OPERATING GUIDE FOR RETAIL MERCHANTS USING CHASE MERCHANT SERVICES, L.L.C.
Welcome to UCLA credit card processing through Chase Merchant Services, L.L.C. You are a valued customer and CMS would like to thank you for the opportunity to service Your needs.

This Operating Guide, as updated from time to time, will provide You with Your specific obligations on Card processing procedures as referenced in Your Bankcard Agreement. Please read this Operating Guide thoroughly and keep it within easy reach for quick reference in handling all aspects of Transaction processing.

Fraud prevention is an important section in this Operating Guide and should be read by any Merchant involved in the Transaction process.

All information and features contained herein are subject to change without notice.

Throughout the remaining Merchant Operating Guide, Chase Merchant Services, L.L.C. will be referred to as “CMS”.

For additional information regarding Retrieval Requests and the Chargeback process, please refer to the Chargeback Protection Services manual.
1 CUSTOMER SUPPORT CONTACT INFORMATION

<table>
<thead>
<tr>
<th>OVERNIGHT</th>
<th>U.S. MAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHASE MERCHANT SERVICES</td>
<td>CHASE MERCHANT SERVICES</td>
</tr>
<tr>
<td>Mail Stop 84</td>
<td>Mail Stop 84</td>
</tr>
<tr>
<td>3975 NW 120th Avenue</td>
<td>P.O. Box 5564</td>
</tr>
<tr>
<td>Coral Springs, Florida 33065</td>
<td>Coral Springs, Florida 33310</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHONE NUMBER</th>
<th>FAX NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-326-7991</td>
<td>954-846-1506 or 954-846-1504</td>
</tr>
</tbody>
</table>

Please note: Your Retrieval Request and Chargeback responses and correspondence are to be sent to a different address and fax number than the Customer Support address and fax number shown above.

Please refer to the “STORAGE & RETRIEVAL” and “CHARGEBACK” section of this Operating Guide for the address and fax number to send Your Retrieval Request and Chargeback responses and correspondence.
2 AUTHORIZATION

2.1 General Authorization Information

Authorization is the means by which a CMS Merchant attempts to obtain Approval for a Card Sale. All Sales must receive an Approval Code before the Transaction is submitted to Interchange for payment.

An Authorization request can be relayed to CMS electronically through a dial Terminal, electronic cash register, online transmission, pc batch, batch, or by placing a call to our Voice Authorization Center using the Q*Net Authorization System.

2.2 Regardless of the method of Authorization, the possible responses and their meanings will be one of the following:

2.2.1 Approval
The Sale is authorized and an Approval Code is given. This Authorization does not constitute a guarantee of payment. Each Merchant type has a specific set of additional responsibilities that must be met when completing a Sale. These responsibilities are independent of the Authorization process and failure to meet these responsibilities may result in a Chargeback or higher Interchange rates.

2.2.2 Decline
The Issuer is not authorizing the Sale and another means of payment must be requested from the Cardholder. Additional information is not given to the Merchant. Please do not give the Cardholder the phone number to CMS. The Cardholder will need to contact their Issuer to remedy the situation.

2.2.3 Decline/Pick-up
The Issuer is declining the Sale and is requesting that You hold the Card and return it to the Issuer for a possible reward. As in the case with a Decline, additional information is not given to the Merchant. Please do not give the Cardholder the phone number to CMS. The Cardholder will need to contact their Issuer directly to remedy the situation. If the Cardholder is irate or poses a threat, please do not attempt to retain the Card however the Cardholder must be advised that another means of payment is required.

2.2.4 Referral
The Issuer requires additional information before making an Authorization decision. Referrals must be handled by calling the Voice Authorization Center. Working with You, CMS will contact the Issuer via telephone or telex (international) and supply the requested information. The Issuer will then make a credit decision. For all Face-to-Face Authorizations approved via the Voice Authorization Center, a clear and legible Imprint of the Card must be obtained on the Sales Receipt that will be signed by the Cardholder.

Note: Transactions where Cards other than Visa and MasterCard are used must be Authorized electronically. In the event of an electronic malfunction, You must call the other Card companies directly. However, if CMS is Your Acquirer for JCB and/or Diners/Carte Blanche Card Transactions, please contact our Voice Authorization Center directly for assistance.
2.3 Q*Net Authorizations

Q*Net is one of the most advanced touch-tone Authorization systems currently available. It provides a quick and easy Authorization response. Q*Net responds to the tones emitted from a touch-tone telephone. If You have a rotary telephone Q*Net will prompt You to hold for a representative.

2.4 Some Features of Q*Net

- Multilingual capacity for English, French, and Spanish
- Multiple Transactions can be handled during a single call
- Message repeat for Approval Code or dollar amount

2.5 When do You need to use Q*Net?

You must call Q*Net for Visa® & MasterCard® Authorizations under the following circumstances:

- When the response received through Your Electronic Device is a “Referral.”
- Your Electronic Device prompts: “call center.”
- When there is suspected or possible fraudulent use of a Card, usually in a Face-to-Face environment. Refer to “Code 10” procedures.
- Your Electronic Device is not operational.

2.6 How to access Q*Net

To access the Q*Net System, use the following steps:

1. Dial the primary toll free number printed on the Authorization Decal provided by CMS. If You are unable to reach Q*Net through Your primary number, dial the emergency backup number listed on Your Authorization decal.

2. Enter the order:
   Sales amount (including cents-no decimals)
   Press [*]
   Enter Your Merchant Number (listed on the Authorization decal)
   Press [*]
   Example: You have a Sale of $289.87 and Your Merchant Number is 12345. **You would enter 28987*12345**.

3. If the Cardholder Account Number and Expiration Date are required, Q*Net will request this information. Q*Net will then provide the appropriate Authorization response.

   To cancel an incorrect entry, press [#]. Q*Net will then ask You to enter the correct information.

**Note:** When using Q*Net, each piece of information must be followed with the [*] character located on the lower left of Your touch-tone telephone keypad.
2.7 Authorization for T&E Card Types

For Card types other than Visa and MasterCard, You must call the appropriate company for Authorization requests:

- **American Express®** 1-800-528-2121
- **Discover®** 1-800-347-1111
- **Diners®/Carte Blanche®** 1-800-525-9040
- **JCB®** 1-800-228-1122

**Note:** If CMS is the Acquirer for Your JCB® or Diners®/Carte Blanche® Card Transactions (i.e. CMS funds You directly versus receiving funding by JCB® or Diners®/Carte Blanche®), You must use the Q*Net System and call the telephone number noted on Your Q*Net decal.

2.8 Authorization Tips

- Do not attempt to split the total value of the Sale in hopes of receiving Authorization for the Transaction. **This is against Visa and MasterCard Rules and Regulations and could result in a Chargeback.**
- If Your Electronic Device receives a Decline response, do not call for Voice Authorization. Ask the Cardholder for another form of payment.
- Always refer the Cardholder to their Issuer for inquiries.
- When obtaining a Voice Authorization or when the Card is Manually Key Entered for all Face-to-Face Card Sales, a clear and legible Imprint of the Card must be obtained on the Sales Receipt that will be signed for by the Cardholder.

**IMPORTANT:** If a Card is Approved via Voice Authorization, You must then Manually Key Enter the Card Sale using Your Electronic Device. This must be completed in order to include the Sale in Your Batch Settlement file.

2.9 Code 10 Procedures

Whenever a suspicious Transaction is encountered, a call must be placed to Q*Net and option 5 (Code 10 or supervisory assistance) must be selected. This will allow further verification before completing the Transaction.

Suspicious situations may include, but are not limited to:

- Different signature or altered signature panel – The signature on the Sales Receipt clearly does not match the signature on the back of the Card. You can see the word “void” on the signature panel or it appears to be altered.
- Incorrect or Missing 4-Digit Number – The small four digit number printed on the Card above the Cardholder Account Number is missing or does not match the first four numbers of the raised Cardholder Account Number.
- You may have suspicions regarding the Cardholder or the Card (e.g., they are purchasing large quantities of the same item; they appear to be anxious, etc.)
• If the Card is not present, the caller may be unable to answer Your questions, willing to take merchandise of any size, unable to give You the name of the Issuer, etc.

2.10 What must be done if suspicious activity is suspected?

• Call Q*Net by dialing the number listed on Your Authorization Decal. The Voice Authorization Center is open 24 hours, seven days a week. When calling Q*Net, press [5] to speak to a supervisor.

• Inform the supervisor that You may have a “Code 10.” The supervisor will ask questions requiring only a “yes” or “no” response. If the Cardholder is present, do not say or do anything to upset or embarrass the Cardholder.

• You will receive further instructions to proceed with the Transaction or retain the Card. If an Approval code is given, record the Approval Code number on the Sales Receipt that will be signed for by the Cardholder. **BE SURE TO OBTAIN A CLEAR AND LEGIBLE IMPRINT OF THE CARD FOR ALL FACE-TO-FACE TRANSACTIONS AUTHORIZED VIA VOICE AUTHORIZATION.**

• If retaining the Card, do so with caution. DO NOT use physical force, nor place Yourself in jeopardy, while attempting to retain the Card.

• Under no circumstances should Your employee attempt to recover a Card if doing so will, in any way, endanger their safety (e.g. the Cardholder is hostile, belligerent, or potentially violent).

2.11 Reward Procedures

Your employee may be entitled to a reward for the recovery of a Visa® or MasterCard® Card if the employee was instructed to Pick Up the Card when they called Q*Net and initiated a Code 10. By completing the Card Recovery Form *(shown on page 8)* and returning the recovered Card, a reward may be provided by Visa or MasterCard.

**Note:** IT IS IMPORTANT TO COMPLETE THE ENTIRE FORM, INCLUDE THE RECOVERED VISA OR MASTERCARD AND RETURN WITHIN 24 HOURS OF RECOVERY.

**MAIL TO:**

<table>
<thead>
<tr>
<th>MERCHANT SERVICES</th>
<th>MERCHANT SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTN: South Rewards</td>
<td>ATTN: North Rewards</td>
</tr>
<tr>
<td>PO Box 5019</td>
<td>PO Box 5019</td>
</tr>
<tr>
<td>Hagerstown, MD 21740</td>
<td>Hagerstown, MD 21741</td>
</tr>
</tbody>
</table>

Please Note: If Your Merchant account is serviced on the South Platform, You must mail to the “South” Rewards Dept. If Your Merchant account is serviced on the North Platform, You must mail to the “North” Rewards Dept. If You are unsure, please contact Your Customer Support Associate.
CARD RECOVERY FORM
(Please Print All Information)

PICK-UP INFORMATION

PICK-UP DATE: _______________________________________________
CARD #: _____________________________________________
CARDHOLDERS NAME: _______________________________________ 
EXPIRATION DATE: __________________________________________

MERCHANT INFORMATION

MERCHANT NAME: ___________________________________________
MERCHANT #: _______________________________________________
PHONE # ( )________________________________________________
ADDRESS: ___________________________________________________
___________________________________________________
___________________________________________________

NAME OF PERSON RECOVERING CARD:

_____________________________________________________________
SOCIAL SECURITY #: _________________________________________

CHECK REASON FOR RECOVERING CARD:

_________ Found or left at place of business
___________ Authorization requested pick up
___________ Clerk Suspicious
___________ Code 10 – Operator # ________
___________ Other (please explain):
___________________________________________________
___________________________________________________

Tape Cut Card Here
Note: Card must be cut lengthwise and do not damage the
Magnetic Stripe or the Cardholder Account Number.

Please note: Make a copy of this form for your records.
2.12 Emergency Broadcast Facility

In the unlikely event of multiple network outages, CMS understands that it is critical to provide You with a facility through which CMS can ultimately facilitate Authorizations.

The Emergency Broadcast Facility is designed to enable You to continue accepting Visa and MasterCard Transactions until service is restored.

The toll-free number for Chase Merchant Services, L.L.C. Emergency Broadcast Facility is:

800-828-7794

IMPORTANT: For all Face-to-Face Sales approved via Voice Authorization, a clear and legible Imprint of the entire Card must be obtained on the Sales Receipt that will be signed by the Cardholder.

2.13 Address Verification Services (AVS)

Address Verification Service (AVS) allows retail Merchants to validate a Cardholder’s billing address through an online system when the Card is present, but the Merchant is unable to swipe the Card.

AVS compares the billing address given to the Merchant by the Cardholder with that of the Issuer's Cardholder billing address file. The result of the comparison is then returned to the Merchant in the form of a “result code.” The result code will normally appear on the Sales Receipt.

AVS is designed to help reduce unauthorized purchaser Chargebacks, fraud-related losses, and processing costs. AVS provides additional information that the Merchant can take into consideration when making a decision on whether or not to continue with the Sale.

An AVS request can be processed in a real time mode or in a Batch Authorization mode.

Please note: AVS is NOT a substitute for Authorization. The AVS inquiry should be initiated at the same time the Authorization request is made.
AVS is processed in numeric form. This means street addresses that are written alphabetically should be converted to numbers.

Visa and MasterCard Examples:

<table>
<thead>
<tr>
<th>STREET ADDRESS</th>
<th>CONVERTED STREET ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 Walnut Street #23</td>
<td>22</td>
</tr>
<tr>
<td>One Elm Street</td>
<td>1</td>
</tr>
<tr>
<td>123 First Street</td>
<td>123</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ZIP CODE</th>
<th>CONVERTED ZIP CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>91234</td>
<td>91234</td>
</tr>
<tr>
<td>91234-0615</td>
<td>912340615</td>
</tr>
</tbody>
</table>

Some of the appropriate “result code” responses are as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Yes</td>
<td>Address and Zip 5 or 9 digit match</td>
</tr>
<tr>
<td>A</td>
<td>Address</td>
<td>Address matches, Zip does not</td>
</tr>
<tr>
<td>Z</td>
<td>Zip Match</td>
<td>Zip code of either 5 or 9 digit matches: Address does not</td>
</tr>
<tr>
<td>W</td>
<td>Whole Zip</td>
<td>9 digit Zip matches, address does not match</td>
</tr>
<tr>
<td>N</td>
<td>No Match</td>
<td>Address and Zip do not match</td>
</tr>
<tr>
<td>R</td>
<td>Retry</td>
<td>Issuer Authorization system is unavailable, try again later.</td>
</tr>
<tr>
<td>U</td>
<td>Unavailable</td>
<td>Unable to perform Address Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Either because address information is unavailable or Issuer does not support AVS.</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Transaction ineligible</td>
</tr>
<tr>
<td>S</td>
<td></td>
<td>Services not supported. AVS not supported at this time.</td>
</tr>
</tbody>
</table>
3 ACCEPTANCE & PRESENTMENT

3.1 Some Basic Card Acceptance Requirements

- A Merchant must not require a Cardholder to pay a Surcharge specifically because a Card is being used for payment of goods or services.

- Disclosures of Your return policies must be printed on the Transaction Receipt within close proximity of the Cardholder signature area. In accordance with MasterCard® and Visa® operating regulations, Disclosures are not a defense against all Cardholder disputes.

The Disclosures and a description of each include:

- **“No Refund”** – Merchant that does not accept merchandise in return or exchange or issue a Refund to a Cardholder

- **“Exchange Only”** – Merchant that only accepts merchandise in exchange for similar merchandise of price equal to the original Transaction amount.

- **“In-Store Credit Only”** – Merchant that only accepts returned merchandise and delivers an in-store Credit that equals the value of the returned merchandise and must be used at the Merchant’s place of business.

- Under no circumstances may You, as a retail establishment, issue cash or check to a Cardholder in exchange for a Card Transaction nor can You impose a minimum or maximum Transaction amount.

- A Merchant must not require a Cardholder, as a condition for honoring a Card, to sign a statement that waives the Cardholder’s right to dispute the Transaction with the Issuer.

- A Merchant must not re-charge a Cardholder for a previously charged back Transaction. You may pursue payment from the Cardholder outside of the Visa / MasterCard system.

- A Merchant must not charge a Cardholder for a Transaction that represents collection of a dishonored check.
3.2 Presentment Requirements when the Card is Present

3.2.1 STEP ONE: Cardholder presents the Card.

• Check the “Valid From” Date and the “Expiration” Date.

  The Card can only be accepted if the presentation date is ON or AFTER the Valid From Date and the presentation date is ON or BEFORE the Expiration Date.

  *For example*: Valid From is 06/2004
  Expiration is 06/2009

  A Transaction cannot be accepted before 06/01/04 or after 06/30/09.

• Ensure that the signature panel on the reverse side of the Card has been signed. Visa® and MasterCard® consider a signature panel with the words “See I.D.” or equivalent language to be blank or unsigned.

  If unsigned, You must do all of the following:

  ✓ Review positive identification to determine that the user is the Cardholder. Such identification must consist of a current, official government identification (such as a passport or drivers license) that bears the Cardholder’s signature.
  ✓ Indicate such positive identification (including any serial number and Expiration Date) on the Sales Receipt.
  ✓ You must also have the Cardholder sign the back of the Card and compare the signature to the identification. *For Your protection, unsigned Cards must not be accepted.*

• Ensure that a Magnetic Stripe is on the reverse side of the Card.

3.2.2 STEP TWO: Authorization Requirements

All Sales must receive an Approval Code / Authorization through Your Electronic Device or when required, by telephoning Q*Net.

• Swipe the Card through Your Electronic Device to obtain an Authorization for the entire amount of the Sale.

  If the Card is unable to be Magnetically Swiped You must Manually Key Enter the Transaction using Your Electronic Device or call our Voice Authorization Center. *IMPORTANT: A clear and legible Imprint of the entire Cardholder Account Number must be obtained on the Sales Receipt that will be signed by the Cardholder.*

*IMPORTANT*: If a Card is Approved via Voice Authorization, You must then Manually Key Enter the Card Sale using Your Electronic Device. This must be completed in order to include the Sale in Your Batch Settlement file.
Please refer to the Authorization section for possible Authorization responses.

3.2.2.1 STEP THREE: Completing the Sale

- The Approval Code obtained must be on the Sales Receipt.

- Verify that all except the last four- (4) digits of the Cardholder Account Number and the Expiration Date is Truncated on the “customer copy” of the Sales Receipt.

  *For example:* The Cardholder Account Number is Truncated when the “customer copy” of the Transaction Receipt is displaying:

  ```
  Card Number: **********1234
  Exp Date: **/**
  ```

- Have the Cardholder sign the Sales Receipt. DO NOT alter the Transaction Receipt after the Cardholder has signed it.

- Compare the signature on the Sales Receipt to the signature on the Cardholder’s Card. The spelling of the name on the signature panel of the Sales Receipt MUST match the spelling of the name in the signature panel of the Card.

- Only the person who signed the signature panel on the back of the Card is authorized to use the Card. *For Your protection, NO exceptions should be made.*

- Verify that all printed and written information is clearly legible on all copies.

  - Give the Cardholder the “customer copy” of the Sales Receipt and return the Card.

3.3 Card Refunds/Credits

- A Refund/Credit must be issued to a Cardholder when an adjustment with respect to a Sale is required. If Your business establishment’s Disclosure states “No Refunds” please follow your established Disclosure policy.

- Your Refunds/Credits must be submitted electronically according to Your internal operating procedures.

- Authorization is not required for Credit/Refund Transactions. However, if dictated by Your own internal operating procedures, You can record the Approval Code from the original Sale on the Credit Receipt. The reason the Credit is being issued should also be briefly noted on the Credit Receipt.
• According to Visa and MasterCard regulations, a Merchant may not give cash, check or process a Refund/Credit to a Card other than the Card that was used for the original Sale. If Refund/Credit is not possible (i.e., Cardholder account closed) You may, at your own risk, process a Refund/Credit in another form however in the event of a Chargeback, You may not have reversal rights.

• The Refund/Credit must not exceed the original Sale amount. To do so, is against Visa and MasterCard regulations.

• The Refund/Credit must not be completed without having processed a previous Sale with the same Card.

• A Merchant must not issue a Refund/Credit to a Cardholder for the purpose of depositing funds to the Cardholder's account.

3.4 Preparing the Credit Receipt

• Prepare a Credit Receipt in the same manner as the Sales Receipt. Ensure the date of the Credit, description of merchandise returned, services cancelled, or adjustment made appears on the Credit Receipt.
• The Cardholder must sign the Credit Receipt in the space provided.
• When the Credit Receipt is completed, check all copies to see that the information is legible.
• The Cardholder is then given the “Customer’s Copy” of the Credit Receipt.

3.5 Even Exchanges

In the event of an even exchange, follow Your current internal operating procedures. Accept the returned merchandise and provide replacement merchandise of equal value.

3.6 Uneven Exchanges

In the event of a partial exchange, proceed as follows:

• Issue a Credit for the total amount of the returned merchandise.
• If applicable, the Merchant and the Cardholder must sign the Credit Receipt.
• Process a Sale on the Card for the total amount of the new merchandise purchased.
• Have the Cardholder sign the new Sales Receipt.
• Provide the Cardholder with the “customer copy” of the new Sales Receipt.
3.7 Expiration Dates

Visa® and MasterCard® do not allow inaccurate Expiration Dates during the Authorization process. CMS highly recommends that You include the valid Expiration Date with all Your Authorization requests. CMS has found that some Issuers Decline Authorization requests if the Expiration Date is not valid or unavailable.

3.8 Tips for Manually Imprinting Transactions

- For all Sales that are **not** Magnetically Swiped, You must obtain a clear and legible Imprint of the entire Card on the Sales Receipt that will be signed by the Cardholder. (This does not apply for Mail Order/Telephone Order Merchants). **This is Your proof that the Card was present at the time of the Sale.**

- CMS recommends that You **DO NOT** place the Sales Receipt on top of the Card and attempt to scratch or trace a pencil or crayon as validation of the Card Imprint.

- CMS **DOES** advise that You utilize an Imprinting Machine to Imprint the Card.

- Your Imprinting Machine must contain a metal plate that includes Your DBA (Doing Business As) name and city and state of the location where the Transaction occurred.

- For Merchants that are supported on the South Platform, supplies can be ordered by calling the Merchant Supply Department at 800-252-7762.

- For Merchants that are supported on the North Platform, supplies can be ordered by calling the Help Desk at 800-896-7161.

- When Imprinting a Card, the Sales Receipt must include the following:
  - Cardholder’s name
  - Entire Cardholder Account Number and Expiration Date
  - Date of the Sale
  - Merchant’s DBA (Doing Business As) name and city and state of the location where the Transaction occurred
  - Approval Code number(s), dates, and amounts given for the Sale
  - Brief description of merchandise or service
  - Dollar amount including sales tax (if applicable)
  - Cardholder’s signature **must** be contained on the signature line of the Sales Receipt.

- Complete the Sale information using a blue or black ballpoint pen. **DO NOT** use red ink, pencil, or a felt-tip pen or marker. They do not make a legible impression on the copies behind the original.
4 Fraud

Merchant education is one of the keys to monitoring and controlling fraud. At the Point of Sale, the Merchant must be educated to control fraud. CMS provides some available tools to educate Merchants and also makes available technology provided by third parties, such as Address Verification Services (See AVS under the Authorization section) to assist with controlling fraud.

Monitoring and increased awareness is also achieved by the use of reports generated by MasterCard and Visa. These various reports monitor and list suspicious and/or fraudulent activity at the Merchant locations. These reports are provided to CMS on a periodic basis and CMS' customer service managers review them periodically.

CMS acts as a liaison between the Issuers and CMS' Merchants when cases of fraud are suspected. CMS will work with Your security personnel, private detectives, and law enforcement officers to assist with the investigation of fraud cases.

4.1 Fraud Tips

There are several simple procedures that Merchants can employ to deter fraud at the time a Cardholder attempts to use a Card.

4.1.1 For Face-to-Face Transactions

- Watch for suspicious behavior. Ask Yourself –
  - Is the Cardholder purchasing an unusual amount of expensive items without regard to size or quantity?
  - Since there is usually little time to perfect a forged signature, a Card thief may be slow and calculating in an effort to the sign the Sales Receipt.
  - Does the Card appear to be damaged, altered, or discolored on the front or back?

- Check the Card’s Magnetic Stripe. Make sure the Magnetic Stripe is on the back of the Card. Using your Electronic Device, verify the Cardholder Account Number on the Sales Receipt to the embossed number on the Card. If it does not match but the Sale is still approved, You must call our Voice Authorization Center and request a “code 10.” (See Authorization section for information on “code 10.”)

- Verify the hologram on the Card. A Visa® Card should have an image of a dove and should seem three-dimensional and appear to move when the Card is tilted in the light. A MasterCard® Card should have a hologram with interlocking gloves showing the continents and should appear three-dimensional and move when the Card is tilted. The word “MasterCard” will appear in the background of the hologram. The letters “MC” are micro-engraved around the two rings.
• Check the “Expiration Date” and if available, the “Valid From Date.”

Transactions made on an invalid Card are a potential loss to You.

4.1.2 For Non Face-to-Face Transactions

• Train the phone order representative to be alerted to unusual activity during the telephone conversation such as:
  
  ➢ Apprehensiveness of the person, indiscriminate ordering of fraud prone merchandise (e.g., electronics) or background noise that may indicate that someone is calling from a public telephone.
  
  ➢ If the Cardholder orders a specific size and color, but will take anything available. This could be a fraudulent order.
  
  ➢ A Cardholder has difficulty spelling or pronouncing their name may be using another person’s Card.

• Ask the Cardholder for the name of the Issuer. Even if You take no action, the person that is ordering the merchandise may hang up if they are not in possession of the Card.

• Call the Cardholder back and verify the information that was originally provided for the Transaction.
If your Electronic Device is setup to prompt for the three-digit number on the back of the Card, ask the caller for the three-digit number. This feature provides a cryptographic check of the information embossed on the Card by dialing out to the Issuer and the Issuer, in turn, sends back a response code.

This also helps to validate whether or not the Cardholder has the Card in his/her possession.

Some of the most common Visa and MasterCard response codes are:

**Visa CVV2 Response Codes**

- **M**= CVV2 match
- **N**= CVV2 No match
- **P**= Not Processed
- **S**= CVV2 Should be on card but merchant indicates it is not
- **U**= Issuer not certified or has not provided Visa with encryption keys.
- **X**= Server Provider did not respond (default)

**MasterCard CVC2 Response codes**

- **M**= Valid or "Matched" CVC2 value
- **N**= Invalid CVC2 value
- **P**= CVC2 not processed
- **U**= Issuer unregistered for CVC2 Processing
5 DO’S AND DON’TS OF CARD ACCEPTANCE

DO...

At the Point of Sale

• Hold Card during entire Transaction.
• Ensure that all Cards are properly authorized.
• Swipe Card through the Terminal in one direction only.
• Truncate Card number on Cardholder copy of the Transaction Receipt.
• Obtain a complete and legible Imprint of the Card on the Sales Receipt for all key entered Sales.
• Obtain a complete and legible Imprint of the Card on the Sales Receipt when a Voice Authorization was performed.
• Compare signatures on the back of the Card and the Sales Receipt.
• Compare last four digits of the Cardholder Account Number on the Card and the Sales Receipt.
• Inform Cardholder of return policy and ensure that proper Disclosure is on the Sales Receipt.
• Process Refunds/Credits only to Card number of original Sale.
• Report any suspicious or fraudulent Card use.

Back Office

• Settle all Transactions on a daily basis for both Visa and MasterCard Transactions.
• Store Visa and MasterCard’s Transaction Receipts for 18 months.
• Respond to all retrieval requests on time with correct, complete, legible receipts.
• Respond to Chargebacks on time with complete, concise, legible explanations and documentation.
• Handle Cardholder complaints promptly to avoid Chargebacks.
• Notify Chase Merchant Services of any changes to Your account (e.g., banking, change of address, contact person, management, adding Card types, ownership of company, etc) to ensure no delay in Your processing.

DON’T...

• Accept a Declined Card for payment. Request another Visa® or MasterCard® or another form of payment.
• Accept an unsigned Card. Request photo ID and have Cardholder sign the Card.
• Split Authorization amounts in order to avoid a Decline.
• Ask for additional identification unless the signature panel is blank or signatures do not match.
• Impose Surcharges or place minimum or maximum amount on Sales.
• Issue cash to a Cardholder as a Refund/Credit for a previous Card charge.
• STORE the information on the MAGNETIC STRIPE! (other than 16 digit Card number, Expiration Date and Cardholder name).
6 PROCESSING & SETTLEMENT

Processing is the method whereby a Merchant’s transmission is entered through CMS to the Issuer for entry onto the Cardholder’s statement. Merchants may choose one of many electronic methods. These include:

- Batch
- Data Capture
- Dial Up or Dedicated Line

6.1 Batch

Merchants may submit files to CMS in a One Pass or Two Pass batch-processing environment. Each type of processing is outlined below.

6.1.1 One Pass

1. A file is submitted to CMS for Authorization. The authorized Transactions are automatically submitted through Interchange for settlement, by CMS.
2. CMS creates a billing file.
3. When submitting Your Transactions on a physical magnetic tape versus a transmission, You will need to provide a blank magnetic tape for Your Authorization responses to be returned to You.

6.1.2 Two Pass

1. A file is submitted to CMS for Authorization only.
2. Once the Authorization file is processed, the file is returned to You with the Authorization results indicated.
3. A file of all approved Transactions is then submitted for settlement to CMS.
4. CMS transmits the Transaction file to Interchange.
5. When submitting Your file on a physical magnetic tape versus transmission, You will need to provide a blank tape for Your Authorization responses to be returned to You.

6.2 Data Capture

If You authorize and settle Transactions through Data Capture Terminals, each Terminal will need to be Closed. Failure to Close Terminals daily will result in delayed payments in accordance with the Data Capture Terminal quick reference guide.

No Transactions will be settled unless Your Terminals have been properly Closed. You may also pay a higher Visa and MasterCard Interchange rate and be subject to Chargebacks and other fees.
6.3 Dial – Up or Dedicated Line

If You transmit Your Transaction file by dialing into CMS on a regular phone line or by Frame Relay or Lease Line, please follow the procedures listed below.

- If You verify Your files before You are ready to transmit, place a call to CMS’ Settlement Control Center Automated Deposit System (ADS) at (800) 884-2020.

- Call the assigned modem number to start Your transmission.

- If the data that is transmitted is out of balance or if there are problems with Your transmission, it cannot be processed. A CMS Representative will call Your designated contact to report the out of balance condition and determine the course of action to be taken.

6.4 Financial Settlement

CMS processes Your Visa and MasterCard Transactions and, if You prefer, T&E Card types (i.e., American Express®, Diners®/Carte Blanche®, Discover®, JCB®). CMS handles the Funding of Your Visa® and MasterCard® Card Transactions. The financial settlement of Your T&E Card Transactions is completed through the appropriate Card companies based upon Your Agreement with the applicable Card company.

If CMS is the Acquirer for Your Diners®/Carte Blanche® or JCB® Card Transactions, then CMS will Fund these Card Transactions.

Upon receipt of Your settlement file, CMS will submit payment to the bank You have designated.

CMS uses ACH (Automated Clearing House) and Wire as methods of payment.

6.5 Payment by ACH with a Non JPMorgan Chase Bank DDA

Your payment is received by Your bank approximately two business days after processing with a Non JPMorgan Chase Bank DDA. A sample time line is shown below.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DATE</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction date</td>
<td>1/14</td>
<td>Monday</td>
</tr>
<tr>
<td>Processing date</td>
<td>1/15</td>
<td>Tuesday</td>
</tr>
<tr>
<td>CMS sends to ACH</td>
<td>1/15</td>
<td>Tuesday</td>
</tr>
<tr>
<td>ACH sends to Your bank</td>
<td>1/16</td>
<td>Wednesday</td>
</tr>
<tr>
<td>Your bank memoposts Funds</td>
<td>1/17</td>
<td>Thursday</td>
</tr>
<tr>
<td>Your bank makes Funds available</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please note: If Your bank is a non-ACH participant, Your payment may be delayed by 24 hours.
6.6 Payment by Wire

Wire Transfer is an electronic funds transfer system where CMS transmits the wire information to the Federal Reserve System. The Federal Reserve will then transmit the Funds to Your bank and Your bank, will in turn, credit Your account.

Your payment is received by Your bank approximately one business day after processing. A sample time line is shown below:

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DATE</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction date</td>
<td>1/14</td>
<td>Monday</td>
</tr>
<tr>
<td>Processing Date</td>
<td>1/15</td>
<td>Tuesday</td>
</tr>
<tr>
<td>Federal Reserve transmits</td>
<td>1/16</td>
<td>Wednesday</td>
</tr>
</tbody>
</table>

**Please note:** Payments to Merchants are delayed by one business day on a day the bank is not open for business (e.g., holidays, weekends). The above timelines are samples and are not guaranteed. This is a general disclaimer on timelines.
7 INTERCHANGE
The exchange of financial and non-financial data associated with Sale and Credit information between Merchant Acquirers and Card Issuers for Visa and MasterCard Transactions.

7.1 What is an Interchange Fee?
A fee paid to an Issuer for Transactions entered into Interchange. The Interchange Fee applied is according to Visa and MasterCard regulations for each Transaction.

There are multiple categories of Interchange and Visa and MasterCard each have their own criteria for their own Interchange categories. A Transaction must meet the specified criteria for an Interchange category in order for that category’s rate to be applied. Each Transaction is evaluated individually.

7.2 How are Interchange Fees determined?
Interchange Fees are determined by Visa and MasterCard Interchange categories, a Merchant’s business type, and the operating procedure used by a Merchant. Visa® and MasterCard® determine these rates by assessing the level of risk and expenses associated with processing a Transaction.

Example: The Interchange Fee for a Face-to-Face Transaction is generally less than a Non Face-to-Face Transaction. The risk of fraud is lower because a Magnetic Swipe can be obtained and signature verified. If processing procedures have a higher risk of fraud, the Merchant may pay higher Interchange Fees.

7.3 What is a Non-Qualifying Interchange Expense?
Non-Qualifying Interchange Expense is the difference between the Interchange rate that the Merchant was set-up to qualify for (based on the type of business) and the Interchange level a Transaction actually qualified for. This expense is passed directly to the Merchant and is assessed as a percentage of the Sale.

The most common Non-Qualifying Interchange expenses occur because of processing errors. Listed below are some tips on how to reduce processing errors:

- Close all batches daily
- Keep Your Electronic Device updated and make sure all swipe readers are in working order
- Obtain a full Magnetic Swipe for all Card Transactions (When You cannot swipe, be sure to make an Imprint of the Card on the Sales Receipt that is signed by the Cardholder to reduce Chargeback liability)
- Authorize all Transactions electronically
- Notify CMS prior to making changes to or upgrading Your software or Electronic Device.
In an effort to combat fraud and reduce Chargebacks that ultimately lead to higher costs and risk for all parties, Visa and MasterCard Associations have developed several programs designed to mitigate fraud risk and reduce Chargebacks.

Essentially, guidelines have been established and Merchant monitoring programs and reports have been developed to track Merchant Transaction activity.

8.1 Failure to comply with the guidelines outlined in each Visa and MasterCard program may lead to any of the following:

- Operating procedure requirement modifications
- Incremental Chargebacks and/or fines and fees
- Settlement delay or withholding subject to a Chase Merchant Services investigation to validate Transactions
- Termination of Your Agreement.

Chase Merchant Services will make a reasonable effort to work on Your behalf and support You in defense of Association concerns where CMS believes You are not at fault or where CMS believes Association enforcement of unreasonable guidelines is evident.

If You would like more information on these programs, please contact Your relationship manager or Customer Support Associate.

8.2 Some, not all, of the Visa programs and a brief description of each are listed below:

8.2.1 Cardholder Information Security Program (CISP)

CISP compliance is required of all Merchants and Service Providers. The program applies to all payment channels, including retail (brick-and-mortar), Mail Order/Telephone Order, and E-commerce.

To achieve compliance with CISP, Merchants and Service Providers must adhere to all CISP requirements including the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all Card brands. This Standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements.

Following is a list of twelve basic security requirements:

1. Install and maintain a working firewall to protect data
2. Keep security patches up-to-date
3. Protect stored data
4. Encrypt data sent across public networks
5. Use and regularly update anti-virus software
6. Restrict access by “need to know”
7. Assign unique ID to each person with computer access
8. Do not use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly test security systems and processes
11. Implement and maintain an information security policy
12. Restrict physical access to data

Additional requirements of CISP and updated information can be found on the Visa website at www.visa.com/cisp
9 MASTERCARD PROGRAMS

9.1 The MasterCard Programs include, but are not limited to the following:

9.1.1 Site Data Protection (SDP)

MasterCard SDP compliance is required of all Merchant types, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to assist with protecting against the threat of Account compromises.

The Payment Card Industry (PCI) Data Security Standard is a component of SDP. It sets forth security standards which are required to be adopted by Merchants, Third Party Processors (TPPs) and Data Storage Entities (DSEs).

For the most updated information on SDP, please visit https://sdp.mastercardintl.com/
10 STORAGE & RETRIEVAL

10.1 Media Retention

Once a Sale or Credit Receipt has been completed, You are responsible for the retention and retrieval of the Transaction Receipts (Media).

In order to comply with Association regulations, You will need to store the original Media or a microfilm copy for:

- Visa – 12 months
- MasterCard - 18 months

10.2 What is a Retrieval Request?

A Retrieval Request is a request for a copy of the Sale or Credit Receipt (Media) and is the result of an inquiry from the Cardholder or their Issuer.

The retrieval functions, including the timeframes for Media retention, confirmation and response to the Issuer, are governed by the regulations established by Visa and MasterCard for Visa and MasterCard Card Transactions.

10.3 CMS Role

CMS may notify You that a request for a copy of the Sale or Credit Receipt has been received from the Issuer. At the Merchant’s request, these can be sent via fax, electronically, or by mail.

10.4 What “key” Information is contained on the Retrieval Request Form?

- Cardholder Account Number
- Transaction amount
- Transaction date
- Merchant reference number (Your reference number for the Transaction, if supplied)
- Merchant Number (Your Merchant Number assigned by CMS)
- Reason for the request
- Case number for each Sale or Credit Receipt request
- Due date to Respond
- Sequence number for better tracking (Each faxed report is sent in numerical order)
- Received items confirmation
- Second request notification
10.5 For North Platform Merchants, Send Your Retrieval Response and Correspondence to:

<table>
<thead>
<tr>
<th>U.S. MAIL</th>
<th>OVERNIGHT</th>
<th>FAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHASE MERCHANT SERVICES</td>
<td>CHASE MERCHANT SERVICES</td>
<td>301-745-7565</td>
</tr>
<tr>
<td>North Media Retrieval Services</td>
<td>North Media Retrieval Services</td>
<td></td>
</tr>
<tr>
<td>P.O. Box 6700</td>
<td>1 Western Maryland Parkway</td>
<td></td>
</tr>
<tr>
<td>Hagerstown, Maryland 21741</td>
<td>Hagerstown, Maryland 21741</td>
<td></td>
</tr>
</tbody>
</table>

SEE PAGE 31 FOR AN EXAMPLE OF THE RETRIEVAL REQUEST FORM.
My Merchant Services
P.O. Box 3009
Hagerstown, MD 21741

November 9, 2001  Faxed to: __________

GOEWIN'S MARKET
ATTN:
ANOTHER LINE
250 MAIN STREET
DINWIDDE, KS 00000-0000
COUNTRY
111111111.111.111111.11111.1

Your response must be received by July 2, 2001. Failure to respond will result in a debit to your account.

Your customer's bank has requested a copy of the transaction document(s) related to the credit card transaction identified below. Since the bank has only provided the transaction information listed below, we are unable to provide any additional information concerning the request (such as the cardholder's name and telephone number). If you have received this request via our automated fax service, we will fax you a confirmation of receipt after we have processed your response. If you would like to receive these requests via our fax service, please contact us at the number below.

TRANSACTION DETAIL INFORMATION

<table>
<thead>
<tr>
<th>Case Number</th>
<th>12346789</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Number</td>
<td>12345678901234567890</td>
</tr>
<tr>
<td>Credit Card Number</td>
<td>12345678901234567890</td>
</tr>
<tr>
<td>Transaction Amount</td>
<td>US$999,999,999,999,999</td>
</tr>
<tr>
<td>Foreign Amount</td>
<td>999,999,999,999,999,999</td>
</tr>
<tr>
<td>Transaction Date</td>
<td>mm/dd/yyyy</td>
</tr>
<tr>
<td>Total Batch Amount</td>
<td>999,999,999,999,999,999</td>
</tr>
<tr>
<td>Batch Date</td>
<td>mm/dd/yyyy</td>
</tr>
<tr>
<td>Reference Number</td>
<td>123456789012345678901234</td>
</tr>
<tr>
<td>Merchant Name</td>
<td>12345678901234567890123456</td>
</tr>
<tr>
<td>Airline Ticket Number</td>
<td>12345678901234</td>
</tr>
</tbody>
</table>

Did you include the following (if applicable)?

- Signature or Imprint of Card
- Receipt or Copy of Card
- Bank Statement or Registration Card
- Address Verification
- Bank Account Statement
- Airline Ticket
- Credit Receipt

Report Sequence Number: 11

FOR FAST PROCESSING, FAX YOUR RESPONSE TO:
301-745-7500

PLEASE FOLLOW THESE INSTRUCTIONS:

- For non-face-to-face transactions (mail/telephone and internet transactions) we recommend that you provide as much information as possible to establish cardholder participation in a transaction.

- For face-to-face transactions, the association's rules require a signed and card-imprinted (or not card-swiped) transaction document to establish cardholder participation in a transaction.

- Tape your original transaction document within the dotted area. Make a legible photocopy of the full document. (Set the photocopier to enlarge and darken, if necessary, to ensure clarity)

- Do not cover the Transaction Information on the left. If the size of your document exceeds the space provided, then attach the document(s) to separate sheet(s) of 8 1/2 by 11 white paper and write the case number on the top right corner of every sheet.

- Please ensure the entire cardholder number is shown on your documentation. If the number has been truncated, please write the full number on the document.

- Set the scan resolution on your fax machine to the finest setting. This will improve the clarity and legibility of the character and graphics on the scanned document.

FOR FAST PROCESSING, FAX YOUR RESPONSE TO: 301-745-7500

OR, MAIL TO:
MERCHANT SERVICES
P.O. BOX 770
HAGERSTOWN, MD 21740

Questions?
Call Merchant Services at:
1-800-332-4345

06:57/R.
10.6 Retrieval Tips

- Respond to all requests within the specified timeframe
- Include the Case Number on every page
- Ensure that You are receiving all Retrieval Requests by tracking the sequence number (located on the bottom left corner of the report)
- Ensure that all Media has the required information and that it is clearly legible.
- Research the item using the Retrieval Request form, locate the Media, make a clear and legible copy, and send to CMS within the specified timeframe.
- Always retain the original Media for Your records.
- Store the Media by the Transaction Date as the Cardholder’s name is not provided by the Issuer

10.7 Retail Media Requirements include:

- Merchant DBA (Doing Business As) name and city & state
- Entire Cardholder Account Number & Expiration Date
- Sale and/or Credit amount
- Transaction date
- Signature of Cardholder on the Sales and/or Credit Receipt
- Itemization or brief description of charge(s)
- All Approval Code number(s) dates, and amounts
- If Card was not swiped, a clear and legible Imprint of the entire Card number and Expiration Date on the Sales receipt that was signed by the Cardholder
- All supporting documentation

Note: T&E Cards (i.e. American Express®, Diners®/Carte Blanche®, Discover®, and JCB®) Media requests are mailed or faxed directly to You from that Card company.

If CMS is the Acquirer of Your Diners®/Carte Blanche® or JCB® Transactions, CMS will forward the Media request to You.
11 CHARGEBACKS

11.1 What is a Chargeback?

A Chargeback occurs when the Issuer refuses to honor a presentment of a settled Transaction because they believe the Transaction violates a specific Visa or MasterCard regulation. The Issuer can charge back a Transaction within the timeframes set forth by Visa and MasterCard.

11.2 CMS’ Role

CMS may assist You with handling Chargebacks when CMS deems appropriate. The Visa and MasterCard Chargeback procedures may change from time to time and it is Your obligation to comply with the requirements.

A reasonable effort is made to reverse the Chargeback to the Issuer on Your behalf if CMS deems a reversal is appropriate. A significant percent of Chargebacks are resolved by CMS without Your involvement. This is done by disproving the validity of the Chargeback or by providing the required documentation. Some of the checks CMS may perform include:

- Verification of Chargeback processing timeframes confirming that the Chargeback was processed within the time periods mandated by Visa and MasterCard regulations

- Detection of duplicated Chargebacks confirming that the same Chargeback has not been processed twice.

- Validation of reference number to confirm that the reference number assigned to each individual Transaction is matched to the reference number for the Chargeback

- Validation of Authorization – Matching Merchant’s Authorizations, Transactions, and amounts on file for a particular Cardholder Account Number to the Cardholder Account Number and dollar amount of the Chargeback.

- Research the Transaction in dispute and determine the proper resolution of the item in accordance with the prescribed MasterCard and Visa regulations.

- Verify proper documentation – Verify that Issuer documentation required by Visa and MasterCard has been provided.

If it is necessary to debit or credit Your account for a Chargeback, You will receive documentation explaining the Chargeback or credit to Your account.
11.3 Merchant’s Role

The following action should be taken if You wish to refute a Chargeback:

- Check the date indicated on the Chargeback Adjustment Advice. Ensure that CMS will receive Your response prior to the “due date.”

- Read the Chargeback documentation requirements. Determine if any information necessary to refute the Chargeback requires external assistance (shipping logs, proof of delivery, technical advice, etc).

The Chargeback documentation consists of:

- Chargeback Adjustment Advice
- Chargeback Response form
- Chargeback Summary
- All documentation in regards to the Chargeback

- **Always** indicate the reason You wish to refute the Chargeback in the space provided on the Chargeback Response Form. Include Your name, the date, and Your phone number. Any further documentation that applies to the Chargeback should be attached to the Chargeback Response Form and returned to CMS. **Again, CMS must be in receipt of Your response by the due date specified.** This will preserve Your Chargeback reversal rights.

- Review the Chargeback documentation prior to returning it to CMS. Ensure that the documents necessary to refute the Chargeback are legible and fulfill the appropriate requirements.

- Understand why You are receiving the Chargeback. If You have any questions, contact Your Customer Support Associate prior to the due date. Before calling, please have available the case number, Chargeback date, and Your Merchant Number.

The CMS Chargeback department will evaluate the information You have supplied in Your rebuttal based on the Visa and MasterCard regulations. In the event the Chargeback is reversed, You will receive a Chargeback Adjustment Advice indicating that the Chargeback has been reversed. If the Chargeback cannot be reversed, You will receive a Merchant inquiry response explaining why the Chargeback cannot be reversed.

The response date is extremely important. **If You fail to provide the specific information by this date, the Chargeback reversal rights as established by Visa and MasterCard regulations, will be forfeited.**
11.4 The fax number and mailing address for Your Chargeback response and correspondence for South or North Platform is the following:

11.4.1 North Platform

<table>
<thead>
<tr>
<th>Fax Number</th>
<th>U.S. Mail</th>
<th>Overnight Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>301-766-5851</td>
<td>CHASE MERCHANT SERVICES</td>
<td>CHASE MERCHANT SERVICES</td>
</tr>
<tr>
<td></td>
<td>P.O. Box 6011</td>
<td>3 Western Maryland Parkway</td>
</tr>
<tr>
<td></td>
<td>Hagerstown, MD 21741</td>
<td>Hagerstown, MD 21741</td>
</tr>
<tr>
<td></td>
<td>Attn: North Chargebacks</td>
<td>Attn: North Chargebacks</td>
</tr>
</tbody>
</table>
12 IMPLEMENTATIONS

12.1 Adding New Locations

When adding new Merchant locations, Student Accounting must be notified at x53739 or x52094. Appropriate approvals must be received prior to requesting a new merchant set up. FS accounts must be verified for correctness, and all requested information must be provided including a valid business need. Credit card setups are not automatically approved.

12.2 Adding New Card Types

All merchants are setup with the ability to process all card types. It is up to the merchant to determine which cards they wish to accept.

12.3 Banking Information Changes

- Any changes to bank information must be pre-approved through General Accounting at UCLA.
Authorization Agreement for Automated Billing and
For Direct Deposits

Company Name: _________________________________________________

Chase Merchant Number: ___________________ Root #’s __________________________

Address_______________________________________________________________________________

City_________________________State_______________________________________Zip___________

Phone number: ____________________

Fax number: _____________________

I (we) hereby authorize Chase Merchant Services, L.L.C. to initiate credit and debit entries and to
initiate, if necessary, credit and debit entries and adjustments for any credit and debit entries in
error to my (our) Checking account indicated below and the depository named below, hereinafter
called Financial Institution, to debit and/or credit the same to such account.

Financial Institution___________________________________Branch____________________________________

Contact at bank: _____________________________Phone # __________________________________

City_________________________________State___________________________________Zip_______

Transit/ABA No._______________________________________Account _________________________

(A voided check must be attached)***No Starter Checks

Payment Method:  ACH ___________ Wire _____________ (fee may apply)

Effective Date for Change: ____________________________

This authority is to remain in full force and effect until Chase Merchant Services, L.L.C. has
received written notification from me (or either of us) of its termination in such time and such
manner as to afford Chase Merchant Services, L.L.C. and Financial Institution a reasonable
opportunity to act on it.

Date_____________________Name_____________________________Signature________________

Fee Charged by CSA: _______ Date: __________ Amount : __________

RETURN VIA FAX TO (954) 845-5884 ATTN: AIS
13 FOCIS

FOCIS (Fast Online Customer Inquiry System) is a system designed to give You greater control in understanding and handling Your Bankcard processing. FOCIS provides up to the minute information on Your account. It provides facts on deposits, Chargebacks, invoices, even specific Transactions and Approval Codes.

Issuing Bank Number
Transaction Files
Terminal Assistance
Supplies

FOCIS is accessed through any touch-tone phone. A FOCIS instruction list, detailing the use of the system is shown on the following page.

If You require further assistance after accessing FOCIS, knowledgeable Customer Support Associates are available to answer Your questions.
CHASE MERCHANT SERVICES, L.L.C.
FAST ONLINE CUSTOMER INQUIRY SYSTEM
Instructions for Use

FOCIS Telephone Number:
800-326-7991

To access a specific extension PRESS 1
For an issuing banks telephone number PRESS 2
To obtain or cancel an Authorization or For Address Verification PRESS 3
For assistance with balancing or Closing Your Terminal or help with Terminal related problems PRESS 4
For information on a specific Sale Or Credit Transaction, including Approval code PRESS 5
For deposit, payment, or invoice Information PRESS 6
For information on a Chargeback PRESS 7
To request a copy of a Daily or Monthly Report PRESS 8
To speak to the next available Customer Support Associate PRESS 0
(Please be sure to have Your Merchant Number available)
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA</td>
<td>Directs electronic ACH deposits to the Merchant’s designated bank. Also referred to as “Transit Routing Number.”</td>
</tr>
<tr>
<td>ACH (Automated Clearing House)</td>
<td>An electric means of payment to a Merchant’s bank account.</td>
</tr>
<tr>
<td>Acquirer</td>
<td>A licensed Visa or MasterCard member that acquires the data relating to a Transaction and submits this data into Interchange.</td>
</tr>
<tr>
<td>Acquiring Bank</td>
<td>A bank that contracts with a Merchant to accept and process Card Transactions.</td>
</tr>
<tr>
<td>Agreement</td>
<td>The binding Agreement between JPMorgan Chase Bank, Chase Merchant Services, L.L.C., and the Merchant to utilize CMS’ Card processing services.</td>
</tr>
<tr>
<td>AIS (Account Implementation Services)</td>
<td>CMS department that is responsible for implementing new Merchants as well as changes to existing Merchant accounts.</td>
</tr>
<tr>
<td>American Express</td>
<td>An entity that issues American Express Cards and supports Merchant’s that accept American Express for processing. Also referred to as “Amex”</td>
</tr>
<tr>
<td>Approval</td>
<td>An Authorization response notifying the Merchant that a Sale may be completed.</td>
</tr>
<tr>
<td>Approval Code</td>
<td>The numerical code(s) that is assigned by the Issuer as proof of an authorization. Also referred to as “Authorization Code.” The Approval Code is returned in the Authorization response message and is usually recorded on the Sales Receipt as proof of Authorization.</td>
</tr>
<tr>
<td>Assessment Fees</td>
<td>Fees assessed by Visa and MasterCard to both the Acquirer (CMS) and the Issuer. These fees are based on a percentage of a processed Transaction.</td>
</tr>
<tr>
<td>Authorization</td>
<td>A procedure used when a Merchant requests Approval for a Transaction.</td>
</tr>
<tr>
<td>Associations</td>
<td>Any entity formed to administer and promote Cards, including Visa and MasterCard, and any other entity as specified in Your Agreement.</td>
</tr>
<tr>
<td>Authorization Decal</td>
<td>A gummed label a Merchant receives designating the phone number for Voice Authorization.</td>
</tr>
<tr>
<td>AVS (Address Verification Service)</td>
<td>A service that allows Merchants to verify the billing address of the Cardholder on the Issuer’s file. AVS was developed to reduce fraud.</td>
</tr>
<tr>
<td>Bank Transit Number</td>
<td>A unique and individual number used to identify a particular bank.</td>
</tr>
<tr>
<td>Bankcard</td>
<td>Used to identify a Card issued by a bank</td>
</tr>
<tr>
<td>Batch Authorization</td>
<td>An Authorization method in which a Merchant accumulates Authorization requests and transmits these requests to CMS. This process consists of one-pass and two-pass Merchants.</td>
</tr>
<tr>
<td>Batch Settlement</td>
<td>A processing method in which a Merchant sends in a settlement file with pre-approved Transactions. These Transactions are then processed by CMS.</td>
</tr>
<tr>
<td><strong>Card</strong></td>
<td>A valid credit card or valid off line debit card bearing the service mark of Visa or MasterCard, and to the extent provided by Your Agreement and applicable, a valid Card issued by any other Associations.</td>
</tr>
<tr>
<td><strong>Cardholder</strong></td>
<td>A person to whom a Card has been issued or who is authorized to use the Card.</td>
</tr>
<tr>
<td><strong>Cardholder Account Number</strong></td>
<td>A unique number assigned to a Cardholder by their bank that is embossed on their Card. Also sometimes referred to as “Account Number.”</td>
</tr>
<tr>
<td><strong>Chargeback</strong></td>
<td>A Chargeback occurs when the Issuer refuses to honor a presentment of a processed Transaction. This may happen because the bank believes there has been a violation of a specific Visa or MasterCard regulation, or a Cardholder disputes the Transaction.</td>
</tr>
<tr>
<td><strong>Chargeback Adjustment Advice</strong></td>
<td>A CMS form that notifies the Merchant of the reason for a particular Chargeback and how it can be resolved.</td>
</tr>
<tr>
<td><strong>Chargeback Reason Code</strong></td>
<td>A two-digit code assigned by Visa or MasterCard identifying the specific reason for the Chargeback.</td>
</tr>
<tr>
<td><strong>Chargeback Response Form</strong></td>
<td>A CMS form that allows the Merchant to write or type an explanation on why the Merchant wishes to refute the Chargeback.</td>
</tr>
<tr>
<td><strong>Chargeback Summary</strong></td>
<td>A CMS form that lists all chargeback items for a particular day.</td>
</tr>
<tr>
<td><strong>Close / Closed / Closing</strong></td>
<td>An action of settling a batch of Card Transactions to CMS for payment. This can either be performed manually or by automatic settlement using a Data Capture Terminal.</td>
</tr>
<tr>
<td><strong>Code 10</strong></td>
<td>A security term used by a Merchant to notify CMS Voice Authorization Center that they are suspicious of a Cardholder. The Authorization center will advise the Merchant on how to proceed.</td>
</tr>
<tr>
<td><strong>Credit</strong></td>
<td>A Refund or price adjustment given by a Merchant for a previous Sale.</td>
</tr>
<tr>
<td><strong>Credit Receipt</strong></td>
<td>A document showing a Cardholder’s Credit/Refund issued by a Merchant. The paper form used by the Merchant, and sometimes signed by the Cardholder, to document the Transaction. Also referred to as “Transaction Receipt,” “Terminal Receipt,” “Media,” “Credit Draft,” or “Credit/Refund Slip.”</td>
</tr>
<tr>
<td><strong>CSA (Customer Support Associate)</strong></td>
<td>A CMS employee who has day-to-day contact with Merchant to answer inquiries and provide assistance.</td>
</tr>
<tr>
<td><strong>CVC2 (Card Validation Code) - MasterCard</strong></td>
<td>A unique three-digit number check for the purpose of validating MasterCard Card information during the Authorization process. The number may be used as an additional means of Cardholder verification during Non Face-to-Face Transactions.</td>
</tr>
<tr>
<td><strong>CVV (Card Verification Value) - Visa</strong></td>
<td>A unique three-digit number check for the purpose of validating Visa Card information during the Authorization process. The number may be used as an additional means of Cardholder verification during Non Face-to-Face Transactions.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Data Capture</strong></td>
<td>A method of processing where Transactions are entered by the Merchant into a Terminal. These Transactions are authorized, stored and captured. At the end of that day, the Terminal is closed and all Transaction information is relayed to CMS for processing.</td>
</tr>
<tr>
<td><strong>Data Storage Entity (DSE)</strong></td>
<td>An entity other than a Merchant or TPP that stores account data on behalf of its Merchants</td>
</tr>
<tr>
<td><strong>DBA (Doing Business AS)</strong></td>
<td>The name a Merchant uses when transacting business with its customers. This name will also appear on the Cardholder’s statement.</td>
</tr>
<tr>
<td><strong>DDA (Demand Deposit Account)</strong></td>
<td>DDA is a Merchant’s designated bank account for debits, credits, deposits, fees, invoices, etc.</td>
</tr>
<tr>
<td><strong>Decline</strong></td>
<td>An Authorization response notifying a Merchant that a Sale cannot be completed.</td>
</tr>
<tr>
<td><strong>Dial-Up</strong></td>
<td>A connection between machines as established over a phone line.</td>
</tr>
<tr>
<td><strong>Diners/Carte Blanche</strong></td>
<td>An entity that issues Diners/Carte Blanche Cards and supports Merchant’s that accept Diners/Carte Blanche for processing.</td>
</tr>
<tr>
<td><strong>Disclosure</strong></td>
<td>A term used to describe a Merchant’s specific merchandise Sales, return, or service policies that must be properly outlined on the Cardholder’s Transaction Receipt.</td>
</tr>
<tr>
<td><strong>Discover</strong></td>
<td>An entity that issues Discover Cards and supports Merchant’s that accept Discover for processing.</td>
</tr>
<tr>
<td><strong>Electronic Commerce (E-Commerce)</strong></td>
<td>The use of the internet for the purpose of buying/purchasing goods or services</td>
</tr>
<tr>
<td><strong>Electronic Commerce Transaction</strong></td>
<td>A Non Face-to-Face Transaction conducted over the Internet or other network using a Cardholder access device, or personal computer in which the Cardholder account information is transferred from the Cardholder to the Merchant.</td>
</tr>
<tr>
<td><strong>Electronic Device</strong></td>
<td>A Point-of-Sale Terminal or PC that reads the Card information encoded in the Magnetic Stripe and electronically authorizes and captures Transaction data.</td>
</tr>
<tr>
<td><strong>Expiration Date</strong></td>
<td>The embossed date on a Card that shows the date a Card expires.</td>
</tr>
<tr>
<td><strong>Expired Card</strong></td>
<td>A Card that the Expiration Date embossed or encoded by the Issuer has passed.</td>
</tr>
<tr>
<td><strong>Face-to-Face</strong></td>
<td>Transaction that involves the presence of Merchant and Cardholder.</td>
</tr>
<tr>
<td><strong>Frame Relay</strong></td>
<td>A phone line used by a Merchant that allows a direct connection into CMS.</td>
</tr>
<tr>
<td><strong>Funding / Funded</strong></td>
<td>A process by which CMS pays the Merchants for their submitted Card activity.</td>
</tr>
<tr>
<td><strong>Imprint</strong></td>
<td>An impression of a Card on a Transaction Receipt as proof that the Card was present. The Imprint can be obtained by using an Imprinting Machine.</td>
</tr>
<tr>
<td><strong>Imprinter / Imprinting Machine</strong></td>
<td>A device used to produce an image onto a Sales draft of the embossed characters of a Card.</td>
</tr>
<tr>
<td><strong>Interchange</strong></td>
<td>The exchange of financial and non-financial data associated with Sale and Credit information between Merchant Acquirers and Card Issuers for Visa and MasterCard Transactions.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interchange Fee</td>
<td>A fee paid to an Issuer for Transactions entered into Interchange. The Interchange Fee applied is according to Visa and MasterCard regulations for each Transaction.</td>
</tr>
<tr>
<td>Issuer</td>
<td>A member of Visa or MasterCard who contractually issues Cards.</td>
</tr>
<tr>
<td>JCB (Japanese Credit Bureau)</td>
<td>An entity that issues JCB Cards and supports Merchant's that accept JCB for processing.</td>
</tr>
<tr>
<td>Lease Line</td>
<td>A point to point connection type that uses SNA, X.25 or IP as its protocol.</td>
</tr>
<tr>
<td>Magnetic Stripe</td>
<td>The stripe on the back of a Card that a Merchant can swipe through a Terminal that reads the Cardholder's Account Number, Expiration Date, etc.</td>
</tr>
<tr>
<td>Manually Key Enter</td>
<td>A term used to describe processing a Card transaction without swiping the Card through a Merchant's Electronic Device.</td>
</tr>
<tr>
<td>MCC (Merchant Category Code)</td>
<td>A code designated by Visa and MasterCard that identifies a Merchant’s business classification.</td>
</tr>
<tr>
<td>Media</td>
<td>A term used to define a legible reproduction of a Transaction Receipt (e.g., Sales or Credit Receipt) and any supporting documentation (e.g. computer printouts, shipping and delivery logs) in support of a Retrieval Request</td>
</tr>
<tr>
<td>Merchant</td>
<td>Any customer utilizing CMS’ Card processing services.</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>A unique CMS number that identifies the Merchant.</td>
</tr>
<tr>
<td>Merchant Response Form</td>
<td>A section of the Chargeback advice or LPS form, which the Merchant completes if they wish to refute a Chargeback.</td>
</tr>
<tr>
<td>MOTO (Mail Order/Telephone Order)</td>
<td>A Transaction that takes place through the mail, fax, Internet, or over the phone.</td>
</tr>
<tr>
<td>Non Face-to-Face</td>
<td>Transaction that does not involve the presence of Merchant and Cardholder. (i.e., transaction takes place over the phone, Internet, fax, etc.)</td>
</tr>
<tr>
<td>North Platform</td>
<td>One of CMS or its affiliates' processing systems with a unique format for Authorization, Settlement, and Interchange for Merchants.</td>
</tr>
<tr>
<td>One Pass Batch Authorization</td>
<td>A type of Authorization where all Sales that receive an Authorization are processed. The Transactions that are not authorized are returned to the Merchant.</td>
</tr>
<tr>
<td>Operating Guide</td>
<td>The then-current manual prepared by CMS containing operational procedures, instructions, and other directives relating to Card Transactions.</td>
</tr>
<tr>
<td>Pickup</td>
<td>An Authorization response given to a Merchant that an Issuer is requesting that the Cardholder’s Card be confiscated.</td>
</tr>
<tr>
<td>Point of Sale (POS)</td>
<td>The Merchant’s location where a Transaction originates between a Cardholder and a Merchant.</td>
</tr>
<tr>
<td>Point-of-Sale (POS) Terminal</td>
<td>An Electronic Device placed in a Merchant location that is connected to the processor’s system via telephone lines and is designed to authorize, record, and settle data by electronic means for all Card Transactions.</td>
</tr>
<tr>
<td><strong>Presentment</strong></td>
<td>A Transaction submitted for the first time by an Acquirer to an Issuer and processed through Interchange.</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Processing Date</strong></td>
<td>The date when a Transaction is processed electronically through settlement.</td>
</tr>
<tr>
<td><strong>Q*Net</strong></td>
<td>Automated Authorization call system that is accessed by touch tone. Also referred to as Voice Authorization Center.</td>
</tr>
<tr>
<td><strong>Refund</strong></td>
<td>See “Credit.”</td>
</tr>
<tr>
<td><strong>Retrieval Request</strong></td>
<td>A form generated to request a copy of a Visa or MasterCard Sales or Credit Receipt. This request is initiated by either the Cardholder or the Issuer.</td>
</tr>
<tr>
<td><strong>Sale</strong></td>
<td>An action that involves a Cardholder’s purchase with a Card.</td>
</tr>
<tr>
<td><strong>Sales Receipt</strong></td>
<td>A document showing a Cardholder’s purchase made with a Card. The paper form used by the Merchant, and signed by the Cardholder, to document a Transaction. Also referred to as “Transaction Receipt,” “Terminal Receipt,” “Media,” “Sales Draft,” “Charge Slip” or “Sales Slip.”</td>
</tr>
<tr>
<td><strong>Service Establishment Number</strong></td>
<td>A Merchant’s account number for a Card type other than Visa and MasterCard. Also referred to as an “SE Number”</td>
</tr>
<tr>
<td><strong>Service Provider</strong></td>
<td>Any entity that provides services and stores, processes, or transmits Visa Cardholder data.</td>
</tr>
<tr>
<td><strong>South Platform</strong></td>
<td>One of CMS or its affiliates processing system with a unique format for Authorization, Settlement, and Interchange for Merchants.</td>
</tr>
<tr>
<td><strong>Surcharge</strong></td>
<td>A fee charged to a Cardholder by the Merchant for Transactions initiated at the Point-of-Sale. Visa and MasterCard have rules governing the use of surcharges.</td>
</tr>
<tr>
<td><strong>T&amp;E (Travel &amp; Entertainment) Cards</strong></td>
<td>Travel &amp; Entertainment Cards (e.g., American Express, Discover, Diners/Carte Blanche) also known as Non-Bankcards because they are not issued by banks however, the private, non-bank companies deal directly with the Cardholder and the Merchant.</td>
</tr>
<tr>
<td><strong>Terminal</strong></td>
<td>A device used to receive or transmit data through a communications system.</td>
</tr>
<tr>
<td><strong>Third Party Processor (TPP)</strong></td>
<td>Any entity that provides services secured by or performing services on behalf of Merchants that stores, processes, or transmits Cardholder data.</td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
<td>Any action between a Cardholder and a Merchant that results in activity on the Card, such as a Sale, Credit/Refund, Void, etc.</td>
</tr>
<tr>
<td><strong>Transaction Date</strong></td>
<td>The date a Transaction between a Cardholder and a Merchant occurs.</td>
</tr>
<tr>
<td><strong>Transaction Receipt</strong></td>
<td>A document showing the specific detail of a transaction (whether it be a Sale, Refund/Credit, Void, etc) processed by a Merchant.</td>
</tr>
<tr>
<td><strong>Truncation / Truncate</strong></td>
<td>Visa and MasterCard regulation requiring all except the last four digits of the Card number and the entire expiration date to be hidden or undetected on the Cardholder’s copy of the Transaction Receipt</td>
</tr>
<tr>
<td><strong>Two Pass Batch Authorization</strong></td>
<td>A type of Authorization where all Sales that receive Authorization, as well as those that do not, are returned to the Merchant. The Merchant identifies those Transactions that are to be processed and then submits them to CMS for processing.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Valid From Date</strong></td>
<td>A date embossed on a Card that shows when the Cardholder may begin using their Card.</td>
</tr>
<tr>
<td><strong>Voice Authorization</strong></td>
<td>An Authorization method used by a Merchant who calls the Voice Authorization Center.</td>
</tr>
<tr>
<td><strong>Voice Authorization Center</strong></td>
<td>CMS Authorization Center used for the purpose of attempting to obtain an Authorization via telephone.</td>
</tr>
<tr>
<td><strong>Void</strong></td>
<td>The total elimination of a captured Transaction in a Terminal as a result of an error while still at the Point of Sale. The Void occurs before the Terminal is Closed.</td>
</tr>
<tr>
<td><strong>Wire Transfer</strong></td>
<td>An electronic means of payment.</td>
</tr>
<tr>
<td><strong>You, Your, Yours</strong></td>
<td>Term to describe Merchant</td>
</tr>
</tbody>
</table>