address numeric matched.
4	Address numeric not matched.
8	Address numeric partially matched.

Position 4 Value	Position 4 Value Description
0	Authorising entity not known
1	Authorising entity – merchant host
2	Authorising entity – acquirer host
4	Authorising entity – card scheme
8	Authorising entity – issuer

Position 5 Value	Position 5 Value Description
0	Reserved
1	Reserved
2	Reserved
4	Reserved
8	Reserved

Position 6 Value	Position 6 Value Description
0	Reserved
1	Reserved
2	Reserved
4	Reserved
8	Reserved

Note:

- *Values other than 0, 1, 2, 4 or 8 are not valid in character positions 1 to 4.*
- *A value of zero in any character position indicates that no additional information is available.*
- *If the Authorising Entity is not known then character position 4 is set to zero and the authoriser is assumed to be the issuer.*

Echo Card Type

Field Name	Description	Size
CardType	<p>The card type used for the transaction – see following table. Only sent back if requested.</p> <p>Returned if transaction request field <code>EchoCardType</code> was set to <code>YES</code>.</p> <p>Not returned if TransactDirect <code>ResponseCode</code> = 30</p>	2

Card Type Code	Card Type
AM	American Express
CF	Clydesdale Financial Services
DI	Diners Club
EL	Electron
JC	JCB
MA	International Maestro
MC	Mastercard
SO	Solo
ST	Style
SW	Domestic Maestro (formerly known as Switch)
VC	Visa Credit
VD	Visa Debit
VP	Visa Purchasing

Echo Receipt Information

Field Name	Description	Size
ReceiptInformation	<p>This returns all the information that a merchant needs to produce a customer receipt. Please contact UPG to enable this facility.</p> <p>Returned if transaction request field EchoReceiptInformation was set to YES. Not returned if TransactDirect ResponseCode = 30</p>	387 max.

Structure of the Receipt Information field

No	Field Name and Contents	Req'd	Size	Type
1	BANK MERCHANT NUMBER	M	15 max.	A
2	UNIT SEPARATOR [US]	M	1	
3	CARD TYPE – Full Name	M	50 max.	A
4	UNIT SEPARATOR [US]	M	1	
5	MERCHANT NAME	M	50 max.	A
6	UNIT SEPARATOR [US]	M	1	
7	MERCHANT LOCATION	M	50 max.	A
8	UNIT SEPARATOR [US]	M	1	
9	DATE - "YYMMDD"	M	6	N
10	UNIT SEPARATOR [US]	M	1	
11	TIME – "HHMM"	M	4	N
12	UNIT SEPARATOR [US]	M	1	
13	TRANSACTION TYPE	M	20 max.	A
14	UNIT SEPARATOR [US]	M	1	
15	CARD NUMBER – First 4 digits and last 4 digits with the remaining digits appearing as asterisks	M	20 max.	N
16	UNIT SEPARATOR [US]	M	1	
17	START DATE – "YYMM"	O	0 or 4	N
18	UNIT SEPARATOR [US]	M	1	
19	EXPIRY DATE – "YYMM"	M	4	N
20	UNIT SEPARATOR [US]	M	1	
21	ISSUE NUMBER	O	2 max.	N
22	UNIT SEPARATOR [US]	M	1	
23	CARD DETAILS ENTRY METHOD	M	20 max.	A
24	UNIT SEPARATOR [US]	M	1	
25	TERMINAL IDENTIFIER	M	8	N

26	UNIT SEPARATOR [US]	M	1	
27	MESSAGE NUMBER	M	4	N
28	UNIT SEPARATOR [US]	M	1	
29	RESPONSE MESSAGE TEXT	M	80 max.	A
30	UNIT SEPARATOR [US]	M	1	
31	TRANSACTION AMOUNT - minor currency units	M	11 max.	N
32	UNIT SEPARATOR [US]	M	1	
33	CASH BACK AMOUNT - minor currency units (This field will be returned as empty unless a merchant is set up to process cash back and has passed a cash back amount to TransactDirect).	O	11 max.	N
34	UNIT SEPARATOR [US]	M	1	
35	GRATUITY AMOUNT - minor currency units (This field will be returned as empty unless a merchant is set up to process gratuities and has passed a gratuity amount to TransactDirect).	O	11 max.	N

M = Mandatory, O = Optional, A = Alpha-Numeric, N = Numeric

ASCII control characters used in the Receipt Information field

Separator	ASCII Character Code
Unit separator [US]	31

Echo Referral Telephone Number

Field Name	Description	Size
ReferralTelephoneNumber	The referral telephone number passed to TransactDirect by the merchant's acquirer in the event of a transaction being referred. Only sent back if requested. Returned if transaction request field EchoReferralTelephoneNumber was set to YES. Not returned if TransactDirect ResponseCode = 30	16 max.

Note: Most UK acquirers do not support this feature and merchants should contact the standard telephone number provided by their acquiring bank in the event of a referral.

The ReferralTelephoneNumber field is only passed back in the event of a referral. The ReferralTelephoneNumber field is not passed back if the acquirer does not pass the referral telephone number to TransactDirect as part of the APACS Standard 30 response.

Echo 3-D Secure Result

Field Name	Description	Size
ThreeDS	The 3-D Secure details as returned from the verify enrolment and payer authentication stages. Comma separated in UPG 2.1 compliant form. Returned if transaction request field <code>EchoThreeDSInformation</code> was set to <code>YES</code> . Not returned if 3-D Secure processing has not taken place	60 max.

Structure of the 3-D Secure Information field

No	Field Name and Contents	Req'd	Size	Type
1	ENROLLED	M	1	A
2	SEPARATOR [COMMA]	M	1	
3	AUTHENTICATED	M	1	A
4	SEPARATOR [COMMA]	M	1	
5	ECI	M	2	N
6	SEPARATOR [COMMA]	M	1	
7	CAVV	M	32 max.	A
8	SEPARATOR [COMMA]	M	1	
9	TRANSACTION IDENTIFIER	M	20	N

3-D Secure Error Details

Field Name	Description	Size
ThreeDSErrorCode	Code issued by 3-D Secure MPI if either enrolment verification or 3D Secure authentication failed with an error.	V
ThreeDSErrorDetail	Error description issued by 3-D Secure MPI if either enrolment verification or 3D Secure authentication failed with an error.	V

AVS/CV2 Check Response

Field Name	Description	Size
AVSCV2Check	AVS/CV2 check response – see following table. Only sent back if requested. Returned if transaction request field AVSCV2Check was set to YES. Not returned if TransactDirect ResponseCode = 30	30 max.

AVS / CV2 Check Response Message	Description
ALL MATCH	AVS and CV2 match.
SECURITY CODE MATCH ONLY	CV2 match only.
ADDRESS MATCH ONLY	AVS match only.
NO DATA MATCHES	No matches for AVS and CV2.
DATA NOT CHECKED	Supplied data not checked.
SECURITY CHECKS NOT SUPPORTED	Card scheme does not support checks.
UNKNOWN RESPONSE	Unrecognised AVS/CV2 response from issuer.

AVS and CV2 checks are supported by Visa (both Credit and Debit), Mastercard/Europay (Both Credit and Debit –Maestro) and American Express. The AVS check is only applicable to cards issued by UK banks.

Normal AVS / CV2 Operating Practice

As part of the AVS/CV2 design, responses are passed back along with the authorisation outcome. This can result in a situation where the transaction has been authorised by the card issuer, but the AVS/CV2 checks have returned negative results. At this point, the merchant may decide not to proceed with the transaction. In these circumstances, under normal UK banking practice, a merchant would need to cancel, reverse or refund the transaction. This is often not practical to achieve in situations where the merchant is not present for the transaction, such as Internet retailers.

TransactDirect removes the necessity for the merchant to explicitly carry out the cancellation, reversal or refund by providing the merchant with AVS/CV2 acceptance parameters governing what action to take dependent upon the AVS/CV2 result.

Merchants can set their own AVS/CV2 acceptance parameters using the TransactDirect TMS. See Appendix 1.

Additional Fields

Additional form or query string fields may be sent to TransactDirect as necessary and are returned unaltered (field values are URL encoded prior to return if `ResponseAction = REDIRECT`).

Note: Fields pertaining to the original transaction request are not passed back e.g. CardNumber, ExpYear, ExpMonth, apart from the customer details fields QAName, QAAddress, QAPostcode, QAPhoneNumber, QAEmailAddress and QAProducts.

Appendix 1: AVS / CV2 Primer

The UK card industry can conduct two optional anti-fraud checks that may be carried out at the same time as an authorisation. Known as AVS and CV2, they have been developed in response to the increase in fraudulent transactions, notably those where the cardholder is not present at the point of sale, for example mail order or Internet transactions.

AVS (Address Verification Service)

The Address Verification Service (AVS) is used to confirm that the postal address given by the cardholder during a transaction matches the cardholder's billing address held by the card issuing bank.

The AVS checks the numeric values of the full address and postcode given by the cardholder against the records held by their card issuer. Upon submission of a full address and postcode, TransactDirect will derive the AVS check value and pass it to the issuing bank for verification.

CV2 (Card Verification Value)

The name CV2 is actually a collective term derived from Card Verification Value (CVV2) used by Visa and Card Verification Check (CVC) used by Mastercard (Europay). It is a three or four digit number usually found printed after the card number on the signature strip on the back of a card. The purpose of this number and the optional check that can be carried out with it is to confirm that the cardholder is actually in possession of the card.

During an authorisation, the CV2 is checked along with the main card number, however, the key difference is that whereas the card number is sometimes stored in transaction terminals and printed on till receipts - thereby making them easy targets - the CV2 is never stored or printed. In the event of any stored or printed card details ending up in the wrong hands, they alone would be of no use to anyone intent on passing fraudulent transactions to a merchant set up to use CV2.

Using AVS and CV2 with TransactDirect

Historically, the banking industry decided that the AVS/CV2 result should not have an impact on whether or not a bank authorises or declines a transaction leaving the decision to continue with the transaction up to the merchant. If the merchant decides not to proceed with the transaction, they would follow normal procedures and either cancel, reverse or refund the transaction (cancel and reversal transactions are not available via TransactDirect therefore refund should be used). This methodology is acceptable in situations where the merchant is present, such as traditional retail and call centres where a merchant is available to make a decision, but awkward to accomplish effectively in situations where the merchant is not present for the transaction, such as the Internet.

To remove these complexities, TransactDirect provides an automated system in which the merchant can set up the AVS/CV2 acceptance conditions. If a transaction response is received from the bank with an AVS/CV2 result within the merchant's acceptance conditions, TransactDirect presents the transaction for settlement and returns an authorisation code to the merchant. On the other hand, if a transaction response is received from the bank with an AVS/CV2 result that does not conform with the merchant's acceptance conditions, the authorisation is automatically reversed by UPG on behalf of the merchant and TransactDirect does not present the transaction for settlement. In this instance, TransactDirect returns a ResponseCode of 05 and a response Message of AVS CV2 DECLINED to the merchant.

Note: there is a current trend towards the banks themselves declining transactions in which there is a CV2 mismatch.

Setting up AVS / CV2 Checks via the TMS

Accept Transactions

Each merchant account can be configured to only accept transactions that meet specific AVS/CV2 criteria:

- Accept transactions with no restriction on AVS or CV2 result.
- Accept transactions when AVS matches.
- Accept transactions when CV2 matches.
- Accept transactions when both AVS and CV2 match.

For example, if the merchant account was configured to "Accept transactions when AVS matches", only transactions with successful AVS check responses will be accepted (ALL MATCH or ADDRESS MATCH ONLY). The rest, even if the CV2 check is successful, will be declined with a ResponseCode of 05 and response Message of AVS CV2 DECLINED. The most secure option, "Accept transaction when both AVS and CV2 match", will only accept (i.e. return an authorisation code and present for settlement) transactions with successful responses to both the AVS and the CV2 checks.

Note: Certain card types such as foreign credit cards, and certain UK card issuers may not support AVS and CV2 checks.

Default Handling

This allows merchants to specify how the gateway should treat AVS/CV2 transactions in a situation where AVS or CV2 cannot be checked e.g. card issuer authorisation host problems. The options are:

- Accept all transactions where security checks cannot be carried out.
- Decline all transactions where security checks cannot be carried out.

If “Accept all transactions...” is selected then, in the event of AVS or CV2 checks not being carried out by the banks, the transactions will be accepted as per normal non-AVS/CV2 transactions. “Decline all transactions...” indicates that in the event of AVS or CV2 checks not being carried out by the banks, the transactions will be declined with a ResponseCode of 05 and a response Message of AVS CV2 DECLINED.

Visa and Mastercard have been supporting AVS and CV2 for some time and all but a few of their card issuers support it. Switch/Solo, however, have only recently introduced this feature with the result that some Switch/Solo card issuers have incomplete implementations. To overcome this, the TMS allows merchants to configure their default handling differently for Switch/Solo than for other cards.

By default, merchant accounts are set to “Accept transactions with no restriction on AVS or CV2 match” and “Accept all transactions where security checks cannot be carried out” for both Visa/Mastercard, and all other cards (Switch, Solo, JCB, etc.)

Changing AVS / CV2 Checks

AVS/CV2 acceptance conditions can be altered via the TransactDirect TMS web site at:

<http://www.universalpaymentgateway.com/merchants>

Appendix 2: How to implement a robust payment system for Internet Merchants

Since TransactDirect is a card payment gateway in the strictest sense – in that it does not display any web pages – it is the responsibility of the Internet merchant to develop their own user interface. In creating this interface there are three areas that the merchant must ensure are secure:

- The integrity of submitted data i.e. ensuring that the data transmitted between the merchant and TransactDirect has not been changed in transit.
- The security of data during posting to a non-display page.
- Transaction spoofing when using `ResponseAction = REDIRECT` i.e. a hacker fooling the merchant's web site into thinking that a successful transaction has been conducted.

Integrity of Submitted Data

The fields sent to TransactDirect can be split into three groups:

1. Fields containing user input, typically card information i.e. `CardNumber`, `IssueNumber`, `ExpMonth`, `ExpYear` etc.
2. Fields that contain transaction information i.e. `Amount`, `QAName`, `QAAddress`, `QAProducts` etc.
3. Fields that contain merchant information i.e. `ResponseAction`, `MerchantID`, `MessageType`, `CurrencyCode` etc.

The recommended technique to avoid a situation in which a hacker can change the data in a field before receipt by TransactDirect is to split the process into two pages. The first page is a display page that requests card details from the cardholder. The data is then passed, usually as form fields, to a non-display page on the merchant's web site. This non-display page adds the merchant information and then either sends the data directly to TransactDirect if `ResponseAction` is set to `HTML/XML` or redirects the web client to the TransactDirect URL with the data appended to the TransactDirect URL as a query string if `ResponseAction` is set to `REDIRECT`.

Note: Transaction information has usually been captured by a shopping cart application prior to the card details request page. The transaction information is normally either passed into the card details request page via query string or picked up in the non-display page as session variables.

An example of ASP VB Script non-display page containing web client re-direction:

```
<%@ LANGUAGE = VBScript %>
<%
Dim strCardNumber, strAmount, strMerchantID, strURL

' Retrieve transaction details from form fields
strCardNumber = Request.Form("CardNumber")
strAmount = Request.Form("Amount")

' Assign values to the fields that need to be passed to TransactDirect
strMerchantID = "0000018"
[etc]
' Build the URL ready for redirection
strURL =
"https://www.universalpaymentgateway.com/secure/transact.ashx?CardNumber=" &
strCardNumber & "&MerchantID=" & strMerchantID & "&Amount=" & strAmount [etc]

' Perform redirection
Response.Redirect strURL
%>
```

This significantly reduces the chances of a hacker being able to change submitted details. You will, however, need to secure the card data during the re-direct as the data is passed between web client and server.

Security of Data During Posting to the Non-Display Page

All data transported between a web client and TransactDirect is encrypted using Secure Socket Layer (SSL) technology. Data is therefore considered safe on its way to TransactDirect and on its way back from TransactDirect. During any call to a page on the merchant's web site, however, information that is passed between the web client and the merchant's server is not encrypted by TransactDirect's SSL.

In order to encrypt the data that is passed to the merchant's non-display page, the merchant must operate either 128-bit SSL environment themselves or pass the data via IPSEC 3DES encryption techniques, as these are the only two encryption technologies that have been ratified by the UK acquiring banks and card schemes.

IPSEC 3DES encryption is usually associated with both the merchant's and client's Internet router/modem hardware and would have to be enabled on both. Most major router/modem manufacturers support IPSEC 3DES encryption as options for their standard products.

Transaction Spoofing

If `ResponseAction = REDIRECT` is used, it is possible for a hacker to fool a merchant's web site into thinking that a successful transaction had taken place. This can be achieved by calling the merchant's site's `RetOKAddress` with spurious but meaningful data.

This is easily overcome by:

1. Creating a random number or code during the processing of the non-display page.
2. Storing a copy of the random number or code locally, for example, using either a session variable, writing to a database or writing to a locally stored file.
3. Submitting the random number as a user defined field together with the other fields sent to TransactDirect.
4. Retrieving the user defined field from the query string appended to your `RetOKAddress`.
5. Comparing the retrieved string with the stored random number or code.

If the comparison shows that the two numbers are identical, then the likelihood of this being a spoofed transaction is extremely low.

Another simple practice to avoid transaction spoofing is to check the 'referring URL' when the `RetOKAddress` is loaded.

For a transaction that was initiated by a bona fide customer, the referring URL will be that of the merchant's web site. If, in calling the `RetOKAddress` URL, a user has not clicked on a link or submit button on the merchant's web site or has not been redirected from the merchant's web site to the page, the referring URL will be either blank or contain another web address.

For example, in ASP the referring URL can be requested by:

```
<%@ LANGUAGE = VBScript%>
<%
strURL = Request.ServerVariables("HTTP_REFERER")

' Write the results to the client for testing
If strURL <> "" Then
    Response.Write strURL
Else
    Response.Write "The Referring URL is blank!"
End If
%>
```

Appendix 3: Processing American Express and Diners Club Card Transactions

This appendix describes the procedure and requirements for passing Line Item Detail information to TransactDirect for American Express and Diners Club cards.

Before a merchant can begin to process American Express or Diners Club card transactions, they must have been issued with merchant number(s) from either American Express or Diners Club, and UPG have completed the necessary set-up procedures for these merchant numbers.

Implementation

In addition to the standard fields passed as part of a normal transaction, a number of extra fields are required for American Express and Diners Club card transactions.

A transaction may consist of between one and six items, with optional information to describe tax or discount changes that have been made to the total value. A transaction must contain the quantity, description and gross value of at least one item.

The content of the purchase details fields are scrutinised by the card issuer to ensure that the cardmember's statement is detailed and meaningful enough to the cardmember to meet American Express or Diners Club standards.

Purchase Detail Fields

No.	Field Name	Description	Req'd	Size	Type
1.1	LIDItem1Quantity	Quantity of item 1	M	3 max.	N
1.2	LIDItem1Description	Description of item 1	M	15 max.	A
1.3	LIDItem1GrossValue	Gross value of item 1 in minor currency units	M	10 max.	N
2.1	LIDItem2Quantity	Quantity of item 2	O	3 max.	N
2.2	LIDItem2Description	Description of item 2	O	15 max.	A
2.3	LIDItem2GrossValue	Gross value of item 2 in minor currency units	O	10 max.	N
3.1	LIDItem3Quantity	Quantity of item 3	O	3 max.	N
3.2	LIDItem3Description	Description of item 3	O	15 max.	A
3.3	LIDItem3GrossValue	Gross value of item 3 in minor currency units	O	10 max.	N
4.1	LIDItem4Quantity	Quantity of item 4	O	3 max.	N
4.2	LIDItem4Description	Description of item 4	O	15 max.	A
4.3	LIDItem4GrossValue	Gross value of item 4 in minor currency units	O	10 max.	N
5.1	LIDItem5Quantity	Quantity of item 5	O	3 max.	N
5.2	LIDItem5Description	Description of item 5	O	15 max.	A

5.3	LIDItem5GrossValue	Gross value of item 5 in minor currency units	O	10 max.	N
6.1	LIDItem6Quantity	Quantity of item 6	O	3 max.	N
6.2	LIDItem6Description	Description of item 6	O	15 max.	A
6.3	LIDItem6GrossValue	Gross value of item 6 in minor currency units	O	10 max.	N

M = Mandatory, O = Optional, A = Alpha-Numeric, N = Numeric

Tax / Discount Fields

In addition, the following optional fields may be used to provide details of tax (7.1a) or discount (7.1b) changes to the total value. If used, either discount or tax value may be present, but not both. The description field (7.2) must be provided if either the tax or discount value fields are used.

These fields appear on the American Express or Diners Club cardmember's statement, enabling them to view net tax and discount on items bought.

No.	Field Name	Description	Req'd	Size	Type
7.1a	LIDTaxValue	Value of tax change to total value in minor currency units.	O	9 max.	N
7.2	LIDTaxDiscountDescription	Explanation of tax change to total value.	O	20 max.	A

O = Optional, A = Alpha-Numeric, N = Numeric

Or

No.	Field Name	Description	Req'd	Size	Type
7.1b	LIDDiscountValue	Value of discount change to total value in minor currency units.	O	9 max.	N
7.2	LIDTaxDiscountDescription	Explanation of discount change to total value.	O	20 max.	A

O = Optional, A = Alpha-Numeric, N = Numeric

Examples

The following examples show the additional fields that may be passed to the gateway to describe the Line Item Detail information.

A one item transaction with no tax or discount changes

No.	Field Name	Value
1.1	LIDItem1Quantity	1
1.2	LIDItem1Description	RING BINDER
1.3	LIDItem1GrossValue	299

A one item transaction with tax changes

No.	Field Name	Value
1.1	LIDItem1Quantity	1
1.2	LIDItem1Description	RING BINDER
1.3	LIDItem1GrossValue	299
7.1a	LIDTaxValue	13
7.2	LIDTaxDiscountDescription	TAX ADJUSTMENT

A one item transaction with discount changes

No.	Field Name	Value
1.1	LIDItem1Quantity	1
1.2	LIDItem1Description	RING BINDER
1.3	LIDItem1GrossValue	299
7.1b	LIDDiscountValue	100
7.2	LIDTaxDiscountDescription	MANAGER DISCOUNT

A two item transaction with no tax or discount changes

No.	Field Name	Value
1.1	LIDItem1Quantity	1
1.2	LIDItem1Description	RING BINDER
1.3	LIDItem1GrossValue	299
2.1	LIDItem2Quantity	2
2.2	LIDItem2Description	STAPLER
2.3	LIDItem2GrossValue	1598

Appendix 4: Guide to handling referrals via TransactDirect

A transaction may be returned as a referral for a number of reasons e.g.

- Cardholder is approaching or has reached their credit limit
- Transaction is of a high value
- Transaction is not typical of the cardholder's regular spending pattern

Having received a referral from the merchant's acquirer, TransactDirect stores the transaction in a 'Pending Referrals' area, informs the merchant via a `ResponseCode` of 02 and a `Message` of `CARD REFERRED` but does not present the card for payment. TransactDirect stores pending referrals for 33 days.

Note: The merchant's system Internet IP address will have to be registered with TransactDirect before the processing of referrals via TransactDirect can be conducted.

Implementation

From the perspective of the merchant's system, the following procedure for handling a referral via TransactDirect would normally be used.

1. The merchant's system receives a transaction returned as: `ResponseCode = 02` and `Message = CARD REFERRED`.
2. Merchant's system should store the returned Cross Reference.
3. Merchant should telephone their acquiring bank using the telephone number provided for this purpose by the acquirer. (If the request field `EchoReferralTelephoneNumber` was sent as `YES` in the transaction request and the merchant's acquirer supports this facility, the telephone number to call will be returned in the response field `ReferralTelephoneNumber`)
4. As a result of the telephone call, the acquirer will either give the merchant an authorisation code over the telephone or inform the merchant that the transaction has been declined.
5. If the acquirer has informed the merchant that the transaction has been declined, the merchant's system need do nothing else. (The merchant may log onto the TMS to remove the transaction from the Pending Referrals area if they wish)
6. If the acquirer has given the merchant an authorisation code, the merchant's system needs to submit a transaction request with the following fields:
 - All the mandatory generic transaction request fields
 - The `MessageType` field prefixed with `PAYMENT_ONLY_`
 - The `CrossReference` field, populated with the Cross Reference stored in step 2, in lieu of the mandatory swipe or keyed request fields
 - The `EMVTerminalType` request field if applicable
 - The `AuthorisationCode` request field

Appendix 5: Guide to handling deferred dispatch via TransactDirect

TransactDirect offers functionality to help merchants who frequently dispatch several days after accepting an order. In these circumstances it is typical for the merchant to 'test out' the validity of the card prior to accepting the order and then submit the transaction for settlement at the time of dispatch.

Note: TransactDirect uses an ordinary sale transaction type immediately followed by a reversal when submitting a dispatch later authorisation request to the merchant's acquiring bank. TransactDirect does this due to the fact that some card issuers, to whom the authorisation request is usually forwarded to by the acquirer, do not support the standard pre-auth message type. Whilst this makes dispatch later transactions more reliable than a standard pre-auth, it does mean that if the cardholder's issuer does not support reversals, the nominal authorisation amount may temporarily appear on the cardholders account. Since dispatch later transactions themselves are never presented for settlement – it is the subsequent dispatch now that is settled – the authorisation will be automatically removed by the card issuer usually within 4 working days. Importantly, the dispatch later transaction does affect the cardholder's available credit, hence the use of a nominal amount to reduce its effect.

Note: The merchant's system Internet IP address will have to be registered with TransactDirect before the processing of deferred dispatch transactions via TransactDirect can be conducted.

Note: The Dispatch = Later system can also be used during the processing of refunds in which the merchant has taken card details at the time of refund agreement but does not wish to process the refund until the goods have been received.

Note: Only merchants who are registered with UPG to conduct deferred dispatch will be allowed to submit transactions of this type. Please contact UPG to register.

Implementation

The recommended procedure for carrying out the above is as follows:

1. Merchant's system submits a transaction request (either sale or refund as appropriate) with the Amount field set to a nominal figure, e.g. £1.01, the DispatchLaterAmount field set to the total transaction amount and the Dispatch field set to LATER. This is accomplished by sending a normal transaction request with the following differences:
 - Amount = 101
 - DispatchLaterAmount = 1299
 - Dispatch = LATER

In the case of a sale, this `Dispatch = LATER` transaction checks to ensure that the card has not been reported as lost or stolen and completes the AVS/CV2 check. It does not check the availability of funds for the full purchase price as this will be checked during a second transaction submission at the time of dispatch.

2. Assuming that the transaction is authorised, the merchant's system should store the Cross Reference that is returned as part of the transaction response. TransactDirect will store the transaction for 40 days.
3. When ready for dispatch, the merchant's system submits a transaction request for the full amount using the Cross Reference stored in step 2 and with the `Dispatch` field set `NOW`. This is accomplished by sending a normal transaction request with the following differences:

- `CrossReference` = Cross Reference of transaction from step 2

Note: AVS and CV2 will not be checked at this stage in the transaction.

Appendix 6: Guide to handling continuous authority transactions via TransactDirect

Continuous authority via TransactDirect is a method of re-charging a cardholder without recourse to the original card details.

- Continuous authority is for regular (daily, weekly or monthly) charging of a card. The cardholder gives permission (authority) to the merchant to charge the card without the merchant needing to contact the cardholder on each occasion.

Note: Continuous Authority is not supported by Maestro or its associated card schemes.

Note: A merchant must have prior arrangement from their acquiring bank before they can begin to process continuous authority transactions.

Note: The merchant's system Internet IP address will have to be registered with TransactDirect before the processing of continuous authority and re-authorisation transactions via TransactDirect can be conducted.

Note: Only those merchants who are registered with UPG to conduct rebilling will be allowed to submit transactions of this type.

Continuous authority implementation

The recommended procedure for carrying out the above is as follows:

1. Merchant's system submits a normal transaction with a `MessageType` field of `SALE_CA`. This will authorise and settle the first transaction.
2. Assuming that the transaction in step 1 is authorised, the merchant's system should store the Cross Reference that is returned as part of the transaction response. TransactDirect will store the transaction for 33 days – allowing for monthly rebilling.
3. When the second transaction is ready to be processed, the merchant's system submits a transaction again with a `MessageType` field of `SALE_CA`. The Cross Reference stored in step 2, however, is used in lieu of the card details fields.
4. Assuming that the transaction in step 3 is authorised, the merchant's system should store the new Cross Reference that is returned as part of the transaction response. TransactDirect will store the transaction for 33 days.
5. When the third transaction is ready to be processed, the merchant's system submits a transaction again with a `MessageType` field of `SALE_CA`. The Cross Reference stored in step 4, however, is used in lieu of the card details fields.
6. And so on.

Contact Details

Technical Enquiries

For all technical enquiries please contact a member of the Universal Payment Gateway technical team on +44 (0) 1827 265005 or by email to support@universalpaymentgateway.com.

Sales Enquiries

For sales enquiries, please contact a member of the Universal Payment Gateway sales team on +44 (0) 1827 265005.