



GPS Real-Time Credit Card POX/XML Web Service

Version 2.0

Guardian Payment Systems

Contents

| | |
|--|---|
| Guardian Payment Systems Credit Card Processing..... | 1 |
| Process Details – Authorization/Settle versus Charge..... | 1 |
| More Process Details - Real-Time Authorization versus Batch Authorization..... | 1 |
| Technical Details | 2 |
| Real-time Credit Card Authorization..... | 3 |
| Submit an Authorization Transaction to the Web Service: Authorize(.....) | 3 |
| Credit Card Authorize Request XML | 3 |
| Authorization Header XML..... | 3 |
| Authorization Request XML | 3 |
| Authorization XML | 4 |
| Lodging XML..... | 4 |
| Authorization Response XML..... | 5 |
| Authorization Results XML..... | 5 |
| Real-Time Credit Card Charge..... | 6 |
| Charge Header XML | 6 |
| Charge Request XML..... | 6 |
| Charge XML | 6 |
| Lodging XML..... | 7 |
| Charge Response XML..... | 7 |
| Charge Results XML..... | 7 |
| Real-time Credit Card Refund | 8 |
| Submit a Refund Transaction to the Web Service: Refund(.....) | 8 |
| Refund Header XML | 8 |

Refund Request XML..... 8

Refund XML..... 9

Refund Response XML 9

Refund Results XML 9

Appendix A - Specific Test Cases..... 11

 Test Data that will pass 12

 Specific Return Values..... 13

Appendix B – PHP Credit Card Charge Example..... 14

 Payment Capture HTML Web Page..... 14

 Example PHP Page to Process a Credit Card Charge..... 14

Guardian Payment Systems Credit Card Processing

The Guardian Payment Systems Real-Time Credit Card Processing system provides a Plain Old XML (POX) Web Service for customers to be able to process individual Credit Card Transactions in “real-time” – receiving instant response/status for each transaction submitted.

This service provides the following methods:

- Credit Card Authorization
- Credit Card Charge
- Credit Card Refund

This document outlines the process that a customer needs to do to use these services. Additionally, a batch Settlement service is available. This document also outlines the process for using this service, and this service can also be consumed via SOAP messaging.

Process Details – Authorization/Settle versus Charge

If you are asking, which credit card process should I use -- Authorization/Settle or Charge? Charge is the most common form of credit card processing, and it is the preferred form for Internet acceptance. Authorization/Settle is a 2 step process. Authorization, the 1st step, can be done via either Guardian’s real-time or batch interfaces, and settle, the 2nd step, is done in batch processing.

When would you use the authorization/settle process? Here are some guidelines:

- If the services offered by you or your merchants include a review or editing of the transaction prior to a final processing you would choose Auth/Settle, or
- Another reason to use Auth/Settle is if there is a delay between the time of purchase and deliver of a product. The original auth will remain active for (3) days*. Once the auth expires the transaction can be sent as another auth/settle or a charge.

Note*: the length the authorization will stay active varies between processors, but all authorizations expire if a corresponding charge is not sent within the allotted time.

More Process Details - Real-Time Authorization versus Batch Authorization

Guardian Payment Systems provides interfaces for both one-time Authorizations and batch Authorizations. Your choice to implement one or the other methods of authorizing Credit Card transactions will be based on how your system acquires the transactions.

However, batch authorization is the preferred method, and one advantage of batch-oriented processing is that Guardian provides reporting at the batch level. Please refer to the Guardian Payment Systems Credit Card Batch spec for more details.

Technical Details

This service is coded in .Net 3.5 and is exposed as an XML Web Service. The WSDL is:

<https://testsvcs.guardianpayments.com/Processing/CreditCardXml/Auth>

<https://testsvcs.guardianpayments.com/Processing/CreditCardXml/Charge>

<https://testsvcs.guardianpayments.com/Processing/CreditCardXml/Refund>

<https://testsvcs.guardianpayments.com/Processing/CreditCardService.svc?wsdl>

Real-time Credit Card Authorization

A Credit Card Authorization places a hold on funds in the customer’s account. The funds in the customer’s account are not removed based on an authorization. An authorization requires a corresponding settlement transactions before funds are moved. Without the settlement transaction, the authorization expires and the funds held in the customer’s account are released.

If you choose to utilize the Guardian Real-Time Credit Card Authorization interface, you will also need to get the Guardian Batch Credit Card Interface spec, because credit card settlement is only available through the batch interface.

Remember that *you must store the authorization result* in order to settle the transaction at a later time.

Submit an Authorization Transaction to the Web Service: Authorize(...)

Submitting a credit card authorization through the XML Web service follows this pseudo-syntax:

```
xmlResponse = httpsPost
(
    https://testsvcs.guardianpayments.com/Processing/CreditCardXML/Create,
    xmlCreditCardAuthRequest
)
```

Credit Card Authorize Request XML

The <xmlCreditCardAuthRequest> element has the following format:

| Field Name | Type | Description |
|--------------------------------|------|---|
| Header | | Information identifying you as a merchant within Guardian’s Payment Director payment gateway. |
| creditCardAuthorizationRequest | | The credit card authorization data. |

Authorization Header XML

The header object contains information to identify you as a merchant within Guardian’s Payment Director Payment gateway. These merchant specific values are provided by Guardian when merchant underwriting is complete, and the <header> element is defined as:

| Field Name | Type | Description |
|----------------|--------|---|
| activationCode | String | Guardian assigned code identifying you as a merchant. |
| endpointToken | String | Guardian assigned unique identifier of you as a merchant. |

Authorization Request XML

The <creditCardAuthorizationRequest> element will contain the specific information on the credit card transaction and is defined as:

| Field Name | Type | Description |
|----------------|----------------|-----------------------------------|
| CreditCardAuth | CreditCardAuth | The transaction being authorized. |

Authorization XML

The Guardian <creditCardAuth> element is defined as follows:

| Field Name | Type | Description |
|------------------------------------|------------|---|
| ClientTransactionIdentifier | string(50) | Required. Your system’s reference number to identify this transaction. |
| CardNumber | String | Required. Credit Card number. Not required if using an account already stored in the Guardian Virtual Account Vault. |
| VirtualCreditCardAccountIdentifier | String | Optional. When the card number is already stored in the Guardian Vault, this value replaces the CardNumber field. |
| ExpirationDate | Date | Required. Valid Formats include any valid date, including “MM-01-YYYY”, “01-MM-YYYY”, “Month 01, Year”, etc. |
| CardholderName | String | Required. Name on card. |
| BillingAddress1 | String | Optional. |
| BillingAddress2 | String | Optional. |
| BillingPostalCode | String | Optional. |
| BillingCountry | String | Optional. |
| CardSecurityCode | string | Optional. CVV code from the back of the card Note: Industry regulations strictly prohibit retention or storage of this field. |
| Amount | Decimal | Required. |
| CashierId | String | Optional. A courtesy field provided to you to identify the source of this transaction. |
| Track | String | Optional. Track data read from the swipe of the card Note: Industry regulations strictly prohibit retention or storage of this field. |
| OriginType | Enum | Optional. Values are (Internet, Phone, Mail or POS) |
| LocationId | String | Optional. A courtesy field to identify the location this transaction originated from |
| IndustryType | Enum | Optional. Values are (Ecommerce, Retail, Moto, Lodging) |
| LodgingDetail | Lodging | Optional. |
| ClientData1 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData2 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData3 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |

Lodging XML

The <lodging> element is defined as:

| Field Name | Type | Description |
|--------------|--------|---------------------------------|
| FolioNumber | String | Optional. Folio number |
| CheckInDate | Date | Optional. Any valid date format |
| CheckOutDate | Date | Optional. Any valid date format |

Authorization Response XML

The Guardian <creditCardAuthResponse> element is defined as:

| Field Name | Type | Description |
|----------------------|----------------------|----------------------------------|
| CreditCardAuthResult | CreditCardAuthResult | The results of the authorization |

Authorization Results XML

The <creditCardAuthResult> element contains the result the transaction and is defined as:

| Field Name | Type | Description |
|-----------------------------|----------|---|
| ClientTransactionIdentifier | String | Your system's reference number to identify this transaction. |
| TransactionIdentifier | String | Guardian's transaction Identifier |
| ResponseCode | String | Response code from the Credit Card processor |
| ResponseMessage | String | Descriptive message of the response from the processor |
| TransactionDate | DateTime | The UTC time stamp of the transaction from Guardian's perspective. |
| ProcessorDate | Date | Time stamp of the transaction from the processor's perspective. |
| AVSResponseCode | String | Processor's AVS response code. |
| AVSResponseMessage | String | Processor's descriptive AVS response message. |
| CVVResponseCode | String | Processor's CVV response code. |
| CVVResponseMessage | String | Processor's descriptive CVV response message. |
| AuthorizationCode | String | The Card Processor Authorization Number; your system will store this value. It is used for settlement and tracking of the transaction. |
| Status | String | Transaction status: <ul style="list-style-type: none"> • Received: transaction has been received, waiting for processing • Invalid: Guardian marked the transaction invalid (e.g. invalid card number) • Processing: transaction is processing • Failed: transaction has completed resulting in an error • Complete: transaction processing has finished normally • Canceled: At your request, Guardian canceled the batch containing this transaction • Hold: At your request, Guardian has put the batch containing this transaction on hold |

Real-Time Credit Card Charge

A Credit Card Charge is an authorization and settlement in a single transaction. The customer’s account is immediately charged for the full amount of the transaction.

Submitting a credit card charge through the SOAP Web service follows this pseudo-syntax:

```
xmlResponse = httpsPost
(
    https://testsvcs.guardianpayments.com/Processing/CreditCardXML/Charge,
    xmlCreditCardChargeRequest
)
```

Charge Header XML

The header object contains information to identify you as a merchant within Guardian’s Payment Director Payment gateway. These merchant specific values are provided by Guardian when merchant underwriting is complete.

Charge Request XML

The <creditCardChargeRequest> element will contain the specific information on the credit card transaction and is defined as:

| Field Name | Type | Description |
|------------------|------------------|------------------|
| CreditCardCharge | CreditCardCharge | The transaction. |

Charge XML

The Guardian <creditCardCharge> element is defined as follows:

| Field Name | Type | Description |
|------------------------------------|------------|---|
| ClientTransactionIdentifier | string(50) | Required. Your system’s reference number to identify this transaction. |
| CardNumber | String | Required. Credit Card number. Not required if using an account already stored in the Guardian Virtual Account Vault. |
| VirtualCreditCardAccountIdentifier | String | Optional. When the card number is already stored in the Guardian Vault, this value replaces the CardNumber field. |
| ExpirationDate | Date | Required. Valid Formats include any valid date, including “MM-01-YYYY”, “01-MM-YYYY”, “Month 01, Year”, etc. |
| CardholderName | String | Required. Name on card. |
| BillingAddress1 | String | Optional. |
| BillingAddress2 | String | Optional. |
| BillingPostalCode | String | Optional. |
| BillingCountry | String | Optional. |
| CardSecurityCode | string | Optional. CVV code from the back of the card Note: Industry regulations strictly prohibit retention or storage of this field. |
| Amount | Decimal | Required. |
| CashierId | String | Optional. A courtesy field provided to you to identify the |

GPS Real-Time Credit Card POX/XML Web Service

| Field Name | Type | Description |
|---------------|------------|---|
| | | source of this transaction. |
| Track | String | Optional. Track data read from the swipe of the card Note: Industry regulations strictly prohibit retention or storage of this field. |
| OriginType | Enum | Optional. Values are (Internet, Phone, Mail or POS) |
| LocationId | String | Optional. A courtesy field to identify the location this transaction originated from |
| IndustryType | Enum | Optional. Values are (Ecommerce, Retail, Moto, Lodging) |
| LodgingDetail | Lodging | Optional. |
| ClientData1 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData2 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData3 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |

Lodging XML

The <lodging> element is defined as:

| Field Name | Type | Description |
|--------------|--------|---------------------------------|
| FolioNumber | String | Optional. Folio number |
| CheckInDate | Date | Optional. Any valid date format |
| CheckOutDate | Date | Optional. Any valid date format |

Charge Response XML

The Guardian <creditCardChargeResponse> element is defined as:

| Field Name | Type | Description |
|------------------------|-------------------------|----------------------------------|
| CreditCardChargeResult | CreditCardCharge Result | The results of the authorization |

Charge Results XML

The <creditCardChargeResult> element contains the result of the transaction and is defined as:

| Field Name | Type | Description |
|-----------------------------|----------|--|
| ClientTransactionIdentifier | String | Your system's reference number to identify this transaction. |
| TransactionIdentifier | String | Guardian's transaction Identifier |
| ResponseCode | String | Response code from the Credit Card processor |
| ResponseMessage | String | Descriptive message of the response from the processor |
| TransactionDate | DateTime | The UTC time stamp of the transaction from Guardian's perspective. |
| ProcessorDate | Date | Time stamp of the transaction from the processor's perspective. |
| AVSResponseCode | String | Processor's AVS response code. |

| Field Name | Type | Description |
|--------------------|--------|---|
| AVSResponseMessage | String | Processor's descriptive AVS response message. |
| CVVResponseCode | String | Processor's CVV response code. |
| CVVResponseMessage | String | Processor's descriptive CVV response message. |
| AuthorizationCode | String | The Card Processor Authorization Number; your system will store this value. It is used for settlement and tracking of the transaction. |
| Status | String | Transaction status: <ul style="list-style-type: none"> • Received: transaction has been received, waiting for processing • Invalid: Guardian marked the transaction invalid (e.g. invalid card number) • Processing: transaction is processing • Failed: transaction has completed resulting in an error • Complete: transaction processing has finished normally • Canceled: At your request, Guardian canceled the batch containing this transaction • Hold: At your request, Guardian has put the batch containing this transaction on hold |

Real-time Credit Card Refund

A Credit Card Refund is a full or partial refund against a single charge or settlement transaction. The customer's account is immediately refunded for the desired amount of the transaction. Note: you are prevented from refunding more than the "current transaction balance". For example, if the original charge was for \$100.00, you can send a single refund for up to \$100.00, or you can send several refunds as long as the running total does not exceed the \$100.00 original amount, so you could send in a refund for \$35.00 and another for \$60.00 and then finally one for \$5.00.

Submit a Refund Transaction to the Web Service: Refund(...)

Submitting a credit card Refund through the XML Web service follows this pseudo-syntax:

```
xmlResponse = httpsPost
(
    https://testsvcs.guardianpayments.com/Processing/CreditCardXML/Refund,
    xmlCreditCardRefundRequest
)
```

Refund Header XML

The header element contains information to identify you as a merchant within Guardian's Payment Director Payment gateway. These merchant specific values are provided by Guardian when merchant underwriting is complete.

Refund Request XML

The <creditCardRefundRequest> element will contain the specific information on the credit card transaction and is defined as:

| Field Name | Type | Description |
|------------|------|-------------|
|------------|------|-------------|

GPS Real-Time Credit Card POX/XML Web Service

| Field Name | Type | Description |
|------------------|------------------|------------------|
| CreditCardRefund | CreditCardRefund | The transaction. |

Refund XML

The Guardian <creditCardRefund> element is defined as follows:

| Field Name | Type | Description |
|-------------------------------|------------|--|
| ClientTransactionIdentifier | string(50) | Required. Your system's reference number to identify this transaction. |
| OriginalTransactionIdentifier | String(50) | Required. The Guardian transaction identifier you are requesting the refund for. |
| RefundAmount | Decimal | The amount of this refund. Must be less than the original transaction amount. Remember that multiple refunds can be issued against the original transaction, and the sum of all refunds must remain less than the original transaction amount. |
| ClientData1 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData2 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |
| ClientData3 | String(50) | Optional. A value from your system that will show up in Guardian Reporting. Examples include Customer Id, Donor Id, Order Description, etc. |

Refund Response XML

The Guardian <creditCardRefundResponse> element is defined as:

| Field Name | Type | Description |
|------------------------|-------------------------|---------------------------------|
| CreditCardRefundResult | CreditCardRefund Result | The results of the transaction. |

Refund Results XML

The <creditCardRefundResult> element contains the result the transaction and is defined as:

| Field Name | Type | Description |
|-------------------------------|----------|--|
| ClientTransactionIdentifier | String | Your system's reference number to identify this transaction. |
| TransactionIdentifier | String | Guardian's transaction Identifier |
| ResponseCode | String | Response code from the Credit Card processor |
| ResponseMessage | String | Descriptive message of the response from the processor |
| TransactionDate | DateTime | The UTC time stamp of the transaction from Guardian's perspective. |
| ProcessorDate | Date | Time stamp of the transaction from the processor's perspective. |
| AuthorizationCode | String | The Card Processor Authorization Number; your system will store this value. It is used for settlement and tracking of the transaction. |
| OriginalTransactionIdentifier | String | Echo of the Guardian transaction identifier for the original transaction being refunded. |

| Field Name | Type | Description |
|------------|--------|---|
| Status | String | Transaction status: <ul style="list-style-type: none">• Received: transaction has been received, waiting for processing• Invalid: Guardian marked the transaction invalid (e.g. invalid card number)• Processing: transaction is processing• Failed: transaction has completed resulting in an error• Complete: transaction processing has finished normally• Canceled: At your request, Guardian canceled the batch containing this transaction• Hold: At your request, Guardian has put the batch containing this transaction on hold |

Appendix A - Specific Test Cases

For your testing, you may wish to generate specific return codes so that you can ensure that your application handles them properly.

This can easily be accomplished on Web Service Authorization and Charge methods by manipulating the “cents” portion of the amount. The following table shows what results you can expect based on the amount field:

| Amount | RC | Message |
|--------|----|--|
| 13.00 | 0 | Approved |
| 13.01 | 1 | Duplicate Approved (Transaction previously Approved) |
| 13.02 | 2 | Partially Approved |
| 13.03 | 3 | Invalid Merchant |
| 13.04 | 4 | Declined |
| 13.05 | 5 | Do not honor |
| 13.06 | 6 | Error |
| 13.07 | 7 | Pick up card – special |
| 13.12 | 12 | Invalid Transaction |
| 13.13 | 13 | Invalid Amount |
| 13.14 | 14 | Invalid Card |
| 13.15 | 15 | Invalid issuer |
| 13.19 | 19 | Re-enter transaction |
| 13.21 | 21 | No Action Taken |
| 13.28 | 28 | File is temporarily unavailable |
| 13.33 | 33 | Expired Card |
| 13.39 | 39 | No credit account Visa ePay |
| 13.41 | 41 | Lost card |
| 13.43 | 43 | Stolen card |
| 13.51 | 51 | Insufficient Funds |
| 13.52 | 52 | No checking account |
| 13.53 | 53 | No savings account |
| 13.55 | 55 | Invalid PIN |
| 13.57 | 57 | Trans not permitted |
| 13.58 | 58 | Transaction not allowed at terminal |
| 13.59 | 59 | Restricted |
| 13.61 | 61 | Amount limit exceeded |
| 13.62 | 62 | Restricted card |
| 13.63 | 63 | Security violation |

| Amount | RC | Message |
|--------|-----|---|
| 13.65 | 65 | Activity count limit exceeded |
| 13.75 | 75 | PIN tries exceeded |
| 13.76 | 76 | Reversal: Unable to locate previous message |
| 13.77 | 77 | Previous message located for a repeat or reversal |
| 13.78 | 78 | Duplicate |
| 13.79 | 79 | Already reversed |
| 13.80 | 80 | Invalid date |
| 13.81 | 81 | PIN crypto error |
| 13.82 | 82 | Incorrect CVV |
| 13.83 | 83 | Unable to verify PIN |
| 13.85 | 85 | No reason to decline a request ... |
| 13.91 | 91 | Try Again- Communications Error |
| 13.92 | 92 | Communications Failure |
| 13.93 | 93 | Law violation |
| 13.94 | 94 | Duplicate transaction |
| 13.96 | 96 | System error |
| 13.99 | 199 | An internal exception has occurred. |

Additionally, if you wish to test how you handle CVV and AVS responses, for any amount other than 13.00 – 13.99 if you pass in the first digit of the cents as an odd digit the test server will return a failure for the CVV code. If you pass in the second digit of the cents as an odd digit, the AVS will send back a failure code. See the table below.

| Amount | CVV | AVS |
|--------|---------|---------|
| 1.00 | Success | Success |
| 1.01 | Success | Fail |
| 1.10 | Fail | Success |
| 1.11 | Fail | Fail |

Test Data that will pass

The following test data will pass the various tests:

CardNumber 4000300020001000
 CardHolderName Mr John Smith
 BillingAddress1 3361 Boyington Dr Suite 180
 BillingPostalCode 75006
 CardSecurityCode 123
 ExpirationDate Any valid future date

Specific Return Values

The following values may be returned for AVS and CVV checks.

The AVS Response Codes vary based on the Credit Card Provider. The following table shows what is returned:

| Description | Visa | Master Card | AMEX | Discover | Diners Club |
|---|------|-------------|------|----------|-------------|
| Address matches, Postal Code does not | A | A | A | Y | A |
| Neither Address nor Postal Code matches | N | N | N | N | N |
| Address Could not be Verified | U | U | U | W | U |
| Address and Postal Code match | X,Y | X,Y | Y | X,A | X,Y |
| Postal Code Matches, Address does not | W,Z | W,Z | Z | T,Z | W,Z |
| System Problem – could not verify | R | R | R | U | R |

The CVV Response Codes that you may get back include the following:

| CVV Code | Description |
|----------|--|
| M | CVV Code matches the account number |
| N | CVV Code does not match the account number |
| P | CVV Code could not be verified |
| U | Card issuer does not support CVV Code Checking |

Appendix B – PHP Credit Card Charge Example

This appendix demonstrates a Credit Card Charge from a PHP Web page.

Payment Capture HTML Web Page

This is a minimal example of an HTML form capturing payment information.

```
<html>
<head><title>Guardian PHP Test page</title></head>
<body>
  <h4>Payment Form</h4>
  <form action="process.php" method="post">
    Name on Card: <input name="nameOnCard" type="text" length="25" value="" /><br />
    Card Number: <input name="cardNumber" type="text" Maxlength="16" value="" /><br />
    Expiration (yyyy-mm): <input name="expiration" type="text" length="7" value="" /><br />
    Zip Code: <input name="zipcode" type="text" length="10" value="" /><br />
    Amount: <input name="tranAmount" type="text" length="10" /><br />
    <input type="submit" value="Pay Now" />
  </form>
</body>
</html>
```

Example PHP Page to Process a Credit Card Charge

This page is a minimal example demonstrating sending a Credit Card Charge from PHP on Microsoft Internet Information Server (IIS).

```
<html>
<head><title>Process Donation</title></head>
<body><h1>results</h1>
<?php
function httpsPost($Url, $strRequest)
{
  // this function performs the HTTPS Post to the Guardian Payment Director gateway

  // Initialisation
  $ch=curl_init();

  // Set parameters
  curl_setopt($ch, CURLOPT_URL, $Url);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // Return a variable instead of posting it directly
  curl_setopt($ch, CURLOPT_POST, 1); // Active the POST method

  curl_setopt($ch, CURLOPT_POSTFIELDS, $strRequest);
  curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
  curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
  curl_setopt($ch, CURLOPT_VERBOSE, 1);

  $xmlLength = strlen($strRequest);
  curl_setopt($ch, CURLOPT_HTTPHEADER, array('Content-Length: '.$xmlLength));
```

```
curl_setopt($ch, CURLOPT_HTTPHEADER, Array('Content-Type: text/xml'));

// Execute the HTTPS Post
$result = curl_exec($ch);

echo "<p>errno=".curl_errno($ch)."<br />HttpCode=".curl_getinfo($ch, CURLINFO_HTTP_CODE)."<br
/>error=".curl_error($ch)."</p>";
echo "<p>HttpHdr=".curl_getinfo($ch, CURLINFO_HEADER_OUT)."</p>";

// Close
curl_close($ch);
return $result;
}

// get the credit card payment data from the HTML form's post
$nameOnCard = $_POST['nameOnCard'];
$cardNumber = $_POST['cardNumber'];
$expiration = $_POST['expiration'];
$zipcode = $_POST['zipcode'];
$tranAmount = $_POST['tranAmount'];
$xmlTemplate =
'<creditCardChargeRequestMessage><header><endpointToken></endpointToken><activationCode>
</activationCode></header><creditCardChargeRequest><creditCardCharge><clientTransactionIdentifier></clie
ntTransactionIdentifier><cardNumber>'. $cardNumber. '</cardNumber><virtualCreditCardAccountIdentifier
/><expirationDate>'. $expiration. '</expirationDate><cardholderName>'. $nameOnCard. '</cardholderName><billi
ngAddress1 /><billingAddress2 /><billingPostalCode>'. $zipcode. '</billingPostalCode><billingCountry
/><amount>'. $tranAmount. '</amount></creditCardCharge></creditCardChargeRequest></creditCardChargeRe
questMessage>';

echo "<p>Input = ($tranAmount)($nameOnCard)($cardNumber)($expiration)($zipcode) </p>";

$xmlPacket = utf8_encode($xmlTemplate);

// call the function to send the payment to Guardian Payment Director
$response = httpsPost("https://devsvcs.guardianpayments.com/processing/creditcardxml.svc/Charge",
    $xmlPacket);

// print out the payment response
echo "<p>Ret = $response </p>";

echo "<p>End.</p>";

?>

</body>
</html>
```