



Integration Guide

HTTP Direct Integration Method.

Version 8.2

Introduction

Cardstream runs a real time card processing system that converts the traditional two-stage authorisation and payment processes into one convenient 'transaction' process. Herein the processing service will be known as the 'payment gateway'.

The payment gateway is designed to be exceptionally easy to integrate into web sites, call centre systems, back office payment systems, or any technology that requires credit or debit card transactions. It is flexible, robust and fast, normally returning authorisations within 3 seconds.

Direct Integration.

In this method the Merchant's customers never leave their site. The transaction is sent to Cardstream securely in the background meaning the transaction is fully inline with the Merchant's website or other technology. This method will also allow the Merchant to take advantage of the ultra-high availability integration method offered for use by all Cardstream Merchants.

The payment gateway is fully multi-currency enable. All Merchants wishing to process multi-currency transactions must check with their Acquiring Bank (Merchant Account Provider) as to the list of currencies they support. For Merchants wishing to process multi-currency transactions, a full list of currencies supported by Cardstream is attached later in this guide.

All Cardstream Merchants have secure access to their own private administration area within the Merchant Management System (MMS). This system is logged into from the home page - www.cardstream.com. MMS login details will have been sent by email following initial account registration.

The MMS allows Merchant's to carry out the following tasks -

- Setup account user profiles with a choice of 3 different access level –
 - Merchant Master (able to set up user profiles, process both sales and refund transactions control of all MMS profile preferences)
 - Administrator (able to process both sales and refund transactions)
 - Sales Clerk (able to process sales transactions only)
- Process all types of manual transactions, both differed and immediate settlement
- Download transaction data in a convenient .csv format compatible with most accountancy packages for easy transaction reconciliation
- Obtain all relevant documentation necessary to ensure that they are processing transactions effectively through the payment gateway.

Before beginning this integration process, Merchants are advised that they will benefit from being 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 the Merchant and the payment gateway using Secure Socket Layer (SSL) environment, it is still a requirement that Internet Merchants obtain their own SSL certificate for capturing cardholder data. Merchants with their own SSL certificate not only ensure in transit security of card details but also help to ensure customer confidence by displaying an indication on their web client (browser) that the session is encrypted.

The Transaction Process

Cardstream Integration Guide

The transaction process is virtually the same for both connection methods that are support by the payment gateway. In depth details will be provided later in this document as to how to carry out both procedures. The flow of a typical transaction is as follows -

1. Customer selects his/her product(s) and begins the checkout process.
2. A secure web page is displayed that captures the card data and any other relevant information that the Merchant wishes to collect.
3. If the Merchant is 3D Secure enabled, then the Customer's web browser must be re-directed (or posted via a pop up window) to Cardstream's 3D Secure platform where the Customer is then re-directed to their bank for 3D Secure authentication. If the Merchant is not 3D Secure enabled, skip to step 5.
4. The Customer is re-directed back to the Merchant's site as an HTTP POST – the Merchant obtains the security code for this 3D Secure transaction and includes it with all other required cardholder data.
5. The Merchant then submits data to the gateway for processing.
6. The payment gateway checks the submitted transaction request to make sure it is valid, checks black lists and if all is in order the payment gateway then submits the transaction data into the banking network for authorisation.
7. The payment gateway will then receive a response from the Acquiring Bank as to the status of the transaction. This is then passed out to the Merchant's website or software package.
8. Merchant software then acts on the results of the transaction request, sending emails, updating databases etc.
9. Transaction request is now completed!

A record of every transaction request is stored in the payment gateway database and is available for reference within the MMS. Successful transactions are stored within the MMS for 180 days and can be used by the Merchant as required. Failed transactions are stored for 7 days to allow the Merchant time to attempt to address the reason for the failed transaction, i.e. get the correct expiry date if the customer entered it incorrectly.

3D Secure Authentication (Optional)

If the Merchant is 3D Secure enabled then the transaction process is two-fold. Firstly the Customer must be re-directed to Cardstream's 3D Secure platform to obtain an authentication key that is then used later in the transaction, upon leaving the 3D Secure platform the Customer is re-directed back to a script on the Merchant's website to which the authentication data is sent via HTTP POST. Any form values posted to the 3D Secure platform will be posted back to the Merchant, which is useful if the Merchant does not wish the Customer to be presented with a second form to add additional information. The Customer must be re-directed, either in the existing browser window, or via a popup, to the following URL -

Please call Cardstream for further information

The request must be HTTP POST and, at the very least, the following fields must be included -

| Mandatory fields |
|-------------------------|
| VPMerchantID |
| VPCardNumber |
| VPAmount |
| VPEpiryDateMM |
| VPEpiryDateYY |
| VPCurrencyCode |
| VPGatewayURL |

With the exception of VPGatewayURL, all fields are described in the next section of this guide. VPGatewayURL must contain the full secure URL of the return script that the Customer will be returned to after completing 3D Secure authentication. When the customer has completed 3D Secure authentication, they will be redirected back to the URL defined in VPGatewayURL as an HTTP POST request. The script defined in this URL must be capable of accepting HTTP POST variables. All form fields submitted at the start of the process will be present in the HTTP POST request, and the following fields may also be sent -

| Field Name | Description |
|-------------------|--|
| ECI | E-Commerce Indicator |
| CAVV | Authentication Code |
| CAVVAAlgorithm | Algorithm setting. |
| TransactionID | 3D Secure transaction ID |
| Enrolled | States whether the cardholder is enrolled for 3D Secure (Y=yes, N=no, U=unknown) |
| Authenticated | States whether the cardholder is authenticated for 3D Secure (Y=yes, N=no) |
| ErrorCode | Numerical error reference |
| ErrorMessage | Description of error, if any |

The Merchant must now send all Customer card data to the payment gateway as a standard transaction described in the next section, for a 3D Secure transaction the fields above must be included in the HTTP POST request.

| Summary |
|---|
| Merchant displays payment screen for Customer entry |
| Customer enters data and Merchant's site re-directs the Customer's browser to Cardstream's 3D Secure facility as an HTTP POST |
| Cardstream checks if the Customer is enrolled for 3D Secure and re-directs the Customer to their Issuing Bank's 3D Secure page (ACS) |
| Customer enters in password |
| Bank's ACS re-directs the Customer back to Cardstream's 3D Secure facility |
| Cardstream completes the authentication |
| Cardstream re-directs the Customer's browser via HTTP POST to the Merchant's site, including the CAVV, Enrolled, Authenticated and ECI form fields. |
| Merchant sends an HTTP POST to the payment gateway, including the extra 3D Secure fields (next section) |

Tip: Re-directing a browser to a page using HTTP POST can be easily achieved by displaying a hidden form on a page and use JavaScript to automatically submit the form, e.g. -

```

<HTML>
<HEAD>
<SCRIPT Language=Javascript>
  function submitform () {
    document.payform.submit();
  }
</SCRIPT>
</HEAD>
<BODY onLoad="submitform()">

<FORM ACTION="https://3dsecure.cardstream.com:8443/cardStream/3DSecure.jsp" NAME="payform"
METHOD=POST>

  <INPUT TYPE=hidden NAME="VPMerchantID" VALUE="xxxxx">
  <INPUT.....
  .....
</FORM>
</BODY>
</HTML>

```

Transaction Request Using HTTP Direct

Card information is captured from a secure form on the Merchant's website or software application. This is then submitted to a processing script or service on the Merchant's system. The processing script then creates the transaction request and passes it via a secure HTTPS post over TCP/IP to the payment gateway. The payment gateway responds down the socket with the response to the transaction. Your processing script then breaks this response down into its component parts and actions accordingly, i.e. for success do X for fail do Y.

Please POST to the following URL -

<https://gateway.cardstream.com/process.ashx>

On registration the Merchant will have received a test account 'MerchantID and Password' that they will need to include in all of their transaction requests.

The following tables detail the variables that are used to pass transaction data from the Merchant's website to the payment gateway. Every transaction that is passed to the payment gateway must include the fields listed in the 'Mandatory Generic Transaction Request HTML Fields' table. Dependent upon the card details entry method, either chip/swipe or keyed/Internet, every transaction submitted must include the fields listed in 'Mandatory Card Keyed Transaction Request HTML Fields' table. A selection of optional fields is provided from which further functionality can be accessed.

| Mandatory Fields | | | | |
|---|--|-------|------|-----------------|
| These fields must be passed to the payment gateway. | | | | |
| Field Name | Description | Req'd | Size | Type |
| VPMerchantPassword | This variable is a control variable to help ensure the security of client transactions. This variable value is created when the Merchant registers with Cardstream and must be set as a value to be passed to the payment page from the Merchant's calling script. Example: VPMerchantPassword=123456 | Yes | 32 | Alpha - Numeric |
| VPMerchantID | This variable is a control variable to help ensure the security of client transactions. This variable value is created when the Merchant registers with Cardstream and must be set as a value to be passed to the payment page from the Merchant's calling script. Example: VPMerchantID= VelIT-DF3SW21 | Yes | 32 | Alpha - Numeric |

Cardstream Integration Guide

| | | | | |
|--|---|-----|----------|-----------------|
| VPAmount | The transaction amount, numeric, minor currency i.e. pence/cents etc. NO DECIMAL POINT e.g. £10.02 = 1002 Example: VPAmount=6545 (This equates to 65.45 of specified currency) | Yes | 10 Max. | Numeric |
| VPCountryCode | ISO standard country code for Merchant location. Use 826 for UK based Merchants. Other options available on request. Example: VPCountryCode=826 | Yes | 3 | Numeric |
| VPCurrencyCode | ISO standard currency code for a transaction. Use 826 for Sterling transactions. Other options available on request. Defaults to 826 if no other currency specified. Example: VPCurrencyCode=826 | Yes | 3 | Numeric |
| VPTransactionUnique | A unique identifier set by the shopping cart. This is normally the invoice or purchase ID from the Merchant's website/application. Example: VPTransactionUnique=Invoice1234567 | Yes | Max 50 | Alpha - Numeric |
| VPOrderDesc | A unique value – most often an invoice number that will be displayed on the Customer's credit/debit card statement. Example: VPOrderDesc=VP Servicek-587811F2 | Yes | Max 50 | Alpha - Numeric |
| For 3D Secure Transactions Only. The following fields are mandatory if they are returned in the 3D Secure authentication request. | | | | |
| CAVV | 3D Secure authentication code | Yes | Variable | Alpha-numeric |
| ECI | E-Commerce indicator | Yes | Variable | Numeric |
| Enrolled | 3D Secure enrollment status | Yes | 1 | Y, U or N |
| Authenticated | 3D Secure authentication status | Yes | 1 | Y or N |

Cardstream Integration Guide

| | | | | |
|----------------|---------------------|-----|--|--|
| CAVVAAlgorithm | CAVV Algorithm Code | Yes | | |
|----------------|---------------------|-----|--|--|

The following variables are mandatory or optional based on the card type that is being processed. As the payment gateway is intuitive it can work out what kind of card the Merchant has passed to it and, therefore, what fields to use. It is best practice to have all the fields present on your form, force entry on the mandatory fields and present all the optional fields as optional form entry. Below M = Mandatory and O = Optional.

| Card Data Fields | | | | | |
|------------------|--------------------|---------|-------|--------|-----------------|
| Fields Name | Description | Service | Req'd | Length | Type |
| VPCardName | Exact Name On Card | VP | M | 50 max | Alpha - Numeric |
| VPCardNumber | Card number | VP | M | 20 max | N |
| VPExpiryDateMM | Expiry month | VP | M | 2 | N |
| VPExpiryDateYY | Expiry year | VP | M | 2 | N |
| VPIssueNumber | Issue number | VP | M/O* | 2 max | N |
| VPStartDateMM | Start month | VP | M/O* | 2 | N |
| VPStartDateYY | Start year | VP | M/O* | 2 | N |

The following table details fields that are optional. Activating or de-activating these fields will control how the payment gateway responds to the Merchant's transaction request.

| Optional & Extra Fields | | | | | |
|-------------------------|---|---------|-------|-------|------|
| Field Name | Description | Service | Req'd | Size | Type |
| VPSDispatch | Merchants can either pre-authorise a transaction or take payment immediately. This is described later in this guide. Two possible settings are: VPSDispatch=NOW, set this to take payment immediately. Or VPSDispatch=LATER, set this to defer taking payment until the Merchant is ready to ship the goods or service. | VP | O | Max 5 | A |

Cardstream Integration Guide

| | | | | | |
|----------------------|--|----|--------|---------|---|
| VPCrossReference | 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 primarily for issuing refunds and completing transactions that were originally submitted as VPDispatch = LATER. Note: Merchants who wish to conduct transactions using Cross References must do so from a static IP address(es) that has/have been registered with Cardstream. | VP | O | 50 max | A |
| VPCV2 | Card Verification Value normally 3 digits printed on the right hand end of the signature strip (if applicable). Note: The CV2 value should not be stored under any circumstances – the value should be passed directly to Cardstream. See also VPAVSCV2Check and VPEchoAVSCV2ResponseCode. | VP | VP O M | 3 or 4 | N |
| VPDuplicateDelay | This delay helps to prevent duplicate transactions passing through the gateway, e.g. in the circumstance that a user accidentally clicks a submission button more than once in quick succession. Supply the delay required in seconds, e.g. 30 = 30 seconds. Supplying a value of 0 disables the duplicate check. The default value is configurable by request, initially set to 300 (5 minutes). | VP | O | 4 max | N |
| VPBillingHouseNumber | Required for AVS check. Customers House Number. This is the house number registered by the Customer with their card Issuing Bank. | VP | O | 100 max | A |
| VPBillingStreet | Required for AVS check. Customers Street Name. This is the street name registered by the Customer with the card Issuing Bank. | VP | O | 100 max | A |
| VPBillingCity | Required for AVS check. Customer's city or town. This is the city or town registered by the Customer with the card Issuing Bank. | VP | O | 100 max | A |
| VPBillingState | Required for AVS check. Customers state or county. This is the state or county registered by the Customer with the card Issuing Bank. | VP | O | 100 max | A |

Cardstream Integration Guide

| | | | | | |
|----------------------|---|----|-----|--------|---|
| VPBillingPostCode | 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 VPBillingPostCode. | VP | O | 10 max | A |
| VPBillingEmail | 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 VPBillingEmail. | VP | O | 50 max | A |
| VPBillingPhoneNumber | 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 VPBillingPhoneNumber. | VP | O | 30 max | A |
| VPMessageType | Used to tell the payment gateway what type of transaction to process. Possible settings are detailed below. | VP | O/M | 33 Max | A |

VPMessageType Possible Settings

Description of the possible settings for VPMessageType and the action that is taken. VPMessageType is basically the instruction message to the payment gateway to inform it what action to take.

| Message Type | Message Description & Function |
|---------------|--|
| 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. |
| ESALE_CARD | eCommerce (Internet) sale transaction, card details read from chip or swiped by cardholder (both Merchant and Customer not present). Cardstream will determine the exact mode of entry from the track 2 or track 2 equivalent data submitted in the Track2Data field. Note: Maybe prefixed with PAYMENT_ONLY_ see following note. |
| ESALE_KEYED | eCommerce (Internet) sale transaction, card keyed by cardholder (both Merchant and Customer not present). Note: Maybe prefixed with PAYMENT_ONLY_ see following note. |
| REFUND_KEYED | Refund transaction, card details keyed at point of sale (Customer present). Note: The Cross Reference of the original transaction – if processed though Cardstream within the previous 180 days – may be used in lieu of card details. |
| EREFUND_KEYED | eCommerce (Internet) refund transaction, card details read from chip or swiped by cardholder (both Merchant and Customer not present). Cardstream will determine the exact mode of entry from the track 2 or track 2 equivalent data submitted in the Track2Data field. Note: The Cross Reference of the original transaction – if processed though Cardstream within the previous 180 days – may be used in lieu of card details. |

| Common Currency Codes | |
|--|---|
| The common currency codes are listed below. For a full list please obtain a copy of the ISO-4217 list. | |
| Currency | ISO-4217 Currency Code (Numeric) |
| Australian Dollar | 036 |
| Canadian Dollar | 124 |
| Czech Koruna | 203 |
| Danish Krone | 208 |
| Euro | 978 |
| Hong Kong Dollars | 344 |
| Icelandic Krona | 352 |
| Japanese Yen | 392 |
| Norwegian Krone | 578 |
| Pounds Sterling | 826 |
| Singapore Dollars | 702 |
| Swedish Krona | 752 |
| Swiss Franc | 756 |
| US Dollars | 840 |

Transaction Response

The response generated after a transaction is completely is dependant upon what variables have been sent with the transaction request. A simple response would look like this -

```
VPResponseCode=00&VPCrossReference=04100514165800502449&VPMessage=AUTHCODE:
00502&VPTransactionUnique=VP ORDER123456789&VPOrderDesc=VP ORDER-
1234567897&VPAmountReceived=1299&VPAVSCV2ResponseCode=222100&VPCV2ResultMessage=CV2
Matched&VPCardType=VD
```

The gateway will return a string similar to the one above. When broken down this example yields the following variables -

```
VPResponseCode =00
VPCrossReference =04100514165800502449
VPMessage=AUTHCODE:00502
VPTransactionUnique =VP ORDER-123456789
VPOrderDesc =VP ORDER-123456789
VPBillingCountry =826
VPAmountReceived=1299
VPAVSCV2ResponseCode =222100
VPAVSCV2ResultMessage =CV2 Matched
VPCardType =VD
```

In this case the transaction was successful as indicated by a response of 00 from the gateway. Full details of response codes are listed below.

| Default Response Variables From The Payment Gateway | | | |
|--|--|--------|------|
| The following fields will be returned with every transaction regardless of what is passed to the payment gateway and they tell the Merchant the status of the transaction request. This will either be an authorisation from the Merchant's Acquiring Bank or in the case of a malformed transaction request a response saying what was wrong with the transaction. Successful transactions are given a unique cross reference that can be used at a later date. | | | |
| Field Name | Contents | Size | Type |
| VPResponseCode | The Cardstream response code. See table that follows. | 2 | N |
| VPMessage | The transaction message either as delivered by the bank or by Cardstream. 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, AVSCV2 DECLINED and ERROR XXXX. Note: In the case where a transaction is either malformed or the payment gateway has detected a problem with the data submitted, the response will return what was detected wrong with the data in this field. The possible responses are two wide and varied to fully list here but are normally self-explanatory. Example VPMessage=CARD EXPIRED | 80 max | A |

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

| Possible Response Codes For VPResponseCode | |
|--|-----------------------------------|
| This is the complete list of the response codes from the Payment Gateway | |
| Gateway Response Code | Description |
| 00 | Transaction successful/authorised |
| 02 | Card referred |
| 04 | Card decline – keep card |
| 05 | Card declined |
| 30 | Exception |

Optional Responses Following Either a Successful or Unsuccessful Transaction

Depending on what the Merchant has sent to the payment gateway with the transaction request. Not all the variables are listed here, just the ones that need an explanation.

| Possible Response Codes For VPResponseCode | | |
|--|--|--------|
| Field Name | Description | Size |
| VPCrossReference | The unique character string supplied by Cardstream to identify this transaction. The value in VPCrossReference following completion of a successful transaction will contain a unique reference that the Merchant may use to run future transactions (re-authorisation, re-run or refund) - please note that cross reference transactions must come from a static IP address that has been pre-registered with Cardstream. To register an IP address, please send details to solutions@cardstream.com with the relevant Cardstream issued MerchantID and it will be added to your account accordingly. | 50 max |

| This variable is returned when VPEchoAVSCV2ResponseCode=YES is submitted to the payment gateway. | | |
|--|--|------|
| Field Name | Description | Size |
| VPAVSCV2ResponseCode | The raw AVS/CV2 code returned by the Merchant's Acquiring Bank – see following tables. Only sent back if requested. Returned if transaction request field VPEchoAVSCV2ResponseCode was set to YES. Not returned if Cardstream VPResponseCode = 30. See tables below for how to interpret the raw response. | 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 Merchant's Acquiring Bank.

| Position 1 Value | Position 1 Value Description |
|------------------|--------------------------------------|
| 0 | No additional information available. |
| 1 | CV2 not checked. |
| 2 | CV2 matched. |

Cardstream Integration Guide

| | |
|---|------------------|
| 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 |

| VPCardType | | |
|---|--|------|
| The variable is returned when VPEchoCardType=YES is submitted to the gateway. Possible card type abbreviations are listed in the table below. | | |
| Field Name | Description | Size |
| VPCardType | The card type used for the transaction – see following table. Only sent back if requested. Returned if transaction request field VPEchoCardType was set to YES. Not returned if Cardstream VPResponseCode = 30 | 2 |

| Card Type Code | Card Type |
|----------------|-----------------------|
| AM | American Express |
| DI | Diners Club |
| EL | Electron |
| JC | JCB |
| MA | UK Maestro |
| MI | Maestro International |
| MC | MasterCard |
| ST | Style |
| VC | Visa Credit |
| VD | Visa Debit |
| VP | Visa Purchasing |

The Integration Process

The Integration process is straight forward for any service with Cardstream. Before beginning to integrate the Merchant must register with us at www.cardstream.com. Following registration and email verification the Merchant will receive emails with details for both their test account and their live account. Note that the live account will be disabled until such time as a Cardstream has connected the Merchant's Cardstream Account to their Merchant Account. The Merchant may run in simultaneous test and live modes.

Integration Support

Cardstream offers integration and post integration support for any Merchant registered with Cardstream. During the integration process the Merchant may have questions that require answering or run into issues that need resolving. Please follow the procedure below when trying to resolve any issues during the Cardstream Integration process.

1. solutions@cardstream.com - Every support request must be initially directed to this support email address. When sending in a request, please provide as much detail as possible in order to assist the support team in providing an answer or resolution. It is very helpful to have the date and time of the transaction attempt, the exact response from the payment gateway in addition to the Merchant ID and Password of the account used when attempting the transaction. If logs or stack traces are available please include these as well. If insufficient information is submitted, the support team will more than likely request the above and this could result in receipt of the answer to the question or the resolution to the issue being delayed.
2. **Direct Developer Contact** – Often Merchant's will employ/contract a developer to create the technology that will be integrating with Cardstream. In our experience, it works best to have the developer or the Merchant's technical staff as the point of contact during the Cardstream Integration. This will provide efficiency in dealing with technical issues.
3. **Telephone Support** – Cardstream offers technical support via the telephone during normal business hours – see www.cardstream.com/contact_us.asp. NB – this is not Cardstream's preferred way in which to deal with support queries and would at all times prefer that first contact regarding a query is made by sending an email to solutions@cardstream.com.

Appendix 1: AVS / CV2 Primer

The card industry has introduced two optional anti-fraud checks that can be carried out at the same time as an authorisation. These checks are known as AVS and CV2, they have been developed in response to the increase in fraudulent transactions. A large majority of these fraudulent transactions occur where the Customer is not present at the point of sale, e.g. mail/telephone order or Internet transactions.

When using AVS/CV2 the Merchant must be fully aware that it is simply a check and in no way should be relied on solely when deciding whether to accept an order and go on to ship goods. It should be used ONLY as a tool to assist in making that decision.

AVS (Address Verification Service)

The Address Verification Service (AVS) is used to confirm that the postal address given by the Customer during a transaction matches the Customer's billing address held by their card Issuing Bank.

The AVS checks the numeric values of the full address and postcode given by the Customer against those details held by their card Issuing Bank. Upon submission of a full address and postcode, Cardstream will derive the AVS check value and pass it to the Customer's Issuing Bank for verification.

The AVS check is one way of attempting to verify that the Customer is the legitimate user of the card but it is by no means fool proof. Sometimes information held by Issuing Banks can be out of date or different from that which the Customer thinks they hold. Also many Issuing Banks do not support the AVS checking facility and on occasion, but rarely, the data simply cannot be checked.

CV2 (Card Verification Value)

The name CV2 is a collective acronym 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 at the right hand end of the signature strip on the back of a credit/debit card. The purpose of this number and the optional check that can be carried out with it is to confirm that the Customer is actually in possession of the card at the time of the transaction being processed.

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 (easy targets for fraudsters), 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 who intends to use the card fraudulently via a Merchant set up to check for CV2 verification.

Using AVS and CV2 with Cardstream

The Banking Industry has 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 with 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. This methodology is acceptable in situations where the Merchant is present, such as traditional retail shops/outlets and call centres where a Merchant is available to make a decision. However, it is more difficult for a Merchant to make a decision when they are not present, e.g. via the Internet.

In order to simplify and automate this decision making process Cardstream provides a system by which the Merchant

can set up their own specific AVS/CV2 acceptance conditions on the payment gateway. If a transaction response is received from the Bank with an AVS/CV2 result within the Merchant's acceptance conditions, Cardstream 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 outside of the Merchant's acceptance conditions, the authorisation is automatically reversed and Cardstream does not present the transaction for settlement. In this instance, Cardstream returns a VPResponseCode of 05, a response VPMessage of AVSCV2 DECLINED and the transaction's Cross Reference to the Merchant. By default AVS/CV2 checking is enabled in its most secure form, to change these settings please contact customer support via email – solutions@cardstream.com.

Appendix 3: Guide to Processing American Express and Diners Club Card Transactions via Cardstream Direct

This appendix describes the procedure and requirements for passing Line Item Detail information to Cardstream Direct for American Express and Diners Club cards. Before a Merchant can begin to process American Express or Diners Club card transactions, they must have first been issued with a Merchant Account Number from either American Express or Diners Club. Once the Merchant has this Merchant Account Number, Cardstream can complete the necessary set-up procedures and create the Merchant another routing in the MMS.

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 Issuing Bank 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 Details Fields | | | | | |
|--|---------------------|---|---|--------|---|
| In order to process an AMEX or Diners Club transaction Merchants will need to submit at least the first three fields listed below in addition to all the standard fields that would normally be submitted. | | | | | |
| 1.1 | VP AEIT1Quantity | Quantity of item 1 | M | 3 max | N |
| 1.2 | VP AEIT1Description | Description of item 1 | M | 15 max | A |
| 1.3 | VP AEIT1GrossValue | Gross value of item 1 in minor currency units | M | 10 max | N |
| 2.1 | VP AEIT2Quantity | Quantity of item 2 | O | 3 max | N |
| 2.2 | VP AEIT2Description | Description of item 2 | O | 15 max | A |
| 2.3 | VP AEIT2GrossValue | Gross value of item 2 in minor currency units | O | 10 max | N |
| 3.1 | VP AEIT3Quantity | Quantity of item 3 | O | 3 max | N |
| 3.2 | VP AEIT3Description | Quantity of item 4 | O | 15 max | A |
| 3.3 | VP AEIT3GrossValue | Gross value of item 3 in minor currency units | O | 10 max | N |
| 4.1 | VP AEIT4Quantity | Quantity of item 4 | O | 3 max | N |
| 4.2 | VP AEIT4Description | Description of item 4 | O | 15 max | A |
| 4.3 | VP AEIT4GrossValue | Gross value of item 4 in minor currency units | O | 10 max | N |
| 5.1 | VP AEIT5Quantity | Quantity of item 5 | O | 3 max | N |
| 5.2 | VP AEIT5Description | Description of item 5 | O | 15 max | A |
| 5.3 | VP AEIT5GrossValue | Gross value of item 5 in minor currency units | O | 10 max | N |

| | | | | | |
|-----|--------------------|---|---|--------|---|
| 6.1 | VPAEIT6Quantity | Quantity of item 6 | O | 3 max | N |
| 6.2 | VPAEIT6Description | Description of item 6 | O | 15 max | A |
| 6.3 | VPAEIT6GrossValue | Gross value of item 6 in minor currency units | O | 10 max | N |

Appendix 4: Guide to handling deferred dispatch with Cardstream

Cardstream offers functionality to help Merchants who frequently dispatch several days after accepting an order. In these circumstances it is typical for the Merchant to *pre-authorise* the card prior to accepting the order and then submit the transaction for settlement at the time of dispatch.

Note: Cardstream uses an ordinary sale transaction type when submitting a dispatch later authorisation request to the Merchant's Acquiring Bank. Cardstream does this due to the fact that some Card Issuing Banks, to whom the authorisation request is usually forwarded by the Merchant's Acquiring Bank, do not support the standard pre-authorisation message type. Whilst this makes dispatch later transactions more reliable than a standard pre-auth, it does mean that the nominal authorisation amount shows on the cardholders account. Since dispatch later transactions themselves are never presented for settlement – it is the subsequent dispatch now that is settled – the Card Issuing Bank will automatically removed the authorization and this will usually happen within 3/4 working days. Importantly, the dispatch later transaction does affect the Customer's available credit; hence the use of a nominal amount will reduce this effect.

Implementation

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

1. Merchant's system submits an authorisation only transaction request for a 'nominal' amount, e.g. £1.01, with the Dispatch field set to LATER. This is accomplished by sending a normal transaction request with the following differences -

VPAmount = 101

VPDispatch = LATER

This transaction request 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. Cardstream will store the transaction for 180 days.
3. When ready for dispatch, the Merchant's system submits a simultaneous authorisation and settlement transaction request for the full amount using the Cross Reference stored in step 2 and with the VPDispatch field set NOW. This is accomplished by sending a normal transaction request with the following differences:

VPCrossReference = Cross Reference of transaction (see step 2) VPDispatch = NOW

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

Cardstream Integration Guide

Version 8.1 © Cardstream Ltd. All rights reserved.

For further help telephone **0845 00 99 575** or email **solutions@cardstream.com**

Appendix 5: Guide to handling continuous authority and re-authorisation transactions via Cardstream

Both continuous authority and re-authorisation via Cardstream are methods of re-charging a Customer without recourse to the original card details. The differences are as follows -

Continuous authority is for regular (daily, weekly or monthly) charging of a card. The Customer gives permission (authority) to the Merchant to charge the card without the Merchant needing to contact the Customer on each occasion. The benefit of using continuous authority over re-authorisation is that when a card expires, the Merchant can continue to charge the card without having to contact the Customer.

Note: A Merchant must have prior arrangement from their Acquiring Bank before they can begin to process continuous authority transactions.

Re-authorisation is for ad-hoc charging of a card. The cardholder's permission should be sought on every occasion.

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

Continuous authority implementation

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

1. The Merchant's system submits a normal transaction with a VPMessageType 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. Cardstream will store the transaction for Continuous Authority purposes for 32 days.
3. When the second transaction is ready to be processed, the Merchant's system submits a transaction again with a VPMessageType 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. Cardstream will again store the transaction for 32 days.
5. When the third transaction is ready to be processed, the Merchant's system submits a transaction again with a VPMessageType field of SALE_CA. The Cross Reference stored in step 4, however, is used in lieu of the card details fields.
6. And this continues for as long as the Customer agreed to be charged.

Re-authorisation implementation

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

1. The Merchant's system submits a normal transaction. This will authorise and settle the first transaction.

Cardstream Integration Guide

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. Cardstream will store the transaction for 32 days.
3. When the second transaction is ready to be processed and having gained the Customer's approval, the Merchant's system submits the transaction. The Cross Reference stored in step 2, however, is used in lieu of the card details fields.
4. And this continues for as long as the Customer gives their permission.