TransactDirect API Guide

The Monek Guide for Secure Internet Transaction Delivery

For use with Transact.ashx and TransactACS.ashx

For further help, telephone +44 (0) 345 269 6645 or email support@monek.co.uk

MONEK

Introduction

Monek'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:

- 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. Transactions initiated with a Cross Reference can also be authenticated with the ValidityID field.

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

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

- Full compliance with Visa and MasterCard's 3-D Secure V1.02.
- Ease of integration using HTML form fields and browser client re-direction.
- Integrated directly into Monek'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 merchant's website.

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

Table of Contents

Methods of Operation

Gateway URLs

Primary: https://elite.monek.com/Secure/Transact.ashx

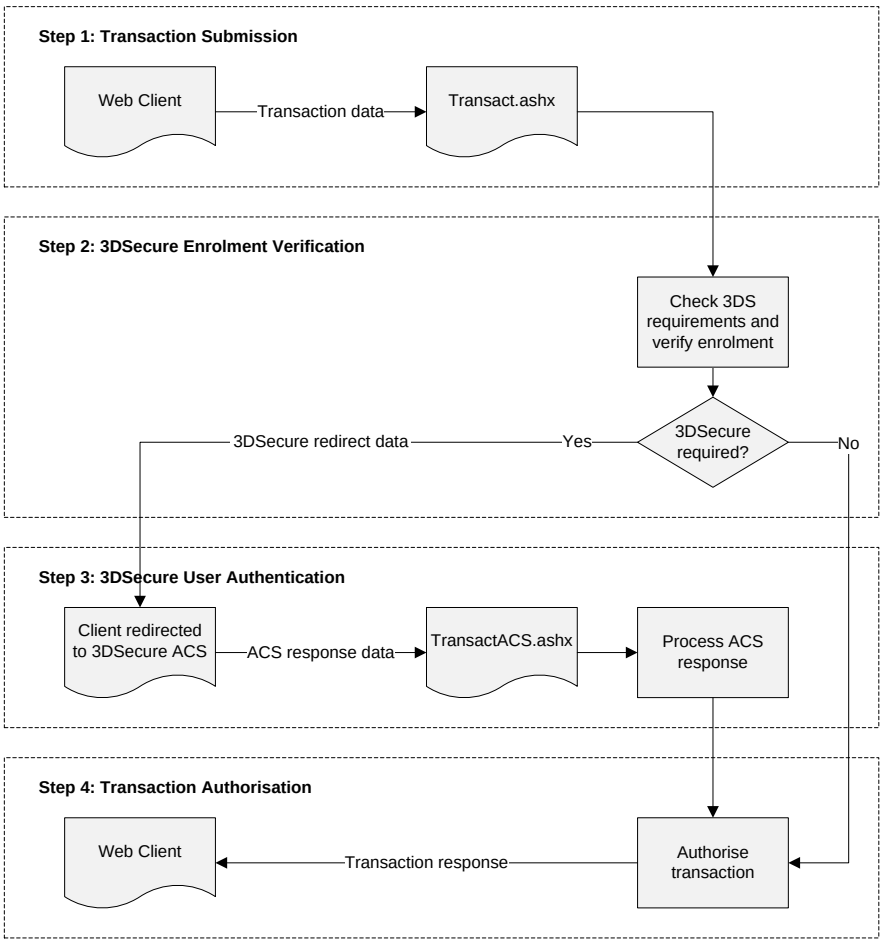
Staging: https://staging.monek.com/Secure/Transact.ashx

Note: Both gateways are LIVE and will process for all Monek Merchant accounts.

The staging API is available for integration and compatibility testing of new features before they are available on the primary platform.

Sequence of Events

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 to the TransactDirect web server at https://elite.monek.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://elite.monek.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 Monek 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 HTMLQS 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 the 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://elite.monek.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:

1. If the ResponseAction field was set to HTMLQS 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
```

2. 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>030507115841061661 63</crossreference>
</transactionresponse>
```

3. 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://elite.monek.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. Every transaction submitted must include the fields listed in the 'Card Keyed Transaction Request Fields' table. The fields from '3-D Secure Transaction Request Fields' are required in order to process 3-D Secure. A selection of optional fields is provided to allow access to further functionality

Mandatory Generic Transaction Request Fields

Field Name	Description	Req'd	Size	Type
Amount	The transaction amount, numeric, in minor currency i.e. pence/cents etc. No decimal point. e.g. £10.02 = 1002	M	10 max.	N
CountryCode	ISO standard country code for merchant location. Use 826 for UK based merchants. Other options available on request.	M	3	N
CurrencyCode	ISO standard currency code of transaction. Use 826 for Sterling transactions. Other options available on request.	M	3	N
Dispatch	Used for deferred dispatch, options are: • NOW • LATER If LATER, DispatchLaterAmount becomes mandatory.	M	5 max.	A
MerchantID	Monek merchant ID. Test accounts are available on request.	M	7	N

MessageType	Indicates the transaction type for the request. See later table for acceptable message types.	M	V	A
ResponseAction	Specifies the return method for the transaction response data. Options are: • HTMLQS • XML • REDIRECT	M	V	A

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric

Card Keyed Transaction Request Fields

Field Name	Description	Req'd	Size	Type
CardNumber	Card number.	M	20 max.	N
ExpiryMonth	Expiry month.	M	2	N
ExpiryYear	Expiry year.	M	2	N
ExpMonth (deprecated)	Expiry month. Deprecated, use ExpiryMonth.	M	2	N
ExpYear (deprecated)	Expiry year. Deprecated, use ExpiryYear.	M	2	N
StartMonth	Start month.	M/O*	2	N
StartYear	Start year.	M/O*	2	N

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric
** Required for certain card types*

3-D Secure Transaction Request Fields

Field Name	Description	Req'd	Size	Type
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 Monek 3-D Secure lookup.	O	125 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) • HTMLQS • XML • REDIRECT • ACSDIRECT	M	V	A
ThreeDSPassword	The 3-D Secure password issued to each merchant by Monek.	M	8	A
ThreeDSOnly	Options are YES or NO. Defaults to NO if not supplied. If set to YES, TransactDirect will only process the 3-D Secure portion of the transaction and not continue to authorisation.	M	2 or 3	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, V = Variable Length, A = Alpha-Numeric, N = Numeric

Additional 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	8 max.	A
CardToken	This is sent in lieu of the card details (card number, expiry month and year, start month and year) and can be used for reprocessing a stored card. e.g. For continuous authority. *Note: Merchants who wish to conduct transactions using Card Tokens must do so from a static IP address(es) that has been registered with TransactDirect.*	O	50 max.	A
CAType	This is to be sent when a transaction forms part of a continuous authority agreement. It should be set on any transaction that initiates a CA agreement and on all subsequent transactions. Options are "R" or "I", see Continuous Authority Types for details.	O	1	A
CrossReference	This is sent in lieu of the card details (card number, expiry month and year, start month and year) and is typically used for completing transactions that were originally submitted as Dispatch = LATER, processing referrals, re-billing or refunding previous transactions. *Note: Merchants who wish to conduct transactions using Cross References must do so from a static IP address(es) that has been registered with TransactDirect.*	O	50 max.	A
CV2	Card Verification Value normally printed after the card number on the card's magnetic strip. **Note: The CV2 value should not be stored under any circumstances.**	O	3 or 4	N

DispatchLaterAmount	The total amount of the transaction. Numeric, minor currency i.e. pence/cents etc. No decimal point e.g. £10.02 = 1002 Mandatory for transactions submitted as DISPATCH=LATER.	M/O	10 Max	N
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
PaymentReference	ID created by the merchant to identify the transaction. Replacement for TransactionIdentifier. See also: TransactionIdentifier	O	50 max.	A
QAName	Customer's name. 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. 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. If populated, the field is automatically returned as the additional response field QAPostCode.	O	10 max.	A
QAEmailAddress	Customer's email address. If populated, the field is automatically returned as the additional response field QAEmailAddress.	O	50 max.	A
QAPhoneNumber	Customer's telephone number. If populated, the field is automatically returned as the additional response field QAPhoneNumber.	O	30 max.	A

QAProducts	Details of products or services purchased. 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
TransactionIdentifier	ID created by the merchant to identify the transaction. Superseded by PaymentReference. See also: PaymentReference	O	50 max.	A
ValidityID	Is used by TransactDirect in conjunction with MerchantID to provide additional security. ValidityID will be issued by Monek and can be used to authenticate repeat transactions and refunds performed by Cross Reference.	M/O	20 max.	A

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric

Additional Form Fields

Additional merchant specific data should be sent in the MerchantData field.

Use of this field for merchant data ensures there are no clashes with fieldnames that may be required to support new functionality on the TransactDirect API.

This field can be used to store a simple value, complex encoded data (such as JSON) or raw binary data. In all cases the supplied value must be Base64 encoded.

Field Name	Description	Req'd	Size	Type
MerchantData	Any merchant required data. **Note: Data must be Base64 encoded.**	O	1024 max	Base 64

Base64 encoding supports the following key goals:

- Supports any underlying data format required by the merchant.
- Data can be returned unaltered without encoding complications.
- Ensures maximum compatibility with security mechanisms.

Additional Form Fields – Legacy Functionality

Additional form or query string fields may also be sent to TransactDirect using any custom name.

This functionality is deprecated and may be removed or restricted in the future.

Use of this feature should be avoided, or removed where used, in favour of the MerchantData field.

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 Monek 3-D Secure pages or a 3rd party 3-D Secure system, the 3-D Secure result fields can still be supplied to Transact.ashx for processing.

Field Name	Description	Req'd	Size	Type
Authenticated	"Y" for successfully authenticated with cardholder's issuing bank. "N" for unsuccessful authentication with cardholder's issuing bank. "U" for an unsuccessful authentication during which an error was raised. "A" when authentication could not be completed but proof of the attempt was provided.	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	"Y" for card enrolled for 3-D Secure as determined by the card scheme directory server. "N" for card not enrolled for 3-D Secure as determined by the card scheme directory server. "U" for an unsuccessful cardholder enrolment attempt during which an error was raised.	O	1	A
TransactionID	A transaction identified derived by merchant. Must be unique for every transaction.	O	20	A

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric

TransactDirect Message Types

MessageType	Description
ESALE_KEYED	E-Commerce (Internet) sale transaction, card keyed by cardholder (both merchant and cardholder not present). Note: May be prefixed with PAYMENT_ONLY_ see following note.
EVERIFY_KEYED	E-Commerce (Internet) account verification transaction, card keyed by cardholder (both merchant and cardholder not present). Note: Transaction amount must be ZERO (0).
SALE_CNP	Sale transaction, cardholder not present (typically from call-centre i.e. telephone, mail order, etc.). Note: May be prefixed with PAYMENT_ONLY_ see following note.

VERIFY_CNP	Account verification transaction, cardholder not present (typically from call-centre i.e. telephone, mail order, etc.). Note: Transaction amount must be ZERO (0).
SALE_CA	Sale transaction with continuous authority. Note: May be prefixed with PAYMENT_ONLY_ see following note.
REFUND_CNP	Refund transaction, cardholder not present (typically from call-centre i.e. telephone, mail order, etc.).
REVERSAL_KEYED	Reverses a previous transaction. Note: Must be performed by Cross Reference. Original transaction MUST be from same day and should be within 2 minutes of reversal.

Note:

- 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 Monek to register.
- Refunds and reversals are only acceptable if the source IP address has been registered with TransactDirect. Please contact Monek to register.
- Transactions prefixed with PAYMENT_ONLY are only acceptable if the source IP address has been registered with TransactDirect. Please contact Monek to register.
- Certain message types, for example, continuous authority (SALE_CA 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.

Continuous Authority Types

TransactDirect allows a transaction to be identified as part of a continuous authority agreement with the cardholder.

This should be specified in the CAType field in the transaction request for the initiating transaction and all subsequent payment requests.

CA Type	Description
R or Recurring	Indicates that this transaction is part of a recurring agreement. Recurring payment transactions may be recharged as required by the merchant to satisfy future purchases.
I or Instalment	Indicates that this transaction is part of an instalment agreement. Instalment transactions should be used to charge a predictable amount at regular intervals.

N	[Optional] Indicates that the transaction is not part of a continuous authority agreement. This is the default if CAType is not supplied.

Payment Only Transactions

TransactDirect Message Types can be prefixed with PAYMENT_ONLY_ to indicate that no authorisation is required. Such transactions are not forwarded to the bank for authorisation and are sent for settlement on the assumption that the merchant has obtained authorisation from some other source. Typical scenarios where this may be appropriate are:

- The original transaction resulted in a referral and the settlement confirmation is being sent following a call to the bank's voice authorisation centre.
- When presenting transactions to TransactDirect following a period of communications failure.
- Where the original transaction was sent as DISPATCH = LATER and is now ready for settlement.

The following standard fields have particular importance for a PAYMENT_ONLY_ transaction:

Field Name	Description	Req'd	Size	Type
AuthorisationCode	Must contain the authorisation code obtained during the referral process or original authorisation.	M	8 max.	A
CrossReference	When processing a PAYMENT_ONLY_ request following an authorisation only or referral transaction the CrossReference from the original transaction should always be used. Not required when a presenting an offline transaction following a period of communications failure. In this scenario the full card details would be required.	O	50 max.	A

Common Currency Codes

Currency	ISO-4217 Code
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.

Examples

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
CardNumber	5301250070000191
CurrencyCode	826
CountryCode	826
CV2	419
Dispatch	NOW
ExpMonth	06
ExpYear	20
MerchantID	0000018
MessageType	ESALE_KEYED

QAName	Martin Brewster
QAAddress	25 The Larches, Narborough, Leicestershire
QAPostcode	LE10 2RT
QAEmailAddress	m.brewster@longshot.com
QAProducts	102293: 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	AAABAnMVNHhgAAAAARU0AAAAAAA=
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://elite.monek.com/secure/transact.ashx">
<input type="hidden" name="ResponseAction" value="HTMLQS">
<input type="hidden" name="MerchantID" value="0000018">
<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="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></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</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>
```


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 HTMLQS 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%3a94
43%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 HTMLQS, 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 3-D Secure authentication host.	V	A

MD	Merchant Data. All merchant data is retained by the Transact.ashx 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 TransactACS.ashx.	V	A
PAReq	The full 3-D 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 to the card issuer's 3-D 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 Transact.ashx response.	M	V	A
PaReq	The full 3-D Secure request. This field should be passed unaltered from the Transact.ashx response.	M	V	A
TermUrl	Termination URL. This is the address that the issuer's ACS will call after payer authentication is complete.	M	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.

ACS Response Fields

If TermUrl is set to direct responses to the merchant web site, 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 TransactACS.ashx.	M	V	A
PaRes	The full 3-D Secure response as returned by the cardholder's issuer. This field should be passed unaltered to TransactACS.ashx.	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 HTMLQS 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>AUTHCO
DE:06166</message><crossreference>030507115841061661 63</crossreference></transactionrespo
nse>
```

If the ResponseAction field was set to REDIRECT TransactDirect issues a re-direct to the web client 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&CrossRe
ference=03050711535801223303
```

Redirecting to the RetOKAddress or RetNotOKAddress depends upon the transaction outcome:

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

Standard Response Fields

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

Field Name	Contents	Size	Type
Amount	Amount sent with transaction request to acquiring bank or, in the event of a payment only transaction, accepted by TransactDirect. Value returned in minor currency i.e. pence/cents etc.	10 max.	N

AuthorisationCode	The authorisation code issued for a successful transaction. Normally this is 2 digits for American Express and 6 for other card schemes. Note: An authorisation code is strictly alphanumeric. While typically numeric an authorisation code may also contain letters.	2-8	A
AVSCV2Check	AVS/CV2 check response. See following table.	30 max.	A
AVSCV2ResponseCode	The raw AVS/CV2 code returned by the acquiring bank. See following tables.	6	N
CardToken	The unique character string supplied by TransactDirect to identify this card. Optional: Will be returned where the merchant is configured to support card tokens.	50 max.	A
CardType	The card type code indicating the card type used for the transaction. See following table.	2	A
CrossReference	The unique character string supplied by TransactDirect to identify this transaction.	50 max.	A
ErrorCode	May contain an additional error detail code where standard response code indicate and error "30". This code can be used by Monek to further diagnose the cause of an error.	4	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

ReferralTelephoneNumber	The referral telephone number passed to TransactDirect by the merchant's acquirer in the event of a transaction being referred. Note: In most circumstances the merchants will have been provided with a standard referral telephone number by their acquiring bank and should primarily use that number in the event of a referral.	16 max.	N
ResponseCode	The TransactDirect response code. See following table.	2	N

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric

Response Code Values

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

AVS/CV2 Response Code Values

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 Description
0	No additional information available
1	CV2 not checked
2	CV2 matched
4	CV2 not matched
8	Reserved
Position 2 Value	**Position 2 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 Description
0	No additional information available
1	Address not checked
2	Address matched
4	Address not matched
8	Address partially matched
Position 4 Value	Position 4 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 Description
0	Reserved
1	Reserved
2	Reserved
4	Reserved
8	Reserved
Position 6 Value	Position 6 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.

AVS/CV2 Check Response Values

AVS and CV2 checks are supported by most major card issuers including Visa, MasterCard, Maestro and American Express.

AVS / CV2 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.

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.

Card Type Values

The following card type codes are currently supported. This list is subject to change as new card types are added.

Card Type Code	Card Type
AM	American Express

CF	Clydesdale Financial Services
DI	Diners Club
DS	Discover
EL	Electron
JC	JCB
MA	Maestro (International)
MC	MasterCard
MD	MasterCard Debit
SO	Solo (Discontinued)
ST	Style
SW	Maestro (UK issued)
VC	Visa Credit
VD	Visa Debit
VP	Visa Purchasing

3-D Secure Result Fields

Field Name	Description	Size
ThreeDS	The 3-D Secure details as returned from the verify enrolment and payer authentication stages. Comma separated in Monek 2.1 compliant form. Not returned if 3-D Secure processing has not taken place	60 max.
ThreeDSErrorCode	Code issued by 3-D Secure MPI if either enrolment verification or 3-D Secure authentication failed with an error.	V
ThreeDSErrorDetail	Error description issued by 3-D Secure MPI if either enrolment verification or 3-D Secure authentication failed with an error.	V

Structure of the 3-D Secure Information field

No	Field Name and Contents	Req'd	Size	Type
1	Enrolled	M	1	A
2	Comma Separator	M	1	

3	Authenticated	M	1	A
4	Comma Separator	M	1	
5	ECI	M	2	N
6	Comma Separator	M	1	
7	CAVV	M	32 max.	A
8	Comma Separator	M	1	
9	Transaction Identifier	M	20	N

Receipt Information

Field Name	Description	Size
ReceiptInformation	This returns all the information that a merchant needs to produce a customer receipt. Please contact Monek to enable this facility. Returned if transaction request field EchoReceiptInformation was set to YES. Not returned if TransactDirect ResponseCode = 30	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] – ASCII character code 31	M	1	
3	Card Type Description	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 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 (discontinued)	O	n/a	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	Cashback Amount - minor currency units	O	11 max.	N

34	Unit Separator [US]	M	1	
35	Gratuity Amount - minor currency units	O	11 max.	N

M = Mandatory, O = Optional, V = Variable Length, A = Alpha-Numeric, N = Numeric

Additional Fields

Additional form or query string fields may be sent to TransactDirect as necessary and are returned unaltered. Field values are URL/HTML encoded as required based on the value of the ResponseAction.

This functionality is deprecated and may be removed or restricted in the future.

See "Additional Form Fields" for further details.

Note:

- Primary fields pertaining to the original transaction request are not passed back e.g. CardNumber, ExpYear, ExpMonth.
- Customer information details are returned by default. e.g. 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. 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 Monek 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 ResponseMessage of AVS CV2 DECLINED. The most secure option, "Accept transaction when both AVS and CV2 match", will only accept 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.

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:

- Fields containing user input, typically card information i.e. CardNumber, IssueNumber, ExpMonth, ExpYear etc.
- Fields that contain transaction information i.e. Amount, QAName, QAAddress, QAProducts etc.
- 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 HTMLQS/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 passed to TransactDirect
strMerchantID = "0000018"
[etc]

' Build the URL ready for redirection
strURL = "https://elite.monek.com/secure/transact.ashx?CardNumber=" & strCardNumber &
"&MerchantID=" & strMerchantID & "&Amount=" & strAmount [etc]

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

This significantly reduces the chances of a hackerbeing 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 Transport Layer Security (TLS) 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 and is subject to the transport mechanisms and security put in place by the merchant.

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 Monek 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 contents of the purchase detail fields are scrutinised by the card issuer to ensure that the card member's statement is detailed and meaningful enough to the card member 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, V = Variable Length, 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 card member'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

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

M = Mandatory, O = Optional, V = Variable Length, 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: Error Codes

Standard Error Codes

Error Code	Description
1005	**Invalid message type** The Monek message type (e.g. ESALE_KEYED) is invalid.
1008	**No TIDs available, using primary** The number of active concurrent transactions exceeds the number of Terminal Identifiers (TIDs) allocated to the merchant. The primary TID will be reused.
1022	**Invalid track 2 data** The track 2 data supplied for a CHIP or SWIPE transaction is not valid.
1026	**Unrecognised Card Type** The card number supplied has not been recognised against the active card ranges.
1052	**Merchant not set up for supplied currency** The merchant is not set up for the currency specified.
1063	**Merchant or Entity Type not found** Merchant configuration error, please contact Monek Support.
1300	**Response sequence error** The transaction response from the acquiring bank was not properly formatted.
1301	**Response Message Type: HOLD** The bank could not process the transaction on this attempt. Depending on the acquirer this can indicate a long running authorisation or an issue with the supplied card details. This is entirely at the discretion of the acquiring bank so it is recommended that under these circumstances the card details should be checked and resubmitted.
1303	**Unexpected response code for acquirer 'xx'** The acquiring bank returned an unknown transaction response code.
1309	**PSF card data malformed** The Payment, Store or Fuel card line item data supplied was malformed.
1314	**Invalid Monek merchant number** The specified Monek merchant number is invalid.
1323	**Unable to extract stored card data** The system was unable to resolve card data for a Cross Reference transaction.

Error Code	Description
1350	**Cannot submit swiped card details for KEYED transaction method** Card details were provided in Track2 format against a keyed card transaction type.
1367	**Connection timed out** The authorisation connection to the acquiring bank timed out.
1374	**Client closed socket before response sent. Acquirer request sent.** The calling client closed the transaction socket before the transaction could be completed. The authorisation request was sent to the acquiring bank but the transaction will NOT be settled.
1380	**Merchant IP address not found** A refund or Cross Reference transaction was received from an IP address not registered against the merchant.
1384	**Client closed socket before response sent. Acquirer request NOT sent.** The calling client closed the transaction socket before the transaction could be completed. The authorisation request was not sent to the acquiring bank.
1401	**Internal timeout** An internal timeout occurred processing the transaction.
1403	**Internal timeout** An internal timeout occurred processing the transaction.
1487	**No TIDs available, TID Limited** The number of active concurrent transactions exceeds the number of Terminal Identifiers (TIDs) allocated to the merchant. TID usage is limited to unique available TIDs.
1488	**Malformed card details** The card details supplied are not in a recognisable format.
1491	**Card Type Not Supported by 3-D Secure** 3-D Secure details were supplied for a card type that does not support 3-D Secure.
1492	**3-D Secure CAVV conversion failed** The CAVV supplied for a 3-D Secure transaction is invalid.
1493	**3-D Secure Enrolled character not valid** The Enrolled value supplied for a 3-D Secure transaction is invalid.
1494	**3-D Secure Authenticated character not valid** The Authenticated value supplied for a 3-D Secure transaction is invalid.

Error Code	Description
1495	**Internet or Keyed Maestro transaction in which no 3DS data has been submitted** Internationally issued Maestro cards processed over the internet must use 3-D Secure.
1500	**Merchant not set up for Streamline settlement country** [Streamline Only] The transaction specified a country code not allowed for the merchant.
1501	**Invalid operation performed using Cross Reference in lieu of card details** A cross reference can be used to settle, recharge or refund a previous transaction. It cannot be used to perform a sale against a refund or to reprocess authorisation only requests.
1509	**VERIFY not supported by acquirer** The acquirer for this merchant does not currently support the Zero Auth transaction type.
1510	**Monek Merchant Closed** The Monek merchant has been closed at the request of the merchant or their acquiring bank.
2152	**Connection timed out** The authorisation connection to the acquiring bank timed out.
2155	**Connection timed out** The authorisation connection to the acquiring bank timed out.
2157	**Authorisation rejected by host** The connection to the acquiring bank was established but the authorisation host refused to accept the transaction.
2166	**Authorisation rejected by host** The connection to the acquiring bank was established but the authorisation host refused to accept the transaction.
2180	**Internal timeout** An internal timeout occurred processing the transaction.
3073	**Invalid request string** The transaction message was invalid.
3074	**Invalid request string** The transaction message was invalid.
3501	**No matching transaction for refund** No suitable transaction could be found to match the refund request

Dynamic Error Codes

Monek request message validation generates dynamic codes to represent field validation failures. Dynamic codes follow this format:

4xyy

where: 4 – Indicate a field validation error
X – Indicates the type of problem
Y – Indicates the field that failed validation

X - Problem Types

The following table details the codes for each validation problem type.

Code	Description
0	MISSING
1	EMPTY
2	TOO SHORT
3	TOO SMALL
4	TOO FEW FIELDS
5	TOO LARGE
6	TOO LONG
7	TOO MANY FIELDS
8	NOT INTEGER
9	NOT NUMERIC

YY - Field Numbers

The following table details the 2-digit codes used to represent the field failing validation.

Code	Description
00	MISSING
02	TERMINAL IDENTIFIER
03	TRANSACTION IDENTIFIER
04	TERMINAL TYPE
05	MESSAGE TYPE
07	Monek MERCHANT ID

Code	Description
08	CARD DETAILS
09	AMOUNT
10	CASHBACK AMOUNT
11	CURRENCY CODE
12	COUNTRY CODE
13	DISPATCH
14	AUTHORISATION CODE
15	CUSTOMER DETAILS
16	CARD SECURITY CODE (CV2)
17	DESCRIPTIVE DATA
18	PURCHASE/STORE/FUEL CARD LINE ITEM DETAIL
19	RESERVED
20	TRANSACTION TIME & DATE
21	EMV TERMINAL TYPE
22	REASON ONLINE CODE
23	ICC TRANSACTION REQUEST DATA
24	CARD NUMBER
25	ISSUE NUMBER
26	EXPIRY MONTH
27	EXPIRY YEAR
28	START MONTH
29	START YEAR
37	SERVICE CODE
56	CUSTOMER NAME
57	CUSTOMER ADDRESS
58	CUSTOMER POSTCODE

Code	Description
59	CUSTOMER TELEPHONE
60	CUSTOMER EMAIL
71	RESERVED
87	CROSS REFERENCE
94	START DATE
95	EXPIRY DATE

Appendix 5: 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.

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.
    a. If 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 keyed request fields
    - The AuthorisationCode request field

Appendix 6: 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 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. If the cardholder's issuer does not support reversals the nominal authorisation amount may temporarily appear on the cardholders account, this will be automatically removed by the card issuer, usually within 4 working days. The dispatch later transaction does affect the cardholder's available credit, hence the use of a nominal amount to reduce its effect.
- 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.
- 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.

Implementation

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

1. Merchant's system submits a request with the Amount field set to a nominal figure, e.g. £1.01, the DispatchLaterAmount field set to the total amount and the Dispatch field set to LATER.
    - Amount = 101
    - DispatchLaterAmount = 1299
    - Dispatch = LATER
2. 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.
3. The merchant's system should store the Cross Reference that is returned as part of the transaction response.
4. 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.

Alternatives

In some scenarios it is preferable to use the Account Verification method (e.g. EVERIFY_KEYED) to verify the card and generate a Cross Reference or Card Token.

Appendix 7: 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.

- The CAType field should be used to indicate the intent of the continuous authority arrangement. See Continuous Authority Types.
- 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.
- Continuous Authority is not supported by Maestro or its associated card schemes.
- A merchant must have prior arrangement from their acquiring bank before they can begin to process continuous authority transactions.
- 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.
- Only those merchants who are registered with Monek to conduct rebilling will be allowed to submit transactions of this type.

Continuous authority implementation by Cross Reference

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

1. Merchant's system submits a normal transaction. This transaction should correctly reflect the capture method (e.g. ESALE_KEYED for eCommerce) and be supplied complete with all relevant security details. 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 Monek Cross Reference that is returned as part of the transaction response.
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.
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.

Continuous authority implementation by Card Token

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

1. Merchant's system submits a normal transaction. This transaction should correctly reflect the capture method (e.g. ESALE_KEYED for eCommerce) and be supplied complete with all relevant security details. 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 Card Token that is returned as part of the transaction response.

3. When a subsequent transaction is ready to be processed, the merchant's system submits a transaction again with a MessageType field of SALE_CA. The Card Token stored in step 2, however, is used in lieu of the card details fields.

4. The Card Token will remain valid for the life of the card.

Contact Details

Technical Enquiries

For all technical enquiries please contact a member of the Monek technical team on +44 (0) 345 269 6645 or by email to support@monek.com.

Sales Enquiries

For sales enquiries, please contact a member of the Monek sales team on +44 (0) 345 269 6645.