# CardEaseMPI

**a technical manual describing the use of CardEaseMPI 3-D Secure Merchant Plug-In.**

Authors: Nigel Jewell

Issue 2.9. November 2014.

**COMMERCIAL-IN-CONFIDENCE**

| Action | Name | Date |
|---|---|---|
| Created | Nigel Jewell | 31/05/2007 |
| Updated | Nigel Jewell | 18/01/2008 |
| Updated | Nigel Jewell | 18/04/2008 |
| Updated | Nigel Jewell | 13/08/2008 |
| Updated | Nigel Jewell | 24/08/2008 |
| Updated | Nigel Jewell | 31/10/2008 |
| Updated | Nigel Jewell | 30/12/2008 |
| Updated | Nigel Jewell | 14/09/2009 |
| Updated | Nigel Jewell | 10/02/2010 |
| Updated | Nigel Jewell | 03/03/2010 |
| Updated | Nigel Jewell | 14/07/2011 |
| Updated | Nigel Jewell | 14/12/2012 |
| Updated | Nigel Jewell | 28/05/2014 |
| Updated | Nigel Jewell | 11/11/2014 |

**Release**

| Version | Date Released | Change Notice | Pages Affected | Remarks |
|---|---|---|---|---|
| Draft A | 31/05/2007 | | | Draft |
| 1.1 | 18/01/2008 | | 4 | URL |
| 1.2 | 18/04/2008 | | 3, 4 | Constraints |
| 1.3 | 13/08/2008 | | 5, 6 | CardEaseXML |
| 2.0 | 24/08/2008 | | All | XML Protocol |
| 2.1 | 31/10/2008 | | 10 | Acquirer BINs |
| 2.2 | 30/12/2008 | | 9 | Error handling |
| 2.3 | 14/09/2009 | | 4, 7 | Merchant IDs |
| 2.4 | 10/02/2010 | | 10, 11 | ACS Warning |
| 2.5 | 03/03/2010 | | 10 | Barclays BIN |
| 2.6 | 14/07/2011 | | 4, 7, 10 | Merchant IDs |
| 2.7 | 14/12/2012 | | 4, 5 | Schemes |
| 2.8 | 28/05/2014 | | 10 | Acquirer BINs |
| 2.9 | 11/11/2014 | | 10 | Test Cards |

**Distribution List**

| Name | Organisation | Title |
|---|---|---|
| David Kinmond | CreditCall | Development Manager |
| Jeremy Gumbley | CreditCall | Chief Security Officer |
| Creditcall Board | CreditCall | |

# CardEaseMPI

### Introduction

CardEaseMPI is a hosted 3-D Secure Merchant Plug-In that allows for E-Commerce sites to accept and process Verified by Visa and MasterCard SecureCode authentications. The result of these authentications can then be used during the payment authorisation process providing conformance with card scheme rules and greater liability shift for the merchant.

For ease of integration and compatibility with existing web technologies, CardEaseMPI makes extensive use of the HTTP protocol, and specifically POST requests. The Merchant Plug-In accepts two kinds of POST data; HTML POST and XML POST. The HTML POST method is the easiest solution to integrate with; however it requires that the merchant website performs additional HTTP redirections of the card holder's web browser and in certain situations (such as session expiry) it can mean that error recovery is impossible. The XML POST method requires additional integration due to the necessity of constructing and parsing XML data, however it allows the merchant website finer control over the redirections required of the card holder's web browser and allows complete control over error conditions.

Detailed below are the specifics of using each of the HTML POST and XML POST MPI requests. For the purpose of integration with a merchant website consideration should be given to the entire process flow before a decision is made between the HTML and XML solutions. If it is required CreditCall can make available a PHP example of each method. These examples are constructed in such a way that they should allow a web developer to understand of the 3-D Secure solution without a need to be a PHP developer.

# CardEaseMPI HTML POST

For integration with CardEaseMPI using HTML POST the card holder's web browser must be directed to post a number of name/value pairs to the MPI.

If the specification of the name/value pairs is correct, the card number is checked for enrolment in the 3-D Secure scheme to which it relates. Cards that are not fully enrolled in the appropriate scheme may cause the card holder's web browser to redirect the enrolment page of the card issuer if they are participating in the 3-D Secure program. If the issuer is not a participant, control is returned to the E-Commerce site with the result of the 3-D Secure transaction.

Cards that are enrolled in either Verified by Visa or MasterCard SecureCode prompt the MPI or the merchant's website to redirect the card holder's web browser to the authentication page of the card issuer. The card holder will be asked for their security information and alternatively provided with the ability to confirm their identity if they have forgotten it.

When the 3-D Secure process is complete the MPI returns control to a user specified success or failure page by posting a number of name/value pairs. These name/value pairs can then be used in the authorisation process to provide 3-D Secure information.

The request and response name/value pairs are described in detail below as well as an overview of how to interpret the responses for the authentication process.

### Request

In order to initiate a CardEaseMPI HTML POST request a number of name/value pairs must be posted to the CardEaseMPI URL.

For test transactions the following address should be used.

https://testmpi.cardeasexml.com

For live transactions the following address should be used:

https://mpi.cardeasexml.com

Please note that live transactions cannot be performed until CreditCall have registered the merchant account with the MPI.  Even then, it can take up to two weeks for the registration process to be completed with MasterCard and Visa meaning that the MPI may not return fully authenticated results initially.

The fields used in the HTML are:

| Field | Description |
|---|---|
| AcquirerBIN | The Bank Identification Number (BIN)/Issuer Identification Number (IIN) of the acquiring institution.  This should be specified as 1 to 11 digit number.  For the test platform this should be specified as 123456.  Please note that for live integrations two BINs will be used, one for MasterCard and one for Visa cards (a list of these can be found at the end of this document).  Card schemes can be recognised by looking at the first few digits of the card number.  Reliable references for these numbers can be found on the internet or can be suggested by CreditCall as required. |
| Amount | The amount that will be charged to the credit card.  This should be specified in the major format for the currency and should not contain and currency identifier.  For example, if the credit card is to be charged £1.23, the amount should be specified as 1.23.  It can be specified without the major or minor part if required.  For example: 12.34, 12 and .34.  The maximum major length is 10 digits. |
| CurrencyCode | The 3-digit ISO4217 code for the currency in which the authorisation will take place.  For example, if the credit card is to be charged in pound sterling, the currency code should be specified as 826. |
| ExpiryDateMonth | The month in which the credit card is due to expire.  This should be specified as a 2-digit number in the range 01 to 12. |
| ExpiryDateYear | The year in which the credit card is due to expire.  This should be specified as a 4-digit number. |
| FailureURL | The URL to which failed authentications should be transferred along with the associated name/value pairs of the result.  The can be the same as the SuccessURL.  It should contain the http:// or https:// prefix. |
| MerchantID | The Merchant ID assigned by the acquiring institution.  This should be specified as a 1 to 24 digit number.  For the test platform this should be specified as 123456789012345.  Please note that for live transactions two Merchant IDs may be used, one for MasterCard and one for Visa cards.  The Merchant ID should be zero padded to a specific length (a list of these can be found at the end of this document).  For example an AIB Merchant ID of 1234567 would become 12345670000.  Card schemes can be recognised by looking at the first few digits of the card number.  Reliable references for these numbers can be found on the internet or can be suggested by CreditCall as required. |
| PAN | The credit card number from which the payment will be made.  This should not contain any spaces or formatting characters.  This should be specified as a 13 to 19 digit number. |
| SuccessURL | The URL to which successful authentications should be transferred along with the associated name/value pairs of the result.  This can be the same as the FailureURL.  It should contain the http:// or https:// prefix. |
| TransactionNarrative | An optional description of the purchase.  This should be specified as a 0 to 125 character string. |
| XID | A 20-character alphanumeric transaction number that is statistically unique.  This can either be created randomly, or assigned on a sequential basis. |

If any user-defined name/value pairs are present that are not a requirement of the MPI these are posted back to the success and failure URL.  In order to ensure compatibility with future revisions of the MPI, it is suggested that user-defined names are prefixed with string specific to the E-Commerce site.

A sample form would look like this:

```
<form action=”https://testmpi.cardeasexml.com” method=”post”>
      <input type=”text” name=”AcquirerBIN” value=”123456”/>
      <input type=”text” name=”Amount” value=”1.23”/>
      <input type=”text” name=”CurrencyCode” value=”826”/>
      <input type=”text” name=”ExpiryDateMonth” value=”12”/>
      <input type=”text” name=”ExpiryDateYear” value=”2020”/>
      <input type=”text” name=”MerchantID” value=”123456789012345”/>
      <input type=”text” name=”PAN” value=”4444333322221111”/>
      <input type=”text” name=”TransactionNarrative” value=”1 Item”/>
      <input type=”text” name=”XID” value=”KmhC40IN3aqJprzalc8P”/>

      <input type=”text” name=”example_shop_custom1” “example1”/>
      <input type=”text” name=”example_shop_custom2” “example2”/>

      <input type=”submit”/>
</form>
```

**Response**

The information returned by the CardEaseMPI contains a number of fields that determine how the result of the 3-D Secure transaction should be interpreted. These are:

| Field | Description |
|---|---|
| AcquirerBIN | The Bank Identification Number (BIN)/Issuer Identification Number (IIN) of the acquiring institution. As supplied in the request. |
| Amount | The amount that will be charged to the credit card. As supplied in the request. |
| CardHolderEnrolled | Whether the card holder is enrolled in the 3-D Secure scheme. Can be one of Y, N, U or an empty value. |
| CurrencyCode | The 3-digit ISO4217 code for the currency in which the authorisation will take place. As supplied in the request. |
| ECI | The E-Commerce indicator returned when a 3-D Secure authentication is attempted. |
| ErrorCode | The code of any error encountered during the authentication process. |
| ErrorDetail | The detailed message of any error encountered during the authentication process. |
| ErrorMessage | The short message of any error encountered during the authentication process. |
| ExpiryDateMonth | The month in which the credit card is due to expire. As supplied in the request. |
| ExpiryDateYear | The year in which the credit card is due to expire. As supplied in the request. |
| FailureURL | The URL to which failed authentications should be transferred. As supplied in the request. |
| IAV | The Cardholder Authentication Verification Value (CAVV)/Accountholder Authentication Value (AAV) returned when a 3-D Secure authentication is attempted. |
| IAVAlgorithm | The algorithm used for the IAV. Returned when a 3-D Secure authentication is attempted. |
| MerchantID | The merchant ID assigned by the acquiring institution. As supplied in the request. |
| PAN | The credit card number from which the payment will be made. As supplied in the request. |
| SuccessURL | The URL to which successful authentications should be transferred. As supplied in the request. |
| TransactionNarrative | An optional description of the purchase. As supplied in the request. |
| TransactionStatus | Whether the authentication of the card holder succeeded. Can be one of Y, N, A, U or an empty value. |
| XID | A 20 character alphanumeric statistically unique transaction number. As supplied in the request. |

If any user-defined name/value pairs are present that are not a requirement of the MPI these are posted back to the success and failure URL.

# CardEaseMPI XML POST

For integration with CardEaseMPI using XML POST the merchant’s website must POST a well formed XML string to the MPI. It is important that the XML string is encoded using UTF-8 and that the Content-Type header (also known as HTTP MIME type) is set to “application/xml”. The XML will be validated against an appropriate schema.

Unlike the HTML POST integration, the XML POST method accepts two different messages; one to determine the enrolment status of a particular transaction, another to determine the result of the card holder authentication.

If the specification of the XML data is correct and an enrolment request is received, the card number is checked for enrolment in the 3-D Secure scheme to which it relates. The result of this enrolment is returned to the merchant’s website. If the card holder is either partially or fully enrolled the resultant XML will contain the address to which the card holder browser must be redirected in order to perform card holder authentication or full enrolment.

The redirection to the card issuer’s Access Control Server must be performed using HTTP POST and three POST parameters should be supplied:

1. PaReq: The Payer Authentication Request as returned from the MPI in the response to the enrolment request.
2. MD: The Merchant Data identifier generated by the merchant’s website. This can be empty, or alternatively it can be used to associate a particular authentication request with a particular session on the merchant web server. MD can contain the ASCII characters 0x20 to 0x7E. If other data is required the field should be Base64 encoded. The field has a maximum length of 1024 characters.
3. TermUrl: The URL on the merchant’s web site to which the card holder’s browser should send the POST data on completion. This POST data will include the PaRes that is required for the MPI authentication process.

The result of the card holder authentication is returned from the card holder’s web browser as HTTP POST data. This POST data includes PaRes and MD fields. It is recommended that the MD field is verified against the web server to validate the source of the message. The PaRes field must then be sent to the MPI as well formed XML. Again, it is important that the XML string is encoded as UTF-8 and that the Content-Type header (also known as HTTP MIME type) is set to “application/xml”. The XML will be validated against the appropriate schema.

If the specification of the XML data is correct the MPI checks the result of the authentication and returns it to the merchant’s website. The result can then be used in the authorisation process to provide 3-D Secure information.

The request and response XML structures are described in detail below as well as an overview of how to interpret the responses for the authorisation process.

**Request**

In order to initiate a CardEaseMPI XML POST request an XML string must be posted to the CardEaseMPI URL.

For test transactions the following address should be used.

https://testmpi.cardeasexml.com

For live transactions the following address should be used:

https://mpi.cardeasexml.com

Please note that live transactions cannot be performed until CreditCall have registered the merchant account with the MPI. Even then, it can take up to two weeks for the registration process to be completed with MasterCard and Visa meaning that the MPI may not return fully authenticated results initially.

The XML structure for an enrolment request is:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<Request>
     <Enrollment>
          <AcquirerBIN></AcquirerBIN>
          <Amount></Amount>
          <CurrencyCode></CurrencyCode>
          <ExpiryDateMonth></ExpiryDateMonth>
          <ExpiryDateYear></ExpiryDateYear>
          <MerchantID></MerchantID>
          <PAN></PAN>
          <Password></Password>
          <TransactionNarrative></TransactionNarrative>
          <XID></XID>
     </Enrollment>
</Request>
```

The fields used in the XML are:

| Field | Description |
|---|---|
| AcquirerBIN | The Bank Identification Number (BIN)/Issuer Identification Number (IIN) of the acquiring institution. This should be specified as 1 to 11 digit number. For the test platform this should be specified as 123456. Please note that for live integrations two BINs will be used, one for MasterCard and one for Visa cards (a list of these can be found at the end of this document). Card schemes can be recognised by looking at the first few digits of the card number. Reliable references for these numbers can be found on the internet or can be suggested by CreditCall as required. |
| Amount | The amount that will be charged to the credit card. This should be specified in the major format for the currency and should not contain and currency identifier. For example, if the credit card is to be charged £1.23, the amount should be specified as 1.23. It can be specified without the major or minor part if required. For example: 12.34, 12 and .34. The maximum major length is 10 digits. |
| CurrencyCode | The 3-digit ISO4217 code for the currency in which the authorisation will take place. For example, if the credit card is to be charged in pound sterling, the currency code should be specified as 826. |
| ExpiryDateMonth | The month in which the credit card is due to expire. This should be specified as a 2-digit number in the range 01 to 12. |
| ExpiryDateYear | The year in which the credit card is due to expire. This should be specified as a 4-digit number. |
| MerchantID | The Merchant ID assigned by the acquiring institution. This should be specified as a 1 to 24 digit number. For the test platform this should be specified as 123456789012345. Please note that for live transactions two Merchant IDs may be used, one for MasterCard and one for Visa cards. The Merchant ID should be zero padded to a specific length (a list of these can be found at the end of this document). For example an AIB Merchant ID of 1234567 would become 12345670000. Card schemes can be recognised by looking at the first few digits of the card number. Reliable references for these numbers can be found on the internet or can be suggested by CreditCall as required. |
| PAN | The credit card number from which the payment will be made. This should not contain any spaces or formatting characters. This should be specified as a 13 to 19 digit number. |
| Password | The CardEaseMPI password that has been supplied by CreditCall. For the test platform this should be specified as P@ssw0rd. |
| TransactionNarrative | An optional description of the purchase. This should be specified as a 0 to 125 character string. |
| XID | A 20-character alphanumeric transaction number that is statistically unique. This can either be created randomly, or assigned on a sequential basis. |

The XML structure for an authentication request is:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<Request>
     <Authentication>
          <Password></Password>
          <PayerAuthenticationResponse></PayerAuthenticationResponse>
     </Authentication>
</Request>
```

The fields used in the XML are:

| Field | Description |
|---|---|
| Password | The CardEaseMPI password that has been supplied by CreditCall. For the test platform this should be specified as P@ssw0rd. |
| PayerAuthenticationResponse | The response returned from the card issuer's website. |

**Response**

The information returned by the CardEaseMPI contains a number of fields that determine how the result of the 3-D Secure transaction should be interpreted. These are:

The XML structure for an enrolment response can contain an Enrollment tag and/or an Error tag:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
     <Enrollment>
          <AccessControlServerURL></AccessControlServerURL>
          <CardHolderEnrolled></CardHolderEnrolled>
          <PayerAuthenticationRequest></PayerAuthenticationRequest>
     </Enrollment>
     <Error>
          <Code></Code>
          <Detail></Detail>
          <Message></Message>
     </Error>
</Response>
```

| Field | Description |
|---|---|
| AccessControlServerURL | The URL of the card issuer's Access Control Server that is to be used for authentication or enrolment purposes. |
| CardHolderEnrolled | Whether the card holder is enrolled in the 3-D Secure scheme. Can be one of Y, N, U or an empty value. |
| Error Code | The code of any error encountered during the authentication process. |
| Error Detail | The detailed message of any error encountered during the authentication process. |
| Error Message | The short message of any error encountered during the authentication process. |
| PayerAuthenticationRequest | The PaReq data to be sent to the card issuer's Access Control Server as HTTP POST data. This should be accompanied by the MD and TermUrl parameters. |

The XML structure for an authentication response can contain an Authentication tag and/or an Error tag:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
     <Authentication>
          <ECI></ECI>
          <IAV></IAV>
          <IAVAlgorithm></IAVAlgorithm>
          <TransactionStatus></TransactionStatus>
     </Authentication>
     <Error>
          <Code></Code>
          <Detail></Detail>
          <Message></Message>
     </Error>
</Response>
```

| Field | Description |
|---|---|
| ECI | The E-Commerce indicator returned when a 3-D Secure authentication is attempted. |
| Error Code | The code of any error encountered during the authentication process. |
| Error Detail | The detailed message of any error encountered during the authentication process. |
| Error Message | The short message of any error encountered during the authentication process. |
| IAV | The Cardholder Authentication Verification Value (CAVV)/Accountholder Authentication Value (AAV) returned when a 3-D Secure authentication is attempted. |
| IAVAlgorithm | The algorithm used for the IAV. Returned when a 3-D Secure authentication is attempted. |
| TransactionStatus | Whether the authentication of the card holder succeeded. Can be one of Y, N, A, U or an empty value. |

## Response Interpretation

The action that should be performed by the E-Commerce site upon receiving the response from either the HTML POST or XML POST process is dependant upon the value that is held in the CardHolderEnrolled and TransactionStatus fields.

| Cardholder Enrolled | Transaction Status | Action |
|---|---|---|
| Y | Y | The card holder was enrolled and authentication successful. Perform an authorisation sending all of the 3-D Secure data to CardEaseXML as part of the Request object (CardHolderEnrolled, TransactionStatus, ECI, IAV, IAV Algorithm and XID). |
| Y | N | The card holder was enrolled and authentication failed. **Do not perform an authorisation.** |
| Y | U | The card holder was enrolled and authentication could not be completed due to a technical problem. Perform an authorisation sending all of the 3-D Secure data to CardEaseXML as part of the Request object (CardHolderEnrolled, TransactionStatus, ECI, IAV, IAV Algorithm and XID). |
| Y | A | The card holder was not fully enrolled and they chose to decline full enrolment. Perform an authorisation sending all of the 3-D Secure data to CardEaseXML as part of the Request object (CardHolderEnrolled, TransactionStatus, ECI, IAV, IAV Algorithm and XID). |
| Y | | The card holder was enrolled however no valid response was obtained from the Access Control Server and therefore authentication could not be determined. Optionally perform an authorisation sending all of the 3-D Secure data to CardEaseXML as part of the Request object (CardHolderEnrolled, TransactionStatus, ECI, IAV, IAV Algorithm and XID). |
| N | | The card holder was not enrolled. Perform an authorisation sending the 3-D Secure result fields (CardHolderEnrolled and TransactionStatus) to CardEaseXML as part of the Request object. |
| U | | It was not possible to determine enrolment due to a technical problem with the Directory Server. Perform an authorisation sending the 3-D Secure result fields (CardHolderEnrolled and TransactionStatus) to CardEaseXML as part of the Request object. |
| | | No valid response was obtained from the Directory Server and therefore enrolment could not be determined. Perform an authorisation sending the 3-D Secure result fields (CardHolderEnrolled and TransactionStatus) to CardEaseXML as part of the Request object. |

### Error Codes

Once integration is complete many of the error conditions should never occur (such as 1015:Invalid Expiry Date or 1004:Missing Parameter). In these cases when an error condition is returned it often relates to an issue outside of the merchants control (such as a MasterCard or Visa directory server that is unreachable). Therefore, it is recommended that CardHolderEnrolled and TransactionStatus fields are processed as described above, and error codes, detail and messages are logged for information.

### CardEaseXML Mapping

When used with CreditCall's CardEaseXML the CardEaseMPI responses should be mapped as:

CardHolderEnrolled

| CardEaseMPI | CardEaseXML |
|---|---|
| Y | Yes |
| N | No |
| U | Unknown |
|  | None |

TransactionStatus

| CardEaseMPI | CardEaseXML |
|---|---|
| Y | Successful |
| N | Failed **(do not perform an authorisation)** |
| U | Unknown |
| A | Attempted |
|  | None |

# Test Cards

The following test cards can be used to perform test transactions on the test platform:

| Scheme | Card Number | Password | CSC | Address | Postcode |
|---|---|---|---|---|---|
| Amex | 376100000000004 | N/A | 3761 | 4 Amex Street, Southampton | SO31 6XY |
| JCB | 3561000000000005 | N/A | 356 | 5 JCB Street, Hereford | HR3 5TR |
| Maestro | 6761000000000006 | 123456 | 676 | 6 Maestro Street, Exeter | EX16 7EF |
| MasterCard | 5761000000000008 | 123456 | 576 | 8 MasterCard Street, Highbridge | TA6 4GA |
| Visa | 4761000000000001 | 123456 | 476 | 1 Visa Street, Crewe | CW4 7NT |

For specific MPI responses the following test cards can be used on the test platform:

| Card Scheme | Card Number | Cardholder Enrolled | Transaction Status |
|---|---|---|---|
| Maestro | 6761000000000006 | Y | Y |
| MasterCard | 5761000000000008 | Y | Y |
| Visa | 4761000000000001 | Y | Y |
| Maestro | 6761000001000005 | Y | N |
| MasterCard | 5761000001000007 | Y | N |
| Visa | 4761000001000000 | Y | N |
| Maestro | 6761000005000001 | Y | U |
| MasterCard | 5761000005000003 | Y | U |
| Visa | 4761000005000006 | Y | U |
| Maestro | 6761000002000004 | Y | A |
| MasterCard | 5761000002000006 | Y | A |
| Visa | 4761000002000009 | Y | A |
| Maestro | 6761000003000003 | N |  |

| | | | |
|---|---|---|---|
| MasterCard | 5761000003000005 | N | |
| Visa | 4761000003000008 | N | |
| Maestro | 6761000004000002 | U | |
| MasterCard | 5761000004000004 | U | |
| Visa | 4761000004000007 | U | |

## Acquirer BINs and Merchant ID Lengths

The following table lists the Acquirer BINs and Merchant ID Lengths for the major acquiring banks:

| Acquiring Bank | MasterCard Acquirer BIN | MasterCard Merchant ID Length | Visa Acquirer BIN | Visa Merchant ID Length |
|---|---|---|---|---|
| Allied Irish Bank (Irish Merchants) | 510213 | 11 | 474198 | 11 |
| Allied Irish Bank (UK Merchants) | 543487 | 11 | 474202 | 11 |
| Barclaycard UK | 523065 | 7 | 492900 | 15 |
| Elavon Financial Services UK | 518422 | 15 | 446365 | 15 |
| First Data Merchant Solutions UK | 520334 | 15 | 405657 | 15 |
| Global Payments UK | 550443 | 15 | 483050 | 15 |
| Lloyds TSB Cardnet UK | 540436 | 15 | 408532 | 15 |
| WorldPay UK | 542515 | 15 | 491677 | 15 |

## CreditCall Branding

The CreditCall brand is respected as being synonymous with security and reliability. You may wish to include this logo on your site:

```
<a href="http://www.creditcall.com">
         <img
                  alt="Secure Payment by CreditCall"
                  border=”0"
                  src=”http://www.creditcall.com/images/Secure_CreditCall_135px.gif”
         />
</a>
```