Getting Started with Online Payments

Getting Started

To get started with online payments, please complete and submit this form to the Merchant Card Services Office: http://www.obfs.uillinois.edu/forms/merchantforms.shtml

Steps for the Online Payment Process

There are six steps to the Online Payment Process.

Step 1 – Customer Visits Web Site

The customer visits the merchant's web site to make a payment. The web site must interact with the customer to display a grand total amount to pay. Once completed, the grand total amount will be sent to the Payment Center for processing.

The UI Payment Center accepts credit card payments and generates reconciliation data, which is fed into the Banner General Ledger or UFAS on a daily basis. Using the Payment Center increases the accuracy of the reconciliation process while simplifying the payment process for participating units.

Step 2 – Redirected to Payment Center

The customer will be redirected to the Payment Center to begin the payment process. At this point, the web form will display where the customer will enter their credit card information (refer to screen shot on page 6). After entering the card information, the payment will be authorized in real-time through the use of a payment gateway.

If the authorization was successful, the customer will be redirected back to the originating unit web site. The method of this return redirection is configurable.

If the authorization failed, the customer may make another authorization attempt.

- After X failures, the payment will be considered failed and no more attempts will be allowed.
- Allowing only X attempts decreases the chance of a criminal randomly attempting card numbers for access to data.

Step 3 – Status Determined

Once back at the unit web site, the status of the authorization must be determined. To determine the status, the unit web site will send a payment status query message to the Payment Center. The status of the authorization will be either success or failure. Up to this point, the customer's credit card has **not** been charged. The card number, expiration date, and the ability to hold the charge amount have been checked but the charge has not been put on their credit card statement. **If the status was a failure**, the unit web site will decide how to proceed. One approach is to ask the customer to verify their credit card information and try again.

Step 4 – Capture Request

If the status was a success, the unit web site will send a message to the Payment Center for a capture request. A capture request will inform the Payment Center the payment should be finalized and the charge should be placed on the customer's credit card statement. In the capture request message, the unit web site will also send reconciliation accounts and amounts that should be used to reconcile the payment.

Step 5 – Payment Receipt

When the payment has been finalized, the unit web site will present the customer with a payment receipt and proceed final processing procedures of unit website for transaction completion.

Step 6 – Payment Processed

All captured transactions and corresponding reconciliation information are processed by the Payment Center Monday through Friday. The reconciliation information will be used to generate feeds to the proper General Ledger (GL) system after the business day ends. Any transactions processed on the weekend are handled on Monday.

Following is how the business day is broken down:

Period 1:	Monday 9 PM – Tuesday 9 PM
Period 2:	Tuesday 9 PM – Wednesday 9 PM
Period 3:	Wednesday 9 PM – Thursday 9 PM
Period 4:	Thursday 9 PM – Friday 9 PM
Period 5:	Friday 9 PM – Monday 9 PM

Cost / Fees

The only cost associated with using online payments is called the "discount." The discount is a processing fee charged to each payment by the credit card processors covering the cost of processing transactions. This fee varies between 2% and 2.5% of the transaction amount. The University of Illinois cannot absorb this fee; therefore the units will be responsible for paying the fee. Keep this in mind when setting prices of the goods or services sold in the unit. University Accounting will collect the discount fees on a monthly basis by deducting the funds from reconciliation accounts credited by the online payment process.

Unit Web Site Modifications

To accept online payments, modifications must be made to the unit's web site. These modifications are necessary to ensure that accurate tracking of payments.

Transaction Database

The web site must have a database back-end. This database will hold payment transaction information. There is no restriction as to what kind of database should be used.

At a minimum, the database should track for each payment transaction and include:

1. Reference ID
2. Transaction ID
3. Token
4. Payment Amount
5. Reconciliation Account(s) and Amount(s)
6. Payment Status
7. Payment Date

Return URL

The web site must have a web page established for the Payment Center to send customers information after they have finished their authorization. This page will complete a variety of functions and output customized HTML; therefore, this page will need to be scripted. Popular script engines include Active Server Pages (ASP), ColdFusion, PHP, and Perl.

Sending and Receiving Messages To and From the Payment Center

Please refer to the document ***"Departmental Payment Message Specifications"*** for information regarding sending and receiving messages to and from the Payment Center.

Customization for the Online Payment Process

There are several areas of the Payment Center that may be customized to a particular web site. Some customizations are required and some are optional.

Required Customization

Return Mode

The Return Mode will define how the customer will return to the originating unit web site. Return Modes include standard hyperlink, standard form post, and automatic redirect.

Standard Hyperlink

This return method may be completed by creating a simple hyperlink of the return URL with the transaction token included in the querystring.

Here is an example:

- https://www.somesite.uillinois.edu/finish.cgi?token-abcd1234

Standard Form Post

Similar to the Standard Hyperlink, a form post may be created.

Here are examples:

- <form method="post" action=https://www.somesite.uillinois.edu/finish.cgi>
- <input type="hidden" name="token" value="abcd1234">
- <input type="submit" name="return" value="Return"> </form>

Automatic Redirect

This return method will send the user back to the originating web site via the return URL without requiring the user to press a button or click a hyperlink. Once a successful authorization has been made, or the maximum payment attempts have been reached, the user will automatically be redirected to the return URL. The token will be passed in the querystring. This is the preferred method of returning customers to unit web sites.

Return URL

This specifies the URL that customers will be sent to after a payment has been authorized. The URL must be able to process information and generate HTML; therefore, it should be a script.

AVS Enforcement

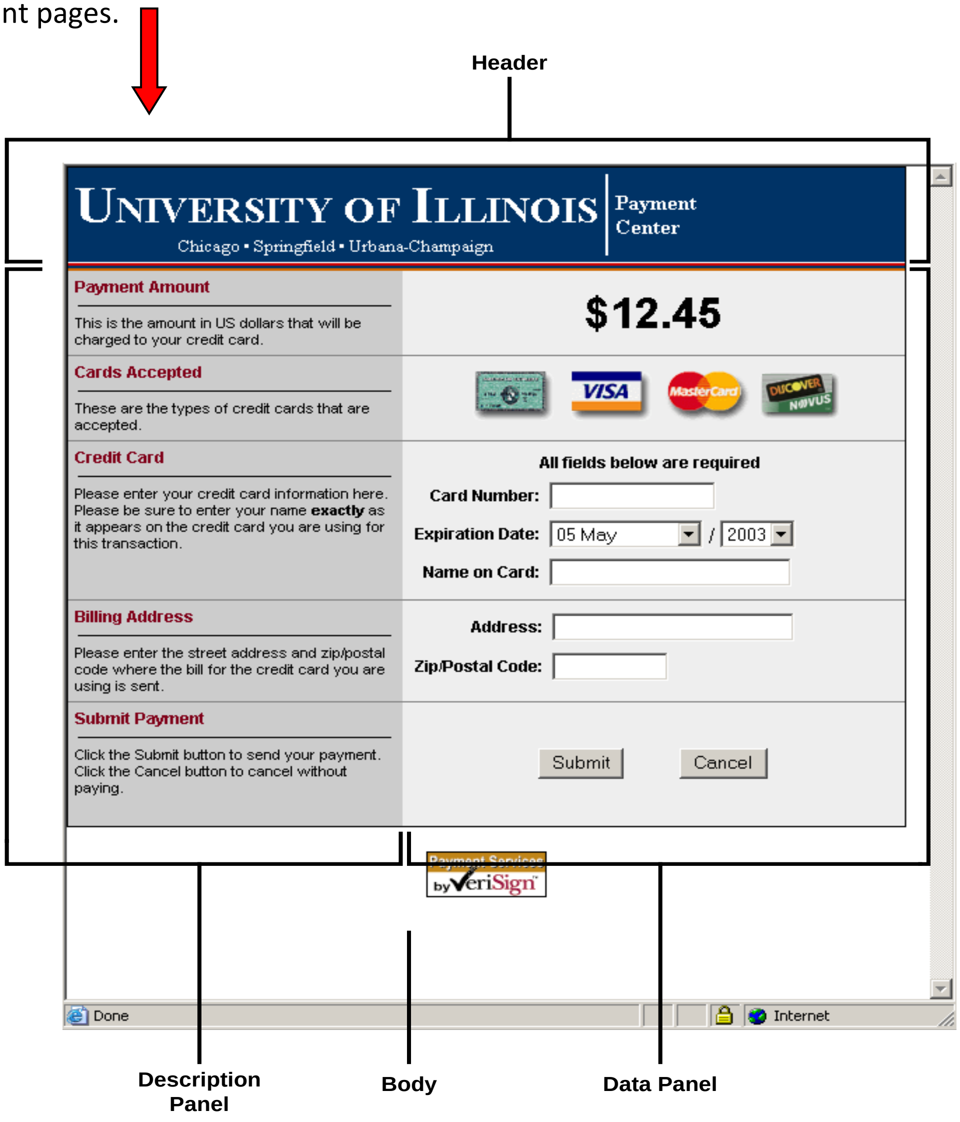
This option determines if an AVS mismatch resulted in a failed payment authorization. If AVS enforcement is turned on and a failure result code is returned, the authorization will be treated as a failure. A successful AVS match or an AVS unavailable code will not affect the result of the authorization.

Card Types

Normally all 4 card types (American Express, Discover, MasterCard, and Visa) will be accepted. If one or more of the cards cannot be accepted, this option will allow one or more card types to be restricted.

Optional Customization

Currently, the only optional customization is the ability to change the look and feel of the payment pages.



Payment Amount

This is the amount in US dollars that will be charged to your credit card.

$12.45

Cards Accepted

These are the types of credit cards that are accepted.

Credit Card

Please enter your credit card information here. Please be sure to enter your name **exactly** as it appears on the credit card you are using for this transaction.

All fields below are required

Card Number:

Expiration Date: 05 May / 2003

Name on Card:

Billing Address

Please enter the street address and zip/postal code where the bill for the credit card you are using is sent.

Address:

Zip/Postal Code:

Submit Payment

Click the Submit button to send your payment. Click the Cancel button to cancel without paying.

The element attributes that may be modified include:

- Header Background Color
- Header Font
- Header Text Color
- Description Panel Background Color
- Description Panel Font
- Description Panel Header Color
- Description Panel Text Color
- Data Panel Background Color
- Data Panel Font
- Data Panel Text Color
- Body Background Color
- Body Font
- Body Text Color

Terminology

Address Verification Service (AVS)

A system used to verify the identity of the person claiming to own the credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company.

Authorization

The verification of a bankcard transaction by a bankcard-issuing bank, other institution, or approved independent service provider. Authorization is initiated by accessing (by voice or electronic terminal) a Global Payments designated authorization center(s). Authorization is based on the cardholder account status and available credit.

Capture

The second part of the credit card transaction. This function puts the charge on the cardholder's account and deposits the funds in the UI bank account. The capture amount can be for less than the authorization amount, but never for a higher amount than the authorization.

Reference ID

A 50 alphanumeric unique identifier assigned to each payment transaction by the unit web site. The algorithm must never generate the same Reference ID for two separate payments.

Return URL

After a payment has been completed, customers are directed to the web site URL, which has been specified by the unit/department.

Site ID

A simple integer unique identifier associated with the web site requesting the processing of an online payment. A Site ID is a logical boundary for grouping transactions.

Transaction ID

A 13 alphanumeric unique identifier assigned to each payment transaction. The Transaction ID is returned as a QueryCCPayment message.

Token

A 48 alphanumeric unique identifier assigned to each payment transaction. The Token is returned as a RegisterCCPayment message.

Note: ***For additional terminology, please refer to the Glossary section of the Merchant Card Services web site.***

http://webtest.obfs.uillinois.edu/obfs/merchants/glossary.shtml

Test Numbers

Test Credit Card Numbers

For testing purposes, the following card numbers may be used for testing transactions. All expiration dates will be valid.

Visa	4111111111111111
Visa	4012888888881881
Visa	4222222222222
MasterCard	5555555555554444
MasterCard	5105105105105100
American Express	378282246310005
American Express	371449635398431
Discover	6011111111111117
Discover	6011000990139424

Test Card Verification Numbers

A card verification code is the 3 digit code located on the back of the Visa, MasterCard, and Discover card or the 4 digit code located on the front of the American Express card. The numbers below will allow you to test this service with a valid card number and expiration date.

001 – 300	Produces a CVN match (success)
301 – 600	Produces a CVN mismatch (failure)
601 – higher	Produces a CVN match (success)

Technical Implementation Tips

1. One technique for beginning the payment process is to create a form. Set the action of the form to a script, and title the submit button ***"Begin Payment."*** In the script send the **RegisterCCPayment message**, create the payment record in the database, and redirect the user to the Payment Center server.

2. When sending test transactions, any charge amount over $1,000.00 will result in a declined payment. This **only** occurs with **test** transactions.

3. When the return URL is invoked, the token will be sent in the querystring. ***For example:*** https://www.someunit.uillinois.edu/return.cgi?token=abcd1234efghi

4. Successful authorizations cannot be captured more than once. A second capture request sent after a successful capture request will return an error.

5. Remember that the web is stateless. It cannot be a guarantee that a customer will only have one browser window open or that they will only click a button once. Design the site so that even if multiple browser windows are opened, a successful payment will be processed only once.

6. It is a good practice to create a new reference id and register that payment each time a payment request is made. For example, while processing registrations for a conference each customer creates a logon and password for their registration data. The conference payment is just one step in the registration process; all steps might not be completed in one session. Each time the customer initiates the payment process, create a new reference id and register it. Once they make a successful payment, stop allowing them to initiate a payment.

Why do this?
The first time a new customer (new reference id) hits the payment server, a session key is created and stored with the payment data and a session cookie. With each subsequent page request on the payment server, the session key stored in the cookie and the key stored with the payment data are compared. If they do not match, the payment is stopped. If the customer were to quit their browser session and then come back at a later time, the correct session key stored in the session cookie would not be available. That would cause the customer to receive an error and they would not be able to make the payment.

By creating a new reference id each time a payment is initiated, the customer would get a new session key and they would be able to complete the payment. Session key enforcement prevents an intruder from hijacking another customer's payment just by guessing the payment token. If the unit's system absolutely cannot handle creating multiple reference id's for a payment, this session key enforcement can be turned off.

Frequently Asked Questions

Q: **Why are both a Transaction ID and Token used?**
A: *Although both are unique, a Transaction ID is much easier to manage by humans. A 48 character token is hard to read over the phone, type, etc. On the other hand, a Transaction ID has a pattern and can be guessed. To prevent a payment from being hijacked, it is necessary to use a unique identifier that would be hard to guess, hence the 48 character token.*

Q: **How are refunds handled?**
A: *Refunds are generally infrequent so they are handled by sending an e-mail to paycenterhelp@uillinois.edu. In the e-mail, please include the Transaction ID and the reconciliation account(s) and amount(s) to be refunded. Credit Card transactions should be refunded to the original credit card. No Credit Card Refund should be given in the form of Cash, Check, Wire Transfer, or to another credit card number.*

Q: **What is considered a business day?**
A: *A business day generally runs from 9 PM to 9 PM (24 hours). The weekend is lumped into Monday's activity.* ***The chart below illustrates how the business day is broken down:***

Period 1:	*Monday 9 PM – Tuesday 9 PM*
Period 2:	*Tuesday 9 PM – Wednesday 9 PM*
Period 3:	*Wednesday 9 PM – Thursday 9 PM*
Period 4:	*Thursday 9 PM – Friday 9 PM*
Period 5:	*Friday 9 PM – Monday 9 PM*

Feeders to the Banner General Ledger (GL) are created Monday – Friday after the business day ends.

Contact Information

Please contact Merchant Card Services for additional assistance.

Merchant Card Services
University of Illinois
Office of Treasury Operations
Merchant Card Services
254Henry Administration Building, MC-363
506 South Wright Street
Urbana, Illinois 61801
Phone: (217) 244-9384
E-mail: merchantcardhelp@uillinois.edu