Merchant Operating Guide:
Payment Processing Solutions

NOVA NETWORK

NOVA NETWORK

ABOUT YOUR CARD PROGRAM

Accepting Cards as a payment option involves several parties. It begins as a Transaction between you and your customer, and expands to involve us, as well as your customer's Card Issuer.

This Merchant Operating Guide is a part of your Agreement with us and is meant to provide you with simple, easy-to-read instructions for processing Transactions and minimizing the risk of fraud to your business.

Please familiarize yourself with this guide as you are the first line of defense in preventing Card fraud. Failure to comply with the guidelines and suggestions set forth in this guide may be considered a breach of the Agreement and may result in a financial loss to your business.

Throughout this guide, defined terms (i.e., terms having a meaning specific to the Card industry) are noted with initially capitalized letters (e.g., Credit Card, Card Present Transactions). If you are not familiar with these terms, refer to Appendix A, *Glossary,* on page 59 for definitions.

TYPES OF CARDS

Types of Cards include:

◆ **Credit Card**: A Credit Card is issued by a financial institution or other Credit Card company (called the Issuer) that extends a line of credit to its Cardholder. Visa and MasterCard Credit Cards are issued by banks (often referred to as "Bank Cards"), while American Express, Discover, and other Credit Cards may be issued by the Card company itself or in some instances by other financial institutions. There are many Issuers that offer Visa and MasterCard Credit Cards, making it possible for a Cardholder to have several different Credit Cards, each of which represents its own line of credit. These Credit Cards allow the Cardholder to

NOVA NETWORK

borrow money against a credit line and to repay the funds with interest if the Balance is carried over from month to month.

◆ **Debit Card**: A Debit Card is issued by a financial institution, and when used to make a purchase, results in the immediate withdrawal of funds from the Cardholder's bank account. Debit Cards do not represent a line of credit; they can only be used to the extent the Cardholder has available funds. Visa and MasterCard offer Debit Cards in addition to Credit Cards. Debit Cards may be PIN-based or signature-based.

◆ **Automated Teller Machine (ATM) Card**: An ATM Card is a plastic card issued by a financial institution and allows a customer to withdraw funds, make deposits, make purchases, or perform other banking functions through an ATM or POS Device against the Cardholder's bank account.

◆ **Electronic Gift Cards (EGC)**: EGCs are sold and issued by Merchants to customers as a set dollar amount of credit for future purchases. When the Cardholder uses an EGC to make a purchase, the Transaction total is deducted from the value remaining on the Card until the pre-paid amount is spent.

◆ **Electronic Benefits Cards (EBT)**: EBTs are Cards used for electronic benefits (e.g., food stamps or cash benefits) transfers between the Cardholder and the Merchant, and are used like Debit or ATM Cards (requiring a PIN). When an EBT is used to make a purchase, the Transaction total is deducted from the value remaining in the Cardholder's account until the pre-paid amount is spent.

ABOUT TRANSACTION PROCESSING

When you accept Credit Cards or Debit Cards for payment, you process the Transactions through your Terminal or software. A group of Transactions is called a Batch, and the process of sending these Transactions to us is called Settlement.

When you settle a Batch, the information for each Transaction is sent to clearing networks across the country and sometimes around the world. Based on each Card number, we send information about a Transaction to the corresponding Issuer so they can charge the Cardholder. Shortly thereafter, the funds for the Transaction are deposited into your Demand Deposit Account (DDA). Refer to

NOVA NETWORK

Chapter 2, *Processing Transactions*, for specific details about processing Transactions.

In exchange for these services, you pay a percentage of each Transaction, known as a Discount, along with transaction fees, authorization fees, and/or other fees. Fees are deducted from your DDA on either a monthly or a daily basis.

Occasionally, a Cardholder does not agree with Transactions posted to their account. When this happens, the Cardholder can contact the Issuer and initiate a dispute which will result in the Transaction amount being debited from your account. In this case, you also receive a notice directly from us. In order to protect your rights, it is important that you respond promptly to any notice you receive. Refer to Chapter 6, *Retrieval Requests & Chargebacks*, for a detailed explanation of this process.

PARTIES INVOLVED IN YOUR CARD PROGRAM

There are many individuals and entities involved in your Card program, each having an important role in Transaction processing. The individuals and entities include:

- **Issuer**: A financial institution or other entity that issues Cards to Cardholders. Issuers may approve the Cardholder for a credit limit, as applicable, or provide access to the Cardholder's bank account and also:
  - Approve or decline Transactions
  - Bill the Cardholder for charges to the Card
  - Collect funds from the Cardholder to pay for purchases
  - Initiate Chargebacks

- **Cardholder**: The person in whose name the Card is issued and who uses the Card for purchasing goods or services, or, in limited instances under a separate agreement, to obtain a Cash Advance.
- **Visa and MasterCard**: Worldwide payment service organizations who provide Credit and Debit Cards to Issuers. Both Visa and MasterCard set and enforce rules and regulations that govern use of their Credit and Debit Cards. Both organizations are also responsible for clearing and settling Card Transactions (Interchange).

◈ **Merchant**: The business entity that provides goods and/or services to Cardholders

◈ **Servicer**: The entity that provides Card processing services to Merchants

◈ **Member**: (also known as an Acquirer) The financial institution, designated by us, that is a principal, sponsoring affiliate or other member of Visa or MasterCard

GENERAL OPERATING GUIDELINES

When you process Transactions, it is important to keep a few general guidelines in mind:

◈ **Do Not Set Restrictions on Card Transactions**: Visa and MasterCard prohibit setting a minimum or maximum purchase amount. You are also prohibited from adding a surcharge to the amount of the Transaction, although you may give a discount from your standard pricing for payment by cash. Card customers are frequently among your best customers due to their available line of credit, purchasing freedom, and their tendency to spend more than cash customers.

◈ **Keep Passwords Secure**: You must keep all passwords that allow you to access our databases or services secure. Remember, you are responsible for the actions of anyone who uses your password. If you believe your password has been compromised or shared with an unauthorized user, please contact us immediately.

◈ **Protect Cardholder Privacy**: Visa and MasterCard regulations prohibit listing a Cardholder's personal information on the Transaction Receipt because it can expose a Cardholder to increased risk of fraud. You may only require a Cardholder's personal information if it is necessary to complete a Transaction (such as a delivery address and/or telephone number for Card Not Present Transactions) or if the Voice Authorization Center specifically requests it. If you obtain a Cardholder's personal information, you may not write it on the Transaction Receipt. You may not refuse to complete an otherwise valid Card Transaction just because a Cardholder refuses to provide additional identification or information.

◈ **Plan Ahead for Fees and Chargebacks**: You must maintain sufficient funds in your DDA to cover all fees, Chargebacks, or any other adjustments that may occur. Monthly fees are debited

NOVA NETWORK

from your DDA near the beginning of each month for the prior month's activity. To cover monthly fees and the possibility of Chargebacks, we recommend that you keep five percent (5%) of your average monthly processing volume available in your account. Keep in mind that this is only a recommendation and your business may require additional available funds. For example, businesses that conduct high-risk Transactions (such as Card Not Present or those with future delivery of products) should consider maintaining a higher percentage of their average monthly processing volume.

- **Keep Cardholder Data Secure**: You should keep all Transaction Receipts in a locked area that is accessible only to select personnel. When you dispose of Transaction Receipts after the designated retention period, make sure that account numbers and Imprints are rendered unreadable, as criminals can commit fraud with even a few pieces of Cardholder data. Your customers will not only appreciate your concern and consideration, but will also gain confidence in your service and integrity.

- **Perform Regular Audits**: In addition to daily receipt balancing, it is a good idea to compare Transaction Receipts to the register tape to ensure that they match. A periodic review can help you identify potential problems associated with a specific register or sales associate. Remember, it is your responsibility to address inconsistencies and educate your staff.

- **Know Your Third Party Vendors**: If you use software or other services (such as an online "shopping cart") provided by a third party or value-added reseller (VAR), you may be impacted by and financially liable for their security breaches or system failures. Be sure to acquaint yourself with their requirements and limitations so you can minimize disruption in service and protect yourself from unauthorized access. It is your responsibility to ensure that all Cardholder information (including that accessed or maintained by your third party vendor) is stored in an encrypted and secure environment.

ADDITIONAL SERVICES

In addition to the traditional Card services offered, we also provide the following services:

- **Electronic Benefits Transfer Service (EBT)**: A service that allows electronic transfer of government funds to individuals through the use of a plastic debit-like Card and a Personal Identification Number (PIN). The federal government requires all states to distribute food stamps and cash benefits in this manner.

- **Electronic Check Services (ECS)**: A service that allows a Merchant to convert paper-based personal checks into electronic Transactions at the Point-of-Sale, eliminating the need to manually deposit checks at a bank. ECS provides you and your customers with efficient, easy, and secure check processing Transactions.

- **Electronic Gift Card (EGC)**: A program that allows a Merchant to sell Electronic Gift Cards redeemable for in-store merchandise or services. EGC provides customers with another form of payment while also encouraging repeat shopping.

- **SCAN**^{TM}: A check verification service that allows a Merchant to decide whether or not to accept a check at the point-of-sale.

- **Address Verification Service (AVS)**: A fraud-reduction service that allows a Merchant to verify a Cardholder's billing address prior to completing a Card Not Present Transaction.

- **MerchantConnect**: A Web-based Transaction reporting and reconciliation system used to manage Transaction data from multiple locations or multiple merchant accounts via any standard Web browser (e.g., Internet Explorer).

- **Automated Customer Service (ACS)**: A desktop application used as a reporting and accounting reconciliation tool for viewing detailed reports of Transaction activity, statement detail, Card type history, and qualification detail.

- **Dynamic Currency Conversion (DCC)**: A service that allows a Merchant to offer international Cardholders in the United States the option at the point-of-sale to pay in their local currency rather than in U.S. Dollars.

Please contact us if you are interested in any of these services.

NOVA NETWORK

PROCESSING TRANSACTIONS

This chapter explains the two steps involved in the Transaction process – Authorization and Settlement – as well as the different types of Transactions.

AUTHORIZATION

The first step in processing a Transaction is to request Authorization from the Issuer to accept a Card for payment. An Authorization request is made via one of the following two methods:

◆ **Electronic Authorization**: The Merchant swipes a Card through the POS Device (or manually enters the Card number) and the POS Device sends the Transaction information electronically to the Issuer for Authorization.

◆ **Voice Authorization**: The Merchant calls the Voice Authorization Center, which then communicates the Transaction information electronically to the Issuer. An operator or an interactive voice response (IVR) unit provides the Merchant with the Authorization Code given by the Issuer. Voice Authorization toll-free telephone numbers are located on a sticker on your POS Device. If there is not a Voice Authorization sticker on your POS Device, call Merchant Services.

Most Authorizations are requested electronically. However, if a Merchant does not have a working POS Device, or if the Issuer requests additional information, Voice Authorization can be used.

An Authorization request is required for every Transaction as it determines if:

◆ The Card number is valid

◆ The Card has been reported lost or stolen at the time of the Transaction

◆ Sufficient credit or funds are available for the Transaction

NOVA NETWORK

Receipt of an Approval Code in response to an Authorization request
does not:

◆ Guarantee that the Merchant will receive final payment for a
Transaction

◆ Guarantee that the Cardholder will not later dispute the
Transaction (Card Transactions are subject to Chargebacks even
when an Approval Code has been obtained.)

◆ Protect you from Chargebacks for unauthorized Transactions or
disputes regarding the quality of goods and services

THE ELECTRONIC AUTHORIZATION PROCESS

To understand the electronic Authorization process, refer to the
diagram below and review the following steps.
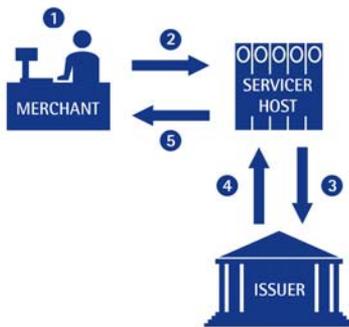
1. **Authorization of Purchase**: The Transaction process begins
when a Cardholder wants to buy goods or services using a Card.
Before the Transaction can be completed, the Merchant must
receive an Approval Code from the Issuer.
2. **Servicer Host**: The Merchant's POS Device sends the Transac-
tion data to the Servicer Host to verify the Merchant ID number,
to read the Card number, and to route the information to the
appropriate Issuer.
3. **Issuer**: The Servicer Host sends the information to the Issuer
through the Visa or MasterCard network, or directly to other
Issuer networks (e.g., American Express, Discover). The Issuer
determines whether the Transaction should be approved and

NOVA NETWORK

sends one of the following responses back to the Servicer, who then forwards it to the Merchant:

◆ **"Approval Code"**: Indicates credit or funds are available to complete the sale and that the Card has not been reported lost, stolen, or otherwise invalid. The Merchant may complete the Transaction.

◆ **"Declined Code**": Indicates that the Issuer does not approve the Transaction. The Merchant should ask for another form of payment.

◆ **"Declined Pick-Up"**: Indicates the Issuer does not approve the Transaction and requests that the Card not be returned to the Cardholder. The Card should be cut lengthwise without damaging the Magnetic Stripe and sent, along with the MID, Merchant address, and the date of the incident to:

> Exception Processing
> ATTN: Card Pick Up
> NOVA Information Systems, Inc.
> 7300 Chapman Highway
> Knoxville, TN 37920

◆ **"Referral" or "Call Auth"**: Indicates the Issuer is requesting the Merchant to call the Voice Authorization Center, which will either provide an Approval Code or ask the Merchant to request additional information from the Cardholder (e.g., mother's maiden name). The Voice Authorization Center will provide this information to the Issuer who will either approve or decline the Transaction.

4. **Servicer Host**: The Servicer Host receives the response from the Issuer and routes it to the Merchant.

5. **Merchant**: The Merchant receives the Issuer's response from the Servicer Host and follows the appropriate steps to complete the Transaction.

SETTLEMENT

The final step in processing a Transaction, which is Settlement, occurs when the Merchant sends all of its Card Transactions to us to receive payment. This step only occurs after a Transaction is approved. It includes paying the Merchant for the Transactions and billing the Cardholder for the Transactions.

> This process could take two or more business days, excluding holidays, unless you are set up on delayed funding.

Refer to the diagram below and review the following steps to better understand the Settlement process.
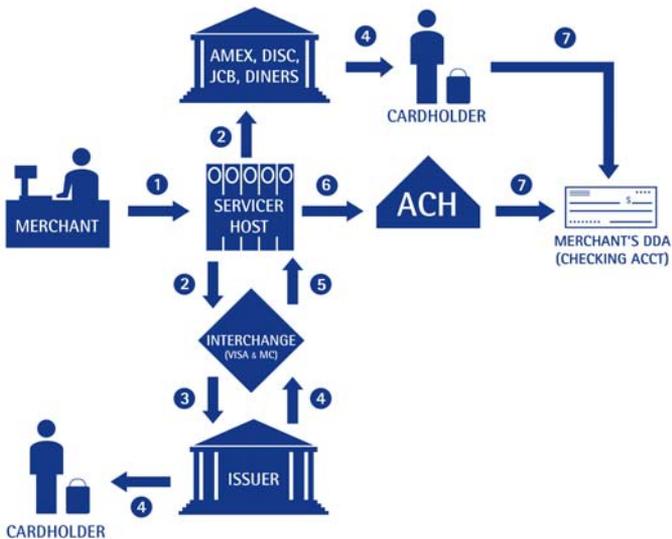
PAYING THE MERCHANT FOR TRANSACTIONS

1. **Merchant**: At the close of business, the Merchant sends all of the Transactions in their POS Device (known as a Batch) to the Servicer Host to close or settle the Batch.

NOVA NETWORK

2. **Servicer Host**: The Servicer Host sends Visa and MasterCard Card Transactions to Interchange and other Card Transactions to the appropriate Issuer (e.g., American Express Transactions to American Express). If the Transactions are not sent to Interchange, go to step 4.

3. **Interchange**: The Interchange identifies the Issuer to which the Transaction data is to be transmitted, and then sends the Transaction data to the appropriate Issuer.

4. **Issuer**: The Issuer posts the Transaction to the Cardholder's account.

    The Issuer either sends to Interchange the difference between the Transaction amount and the Interchange fee charged to the Servicer, or sends the funds to the Merchant's DDA (see step 7).

5. **Interchange**: Sends the difference between the Transaction amount and the Interchange Fees to the Servicer Host.

6. **Servicer Host**: Sends a message to the Automated Clearing House to pay the Merchant for the Transactions.

7. **Automated Clearing House (ACH)**: Electronically sends the funds from us to the Merchant's DDA. Fees are debited from the Merchant's DDA on a monthly or daily basis.

TRANSACTION PROCESSING PROCEDURES

Follow these guidelines when you process Transactions:

◆ Keep the Card in your hand until you complete the Transaction—the Card is required in several Transaction processing steps.

◆ If your POS Device displays "Referral" or "Call Auth" during a Transaction, call your toll-free Voice Authorization telephone number (located on a sticker on your Terminal) and follow the instructions.

◆ If you receive an Approval Code, but are still suspicious about the Cardholder, Card, or circumstances of the Transaction, call for a Code 10 Authorization and follow the instructions. Refer to Chapter 5, *Code 10 Procedures*, for additional information.

◆ Use a ballpoint pen for steps that require handwritten information. Never use a marker or a pencil to write on a Transaction Receipt.

◆ Do not write additional information (e.g., Cardholder's telephone number, address, driver's license number, Social Security number) on any Transaction Receipt.

To process a Transaction, follow these steps:

1. **Make Sure the Card is Valid**. Check the Card's expiration date to ensure that it has not expired and that it is not being used before it becomes valid. Additional loss prevention information can be found in Chapter 4, *Preventing Card Fraud*.

2. **Swipe the Card Through the POS Device**. If the Card is successfully swiped, the POS Device may prompt you to enter the last four digits of the Card number. This process compares the account number in the Magnetic Stripe with the account number embossed on the Card.

   If the POS Device cannot read the Magnetic Stripe, press the appropriate key on your POS Device to initiate a Transaction. When you are prompted by the POS Device, enter the Card number embossed on the front of the Card, as well as the expiration date. Make an Imprint of the Card on a paper Transaction Receipt to prove that the Card was present during the Transaction. Keep the Imprinted receipt with the electronically printed Transaction Receipt from the POS Device.

   Ensure that the paper Transaction Receipt contains all of the information related to the Transaction, such as the Transaction amount, signature, Transaction Date, Merchant information, and Authorization Code.

3. **Enter the Amount of the Transaction**. When prompted by the POS Device, enter the amount of the Transaction using the numeric key pad on your POS Device. You do not need to include a decimal point.

   Example:

   A Transaction for $125.00 would be entered by pressing the **1**-**2**-**5**-**0**-**0** keys consecutively, and then pressing the **ENTER** key.

   The POS Device will display a message that indicates when the Transaction is being processed for Authorization.

4. **Obtain the Authorization Code**. If the Transaction is approved, your POS Device will display an Approval Code when a printer is not present. If the POS Device has a printer, the Transaction Receipt is printed. If you have to Imprint the Card, remember to record the Approval Code on the Transaction Receipt.

If the Transaction is declined, the POS Device will display "Declined" or "Declined—Pick-Up". In these cases, you should ask for another form of payment.

If the POS Device displays a "Referral" or "Call Auth" message, call the toll-free Voice Authorization telephone number (located on a sticker on your Terminal) and follow the instructions. If you receive an Approval Code, you must enter it into your POS Device to complete the steps for processing the Transaction. If Authorization is declined, the Voice Authorization Center may ask you to retain the Card. If this occurs, follow the instructions. A reward may be paid for the return of a Card at the Voice Authorization Center's request.

5. **Have the Cardholder Sign the Transaction Receipt, and then Compare Signatures**. Compare the signature on the Transaction Receipt with the signature on the back of the Card. If you cannot tell whether the signatures are similar, ask to see another form of identification and compare the second signature with the others. You may also compare the appearance of the Cardholder with the picture on the identification cards. If you are still suspicious of the Transaction or the Cardholder, you may opt to perform a Code 10 Authorization.

6. **Return the Card and the Customer Copy of the Transaction Receipt to the Cardholder**. When the Transaction is complete, return the Card to the Cardholder, along with the customer copy of the Transaction Receipt. Make sure to keep the Merchant copy of the Transaction Receipt for your records.

TRANSACTION RECEIPTS

A Transaction Receipt is a paper or electronic record of the purchase of goods or services from a Merchant by a Cardholder using a Card. You must provide the Cardholder with a Transaction Receipt for their personal records.

Transaction Receipts are required for all Transaction types and must be retained for a minimum of eighteen (18) months. Transaction Receipts should also be stored in a secure and safe area, organized in chronological order by Transaction Date.

ELECTRONIC TRANSACTION COMPONENTS

The Merchant must ensure that the Cardholder's Transaction Receipt
contains the following information:

◆ Transaction Date
◆ Total Transaction amount
◆ Card account number (must be truncated on the Cardholder copy)
◆ Cardholder signature
◆ Authorization Code
◆ Merchant name and location
◆ Terminal or Merchant Identification Number
◆ Special return or refund terms printed in close proximity to the
   Cardholder signature line on the Transaction Receipt

MANUAL TRANSACTION COMPONENTS

A properly produced manual Transaction Receipt must contain the
following:

◆ Imprint of the Card (not a photocopy)
◆ Identification of the Transaction type (sale, credit/refund, etc.)
◆ Transaction Date
◆ Total Transaction amount
◆ Cardholder signature
◆ Authorization Code
◆ Merchant name and location
◆ Terminal or Merchant Identification Number
◆ Description of the merchandise
◆ Special return or refund terms printed in close proximity to the
   cardholder signature line on the Transaction Receipt
◆ Salesperson's initials or department number

DELIVERY OF TRANSACTION RECEIPTS

The Merchant must provide a complete and legible copy of the
Transaction Receipt to the Cardholder in the following manner:

◆ **Card Present Transactions**: Provide the Transaction Receipt to
   the Cardholder at the time of the Transaction.

NOVA NETWORK

◆ **Card Not Present Transactions**: Provide the Transaction Receipt to the Cardholder in either electronic (e.g., e-mail or fax) or paper (e.g., handwritten or Terminal-generated) format. Electronic Commerce Transactions must not include the Cardholder's account number.

CARD NOT PRESENT TRANSACTIONS

Card Not Present Transactions—Mail Order (MO), Telephone Order (TO), and Electronic Commerce (EC) Transactions—occur when the Card is not physically presented to the Merchant at the time of a sale. You must be authorized by us to process Card Not Present Transactions.

If more than 20% of your Transactions are MO/TO, you must apply for a separate Merchant Identification Number (MID) for those Transactions. If more than 1% of your Transactions are Electronic Commerce orders, you must also apply for a separate Merchant Identification Number for those Transactions.

Before you begin to process Card Not Present Transactions, note these general guidelines:

◆ **Use a ballpoint pen when handwritten information is required**. Never use a marker or pencil when writing on a Transaction Receipt.

◆ **Obtain the following information from the Cardholder, if needed**:

- ◆ Cardholder's billing address
- ◆ Shipping address, if different from billing address
- ◆ Cardholder's telephone number
- ◆ CVV2/CVC2/CID number

This data element must not be retained beyond use in the original authorization request, must not be printed on the Transaction Receipt or any other document provided to the Cardholder, and must not be otherwise retained in the Merchant's internal reports.

- ◆ Cardholder's account number
- ◆ Card expiration date

NOVA NETWORK

◆ **Do not settle a Transaction before shipping the goods**. This
increases the risk of a Chargeback to the Merchant and is
prohibited by the Agreement.

◆ **Do not retain magnetic stripe data except for first time use**.

Card Not Present Transactions pose a higher risk of fraud and
Chargebacks, so it is important that you take precaution in processing
these Transactions. Follow these steps **prior** to processing a Card Not
Present Transaction, as applicable.

MANUAL TRANSACTION RECEIPTS

Follow these steps for manual transaction receipts:

1. **Write the Cardholder's Name and Card Number on the
   Transaction Receipt**. Refer to the *Electronic Transaction Com-
   ponents* section on page 14 for information on what is required on
   Transaction Receipts. On a manual Transaction Receipt you may
   record the full Card Number and the expiration date. Record in
   your records the Cardholder's billing address (and shipping
   address, if different) and telephone number. You must not record
   CVV2/CVC2/CID data elements on the manual Transaction
   Receipt.
2. **Record the Order Type on the Transaction Receipt**. Write one
   of the following on the signature line of the Transaction Receipt:

   ◆ "Mail Order"
   ◆ "Telephone Order"
   ◆ "Internet"

POS DEVICE GENERATED RECEIPTS

If you are using a POS Device, enter the Transaction into the device
by following these steps:

1. **Press the appropriate key on your POS Device to initiate a
   Transaction**.
2. **When prompted, enter the Card number**.
3. **When prompted again, enter the Card expiration date**.
4. **Finally, when prompted, enter the Transaction amount**. See
   the *Transaction Receipts* section on page 13 for more informa-
   tion.

5. **Record the Authorization Code on the Transaction Receipt**. Refer to the *Transaction Receipts* section on page 13 for details on recording the Authorization Code.

There are services available that can assist you in making a more informed decision on whether to process a Card Not Present Transaction. The use of CVV2/CVC2/CID and AVS can lessen your risk of Chargebacks by providing you with additional information to assist with your decision on whether or not to process a Card Not Present Transaction.

The use of CVV2/CVC2/CID and AVS will not relieve you of liability for Chargebacks. Remember, you bear the risk of loss associated with any Chargeback.

If you are using these services, follow the next two steps **prior** to processing a Transaction.

1. **Verify the Card Validation Code (CVV2/CVC2/CID) Printed on the Front or Back of the Card (at the end of the account number in the signature panel), as applicable to the specific Card type**. If your POS Device is set up for CVV2/CVC2/CID and if the CVV2/CVC2/CID number is provided at the time of Authorization, either a "match" or a "no match" response will be provided by the Issuer. A "match" response means it is more likely that the Card is present and in the hands of the Cardholder at the time of the Transaction. A "no match" response means you should consider whether or not to process the Transaction. The decision to process a Transaction, regardless of the response received, is up to you, because you are responsible for any risk associated with processing a Transaction.

You must not retain the CVV2/CVC2/CID data element beyond the original authorization request. Further, the CVV2/CVC2/CID data element must not be printed on the Transaction Receipt nor on any document given to the Cardholder, nor otherwise retained in the Merchant's internal records.

Most customers do not know where the CVV2/CVC2 code is located. To assist a customer, have them locate the last three (or four) alphanumeric characters in the signature panel on the back or the front of their Card for Visa or MasterCard Card types. (In the Glossary see "Card Identification Number (CID)" for more information on other Card types.)

> Refer to the *Unique Card Characteristics* section on page 34 for more details concerning the Card Validation Code.

2. **Verify the Cardholder's Address by Using the Address Verification Service (AVS)**. If your POS Device is set up for AVS, it will prompt you to enter the numeric portion of the Cardholder's billing address and the five digit zip code to verify that the individual providing the Card account number is the Cardholder. A result code is generated indicating whether the address given by the Cardholder matches (exactly, partially, or not at all) the address that the Issuer has on file for the Card. A response of "exactly" means it is more likely that the Card is being used by the authorized Cardholder. A "partially" or "not at all" response means you should consider whether or not to process the Transaction. The decision to process a Transaction, regardless of the response received, is up to you, as you are responsible for any risk associated with processing a Transaction.

> For more information about CVV2/CVC2 and AVS, contact Merchant Services.

If you need more information about processing Card Not Present Transactions, you may contact the following resources:

◆ MC (MasterCard) Assist: (800) 622-7747
◆ Visa's Merchant Assistance Service: (800) 847-2750

NOVA NETWORK

◆ American Express: (800) 528-2121
◆ Discover Business Services: (800) 347-1111

These resources allow you to verify a Cardholder's address and to obtain the Issuer's telephone number.

PAPER DRAFTS

To process paper drafts, you must maintain a supply of materials to execute your Transactions. As part of our service, we will supply you with the materials and forms that you need to process Visa or MasterCard Transactions.

It is important to keep copies of your Transaction Receipts in a safe place, filed by Transaction Date. This is especially important for quickly locating a receipt if questions arise.

Before you process a paper draft, please note the following guidelines:

◆ Keep the Card in your hand until you complete the Transaction—the Card is required in several steps when processing a Transaction.

◆ After receiving an Approval Code, call for a Code 10 Authorization if the Cardholder, Card, or circumstances of the Transaction seem suspicious. Once connected, follow the instructions. Refer to Chapter 5, *Code 10 Procedures*, for more information.

◆ Use a ballpoint pen when handwritten information is required. Never use a marker or pencil when writing on a Transaction Receipt.

To correctly process a paper Transaction, follow these steps:

1. **Make Sure the Card is Valid**. Check the Card's expiration date to ensure that it has not expired and that it is not being used before it becomes valid. Loss prevention information can be found in Chapter 4, *Preventing Card Fraud*.

2. **Imprint the Transaction Receipt**. Make a legible Imprint on all copies of the Transaction Receipt.

3. **Call for Authorization**. When you call for Authorization, please have the following information available:

   ◆ Card number
   ◆ Merchant Identification Number (MID)

◆ Amount of sale (dollars and cents)
◆ Card expiration date

4. **Write the Approval Code in the Space Provided on the Transaction Receipt**. The Approval Code is required.
5. **Ask the Cardholder to Sign the Transaction Receipt**. Hold the Card in your hand while you watch the Cardholder sign the Transaction Receipt.
6. **Compare the Signature on the Card to the Cardholder's Signature on the Transaction Receipt**. If you cannot tell whether the signatures are similar, ask to see another form of identification and compare the second signature with the others. You may also compare the appearance of the Cardholder with the picture on the identification cards. If you are still suspicious of the Cardholder, the Card, or the circumstances of the Transaction, you can perform a Code 10 Authorization.
7. **Return the Card and the Cardholder Copy of the Transaction Receipt to the Cardholder**. When the Transaction is complete, return the Card to the Cardholder, along with the Cardholder copy of the Transaction Receipt. Make sure to keep the Merchant copy of the Transaction Receipt for your records.

RECURRING PAYMENTS AND PRE-AUTHORIZED ORDERS

Recurring Payments are Transactions for which a Cardholder provides written permission or electronic authorization to a Merchant to periodically charge their Card for recurring goods or services (e.g., monthly membership fees, utility bills, or subscriptions). When processing Recurring Payments, you must obtain a separate Authorization Code for each Transaction.

Pre-authorized Orders are Transactions in which the Cardholder provides written or electronic authorization to charge their Card, one or more times, at a future date. You must be authorized by us to process Pre-authorized Orders.

To perform a Pre-authorized Order, follow these specific guidelines:

◆ Separately authorize each Transaction for the exact amount of that Transaction, instead of authorizing the entire amount of all the Transactions or no amount at all.

NOVA NETWORK

◆ If applicable to the Transaction, write the words "Delayed Delivery," and "Deposit" or "Balance" on the Transaction Receipt. The Authorization date and Authorization Code must also be printed on the Transaction Receipt.

◆ While you may process the Transaction for the "Deposit" before delivery of the goods and/or services, you may not process the "Balance" of the Transaction until the goods and/or services are delivered.

You must obtain a signed order form or other written agreement with the Cardholder for all Recurring Payments and Pre-authorized Orders. The order form or agreement must contain the following information:

◆ Card number
◆ Card expiration date
◆ Cardholder's name
◆ Cardholder's signature
◆ Transaction amount (charged to the Cardholder's Card)
◆ Charge frequency (weekly, monthly, etc.)
◆ Length of time over which the recurring charges will occur
◆ The words "Recurring Payment" or "Pre-authorized Order" written on the signature line of the Transaction Receipt

You must keep a copy of the order form or written agreement for the duration of the recurring service. You must also provide a copy of the order form or agreement for Recurring Payments or Pre-authorized Orders to us upon request. A new order form or written agreement with the Cardholder is needed when a Recurring Payment is renewed.

QUASI-CASH TRANSACTIONS

Quasi-Cash Transactions represent a Merchant's sale of items that are directly convertible to cash. Examples of Quasi-Cash Transactions include:

◆ Casino gaming chips
◆ Money orders
◆ Deposits
◆ Wire transfer money orders
◆ Travelers cheques (if not processed as a cash disbursement)

NOVA NETWORK

◆ Travel money cards (if not processed as a cash disbursement)

◆ Foreign currency (if not processed as a cash disbursement)

You must be authorized by us to process Quasi-Cash Transactions.

ACCEPTANCE AND ADDITIONAL REQUIREMENTS

In addition to general Transaction Receipt requirements (see the *Transaction Receipts* section on page 13), Merchants processing Quasi-cash Transactions need to:

◆ Review identification (such as a valid passport or driver's license) to validate the Cardholder's identity.

◆ Record the type of identification presented by the Cardholder on the Transaction Receipt, along with the serial number, expiration date, and Cardholder name (if different than the embossed name) and address.

◆ Record the printed four digits from the face of the Card (found above or below the embossed account number) on the Transaction Receipt. Refer to Chapter 4, *Preventing Card Fraud*, for more details.

◆ Compare the first four digits of the account number on the printed Transaction Receipt with the first four digits of the embossed account number. If they do not match, decline the Transaction and attempt to recover the Card (reasonably, lawfully, and peacefully), while also noting a description of the Cardholder.

RETURNS AND EXCHANGES

Refunds for a Transaction must be processed by issuing a credit to the Card on which the original purchase was made. You must also prepare a Credit Transaction Receipt for the amount of credit issued.

Do not issue a credit by giving the Cardholder cash (or a check) if the original purchase was made by Card. Also do not credit a Card if the original purchase was made by cash or check.

If you have a special policy regarding returns or refunds, make sure that the policy is:

◆ Clearly posted at the point-of-sale

◆ Printed on the Transaction Receipt using letters approximately ¼ inch high and in close proximity to the signature line

If you are processing an even exchange, no action is necessary. However, if an exchange involves merchandise of greater or lesser value, you must issue a Transaction Receipt or a Credit Transaction Receipt for the difference. If you prefer, you may instead give a full refund to the Cardholder for the original Transaction amount and process the exchange as a new Transaction.

NOVA NETWORK

SETTLING DAILY TRANSACTIONS

This chapter describes how to settle your daily Transactions. The guidelines for Settlement can help you:

◆ Eliminate balancing errors
◆ Promptly record deposits to your DDA
◆ Prevent duplicate billing to customers
◆ Minimize Chargebacks

SETTLING THE DAILY BATCH

To settle the daily Batch, perform the following steps:

1. **Total the day's Transaction Receipts and Credit Transaction Receipts**.
2. **Verify that the Transaction Receipts equal the POS Device totals**. You may print a report from your POS Device to assist you with balancing. For more information about balancing, refer to the instructions that came with your POS Device.

   If the totals do not balance, then:

   ◆ Compare the Transaction Receipts to the individual entries in the POS Device
   ◆ Make any necessary adjustments before transmitting or closing the Batch. To make adjustments, refer to the instructions for your POS Device

3. **Close the Batch according to the instructions for your POS Device**.

PAPER DEPOSITS

If you are not using a POS Device, you must deposit Visa and MasterCard Transaction Receipts or Credit Transaction Receipts

NOVA NETWORK

within three (3) business days. Please include a Batch Header with your Transaction Receipts.

PREPARING PAPER DEPOSITS

To prepare a paper deposit, follow these steps:

1. **Place your Merchant Identification Card and the Batch Header in the Imprinter**.
2. **Imprint the information onto the Batch Header**.
3. **Enter the total number of Transaction Receipts and their dollar amount**. It is not necessary to separate the Visa and MasterCard Transaction Receipts.
4. **Enter the total number of Credit Transaction Receipts and their total dollar amount**.
5. **Review the Transaction Receipts and Credit Transaction Receipts to make sure they bear legible Visa or MasterCard numbers and amounts**. Visa uses 16-digit account numbers beginning with a "4" and MasterCard uses 16-digit account numbers beginning with a "5."
6. **Enter the net amount of the Transaction Receipts and the Credit Transaction Receipts**.
7. **Fill in the date and your DDA (Demand Deposit Account) number**.
8. **Place the bank copy of all Transaction Receipts and Credit Transaction Receipts behind the Batch Header and insert them into the Merchant deposit envelope, which is addressed to the paper processing center**. If you need additional Merchant deposit envelopes, please call Merchant Services.
9. **Retain a copy of the Batch Header, along with your copies of the Transaction Receipts and Credit Transaction Receipts for your records**.
10. **Make sure the paper processing center address is on the front of the envelope**.
11. **Mail the Merchant deposit envelope**.

ADJUSTMENTS

If we detect an imbalance between your Batch Header and the attached Transaction Receipts we will make an adjustment to your DDA and send you an adjustment notice. Remember, adjustments

NOVA NETWORK

differ from Chargebacks. If you have any questions concerning an adjustment, contact Merchant Services.

The most common reasons for adjustments include:

◆ The Transaction Receipts received do not match the amount shown on the Batch Header.

◆ A Card number is invalid or illegible. To receive credit, you must correct the number and resubmit the Transaction Receipt with a new Batch Header.

◆ Your DDA was credited in error or has been debited to reflect a Negative Deposit.

Remember to reconcile your monthly Merchant Statements with your DDA statement, along with any adjustment notices you may have received.

NOVA NETWORK

PREVENTING CARD FRAUD

It is important to take steps to educate yourself and your staff in order to reduce your risk of accepting a counterfeit or fraudulent Card Transaction. Remember that you are responsible for all Chargebacks, including those for fraudulent Transactions. A fraudulent Card sale could involve an invalid account number or a valid number presented by an unauthorized user (the most common form of fraud). Fraud normally occurs within hours of the loss, theft, or compromise of the Card number or Card, and before most victims report the Card missing or discover the compromise.

If you receive an Approval Code but suspect a Card has been altered or is counterfeit, call the Voice Authorization Center and request a Code 10 Authorization (see Chapter 5, *Code 10 Procedures*). If the Transaction is declined, do not request a Code 10 Authorization and do not complete the Transaction.

The following sections provide tips to assist you in protecting yourself against fraud losses.

IDENTIFYING SUSPICIOUS CUSTOMER ACTIONS

Common sense is the best guide for spotting suspicious behavior. Be sure you combine watchfulness with proper Card identification and validation techniques.

Be aware of customers who:

- Make indiscriminate large dollar purchases without regard to size, color, style, or price
- Question the sales clerk about credit limits or the Authorization process
- Attempt to distract the sales clerk (e.g., continually delay selections or talk continuously)

◆ Hurry a clerk at quitting time

◆ Purchase a high-ticket item, such as a wide-screen HDTV monitor or other large item and insist on taking it immediately, rather than having it delivered—even when delivery is included in the price

◆ Buy a high-ticket item and request that it be sent next day air or request for someone else to pick up the purchase at a later time

◆ Pull a Card from a pocket rather than a wallet

◆ Sign the Transaction Receipt in a deliberate or unnatural manner

◆ Appear too young to make purchases with a Card

◆ Buy clothing without trying it on for size or decline alterations that are included in the price

◆ Charge expensive items on a newly valid Card

◆ Do not have a driver's license, tell you that their driver's license is in the car, or provide only a temporary license without a photo

◆ Do not ask questions on major purchases

◆ Make purchases, leave the store, and return to make more purchases

◆ Make purchases just after the store opens or just before it closes

◆ Use a Card belonging to a friend or relative

◆ Ship purchases to an address outside of the U.S.

◆ Recite the Card number from memory, rather than presenting the Card itself

◆ Ask to see the Card again before signing the Transaction Receipt

IDENTIFYING SUSPICIOUS CARD NOT PRESENT TRANSACTIONS

The increased use of Electronic Commerce, mail, and telephone orders has given rise to an increasing amount of fraud. If you accept Card Not Present Transactions, take caution if a customer attempts to:

◆ Use more than one Card for any given purchase (also known as a "Split Ticket")

◆ Use Cards that have sequential numbers or patterns

◆ Place an unusually large or uncommon order compared to your typical Transactions

◆ Use a Card issued by a foreign bank along with one of the other actions within this list
◆ Request delivery to a post office box
◆ Request delivery to a foreign country
◆ Utilize phone relay service where the Cardholder does not speak directly to the Merchant

> If you receive an order for a large purchase for delivery to a foreign country or to a freight forwarder, we recommend that you contact your Voice Authorization Center to request a Code 10 specifically identifying the Transaction as a large foreign shipment transaction.

◆ E-mail purchase orders that involve multiple Card accounts in which each order includes the same product and dollar amount. This is sometimes common for Transactions resulting in foreign Card fraud
◆ Place an order and then call back to place subsequent orders using the same or different Cards

You should be particularly careful if you sell products that are easily resold. For example, computers and computer equipment, printer cartridges, and jewelry are more susceptible to fraud than perishable items such as food – although criminals can victimize virtually any type of business.

IDENTIFYING VALID CARDS

Cards share similar qualities to help identify their validity, and there are anti-fraud safeguards unique to each Card brand.

CARDS AND SIGNATURES

You should not accept a Card that is not signed. Many Card users are writing "Use other ID" (or something similar) in the signature panel because they believe it provides a higher level of security. Actually, this is not true – it simply allows thieves to sign their own name or to use a fake ID with any signature.

If an unsigned Card is presented to you:

NOVA NETWORK

1. Inform the customer that the Card must be signed.
2. Have the customer sign the Card in your presence and provide a current, valid government ID that has been signed (such as a passport or driver's license). Do not accept a temporary form of ID, such as a temporary driver's license that does not have a photo.
3. Compare the signature on the ID to that on the Card.
4. If the customer refuses to sign the Card, do not complete the Transaction. Remember, you are liable for any Transaction processed with a fraudulent Card.

CARD PROCESSING TIPS

After swiping a Card, the POS Device prompts you for specific information. The POS Device may also prompt you to enter the last four digits of the account number to verify that the embossed account number matches the number on the Magnetic Stripe (on the back of the Card). If the numbers do not match, the POS Device indicates a mismatch of the digits or an invalid Card. Do not accept the Card.

Once you receive an Approval Code, verify that the Card number on the Transaction Receipt matches the number embossed on the Card. If it does not match, do not accept the Card.

Characteristics of Most Cards

These characteristics typically apply to most Card brands.

◆ **Overall Card Quality**: A Card may be any color (but never faded or washed out) or feature a background pattern or photograph. The Card's edge should be smooth and clean, never rough. The print should be crisp and clear.

◆ **Matching Account and BIN Numbers**: An identical series of numbers, known as the Bank Identification Number (BIN), is printed directly above or below the first four embossed numbers on the Card and in the signature panel.

◆ **Embossing Quality**: A hot iron is sometimes used to smooth embossed numbers and then emboss new numbers. When this is done, the numbers can appear irregular in spacing or in vertical alignment, or there can be a slight "halo" around the numbers. This technique is also used to modify the expiration date, so check both the month and the year for alterations. See *Examples of Tampering* on page 39 for specific illustrations.

◆ **Hologram Quality**: An authentic Hologram should reflect light and change in appearance as you move the Card. It should barely catch your fingernail, but should not be such that you can peel it off. A fake Hologram is often a sliver of tin foil lacking the features of an authentic Hologram.

◆ **Embossing Within the Hologram**: The last four Card numbers should be embossed numbers within the Hologram itself, or should at least partially overlap it (applies to Visa, MasterCard, and Discover Card products).

◆ **Account Number and CVV2/CVC2/CID Code**: The signature panel on the back of the Card should include either the entire Card number or its last four digits, followed by the CVV2/CVC2/CID code. These numbers should be printed in reverse italics and should match the embossed numbers.

◆ **Signature Panel Quality**: The signature panel should not be defaced (e.g., peeled-off white plastic, smudged imprinting, or "void" appearing in the signature panel). See the *Examples of Tampering* section on page 39 for specific illustrations.

◆ **Signature Panel Print Design**: With the exception of some ATM Cards and various store-branded Cards, signature panels are seldom plain white.

UNIQUE CARD CHARACTERISTICS

This section provides Card design elements specific to the listed Cards.

MASTERCARD

MasterCard uses the same basic design elements on nearly all of their Card types.

Figure 4-1: MasterCard Characteristics

1. **Embossed Account Number & Printed Four Digit Number**: All MasterCard accounts begin with a "5" and have 16 digits. The four digit number must be printed below the embossed account number and must exactly match the first four numbers of the embossed account number.
2. **MC Security Characters**: Known as the "flying MC," these characters appear on the lower right portion of the Card's front. The letters are a special shape and must never appear as a plain typeface or as characters from a typewriter.
3. **Twin Globes**: This is a three-dimensional Hologram with inter-locking globes ("Twin Globes") which reflect light and appear to move as you rotate the Card. The word "MasterCard" is printed repeatedly in the background of the Hologram, and the letters "MC" are micro-engraved around the two rings.

4. **Signature Panel**: Contains a repetition of the word "Master-Card", in alternating blue, yellow, and red colors, all at a 45 angle, and also includes the account number followed by the CVC2 code in reverse italics.

VISA

Visa uses the same basic design elements on nearly all of their Card types.

Figure 4-2: Visa Card Characteristics

1. **Embossed Account Number & Printed Four Digit Number**: All Visa embossed account numbers begin with a "4" and have 16 digits. All digits must be clear, even, and the same size and shape. The four digit number must be printed below the embossed account number and must exactly match the first four numbers of the embossed account number.
2. **Flying Dove Hologram**: All Visa Cards include the "flying dove" Hologram. The dove should appear to fly when you tilt the Card back and forth.
3. **"Good Thru" (or "Valid Thru") Date**: Identifies the expiration date of the Card and is located below the embossed account number. If the Transaction Date is after the Good Thru date, the Card is expired.

4.   **Flying "V"**: This is an embossed security character located next to the Good Thru date. If the "V" is not italicized or is missing, the Card is counterfeit.

5.   **VISA Logo**: The logo has a fine print (micro-print) around its border that is barely readable without magnification. If the actual words are difficult to read (even with a magnifying glass), they should at least appear as a thick dotted or dashed line.

6.   **Signature Panel**: Includes a white background with the word "VISA" repeated in a diagonal pattern in blue and gold print. The Card account number should be printed within the panel. If the word "Void" appears within the panel, someone has tried to erase the signature. In this case, do not accept the Card.

7.   **CVV2 Value**: A three-digit code located within the signature panel to the right of the printed account number. This value assists Card Not Present Merchants in validating that a customer has the Card in his or her possession, and that the Card is valid.

AMERICAN EXPRESS

Common features exist on American Express Card types.

Figure 4-3: American Express Card Characteristics

These include:

1.   **Non-transferable**: Only the person whose name is embossed on the Card is entitled to use it.

2. **The Centurion Portrait**: This image is printed with a high degree of clarity and detail similar to that on U.S. currency. When examined under an ultraviolet light, the letters "AMEX" and a phosphorescence in the portrait of The Centurion become visible.

3. **Card Identification Number (CID)**: The CID is a four-digit, non-embossed number printed above the account number on the front of the Card. This number is an additional form of security, as it assures a Card's validity.

4. **Account Number:** Located on the front and back of the Card, the American Express account number always begins with "37" and has 15 digits.

5. **Valid Thru & Member Since Dates**: Identifies the expiration date of the Card, as well as the year the Card was issued to the Cardholder.

6. **Signature Panel**: Contains a set of wavy lines that, if tampered with, appear smudged.

7. **Card Member Agreement Statement**: A statement by American Express that provides the Merchant the right to "pick up" a Card at any time.

NOVA NETWORK

DISCOVER

Discover Cards contain the same characteristics. These include:
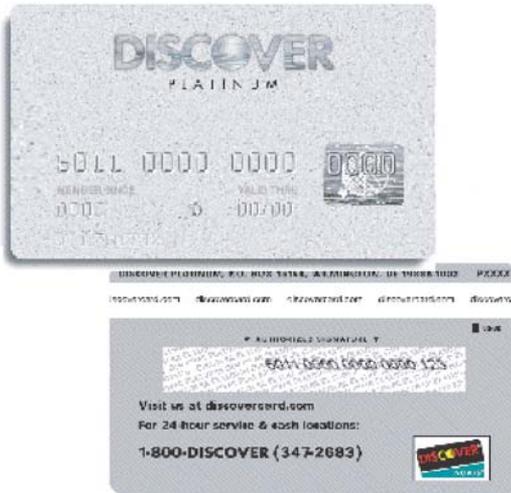
Figure 4-4: Discover Card Characteristics

1. **Embossed Account Number**: Each Discover account number contains 16 digits beginning with "6011". The embossed account number should match the account number in the signature panel and on the Magnetic Stripe located on the back of the Card.
2. **Embossed Letter**: Displays one of two special embossed characters ("n" or "D") on the Member Since and Expiration Date information line. All Cards issued after October 2003 display the "D" character.
3. **DISCOVER**: Appears on the front of the Card when held under an ultraviolet light. Until October 2005, some Cards will display "NOVUS"; all Cards issued after that date will display "DISCOVER".
4. **Hologram**: Displays one of four distinct images.
5. **Repetitive Fine Line Printing**: The name shown on the top face of the Card (e.g., "DISCOVER Card", "Private Issue", etc.) also appears in repetitive fine line printing on the back of the Card (or on both sides for some Cards).
6. **Signature Panel**: Depending on the issue date for a Card, displays an overprint pattern on the signature panel that reads "NOVUS" or the name of the Card (i.e., "DISCOVER", "DIS-

NOVA NETWORK

COVER PLATINUM", etc.) and an underprint of "VOID". This panel also contains the account number followed by the CID, which is a three-digit validation number, both in reverse italics.

EXAMPLES OF TAMPERING

The following section identifies common Card tampering techniques. Although an American Express Card is used in the examples, these tampering methods are widespread among all Card types.

FRAUDULENT EMBOSSING

- The black ink on the card number or cardholder name is smudged or messy
- The embossed numbers are crooked, out of line, or unevenly spaced
- The typeface of the account number does not match the rest of the card typeface
- The card number embossed on the front does not match the number imprinted on the back

ALTERED MAGNETIC STRIPE

- The card number on the printed receipt does not match the number embossed on the front of the card or imprinted on the back
- The name printed on the receipt does not match the name embossed on the card
- The magnetic stripe is deliberately scratched or altered making it necessary to manually key the account number
- The signature panel has been whited out, taped over or erased

IDENTIFYING SUSPICIOUS EMPLOYEE ACTIONS

Be aware – not all Card fraud is committed by customers. Sometimes employees:

- **Record Card Numbers**: Employees may pocket receipts left behind by Cardholders or may write Card numbers on another piece of paper.

◈ **Use Card Skimmers**: Employees may use a Card Skimmer (i.e., a battery-operated, hand-held electronic device) that reads a Card's Magnetic Stripe and records it to memory. Card numbers are then downloaded from the skimmer and used to make counterfeit Cards or make unauthorized purchases. Some Card companies offer a reward for information leading to the arrest and conviction of anyone involved in the manufacture or use of counterfeit Cards.

◈ **Process a Credit Transaction to their own Card Account**: Employees may issue credits to their own Card or to an accomplice's Card using the Merchant's POS Device. Often these credits do not have an offsetting prior sale.

> Most products allow a Merchant to require a password in order to process a Credit Transaction.

There are several ways to prevent fraud committed by employees, such as:

◈ Reconcile your work daily rather than monthly.

◈ Password protect your POS Device, if this feature is available.

◈ Disable the credit function on your POS Device.

◈ Secure your POS Device during non-business hours.

FACTORING

Factoring (also known as Laundering) occurs when you process another person's transactions through your Merchant account. Processing transactions which belong to another person or business is in violation of your Agreement and is prohibited by law in many states. Factoring may result in the termination of your Card acceptance privileges.

Be wary of the "fellow business person" who offers to pay you to process card transactions in return for a fee. These transactions are often questionable or fraudulent. These schemes typically result in a flood of Chargebacks which will be debited from your DDA. By the

NOVA NETWORK

time you realize this has occurred, the other business will most likely
have relocated under a different name.

To protect you from these schemes and the devastating losses that
ensue, educate yourself and your staff about this serious problem and
immediately report Factoring propositions to us or to the U.S. Secret
Service. Remember, you are responsible for all transactions processed
using your Merchant Identification Number, so make sure that all
transactions processed through your account represent transactions
between you and the Cardholder.

NOVA NETWORK

CODE 10 PROCEDURES

Code 10 is a term used by the Card associations to refer to suspicious or questionable Transactions, Cards, or Cardholders.

If you are suspicious of a Card Transaction, contact your Voice Authorization Center and request a Code 10 authorization. Using the term "Code 10" allows you to call the Voice Authorization Center to question the Transaction without alerting the Cardholder. Follow the instructions given to you on how to proceed to minimize any discomfort between you and the Cardholder.

Be alert to individuals who contact your business via phone or the Internet attempting to make large purchases for overseas shipment, direct or through a freight forwarder. These individuals may utilize one or more Cards in their "urgent" request. Based on our experience at this time, fraudulent purchase trends are most prevalent in shipments to Nigeria, Ghana, and Indonesia, to name only three of the highest risk countries. If you receive such a request, we encourage you to contact your Voice Authorization Center to request a Code 10, specifically identifying the Transaction as a large foreign shipment transaction.

Fraudulent transactions, even when authorized, are subject to Chargebacks, and final payment is not guaranteed.

CODE 10 AUTHORIZATION NUMBERS

To request a Code 10 Authorization for a Visa or MasterCard Transaction, call the telephone number on your Voice Authorization sticker (located on the Terminal). To request a Code 10 Authorization for other Cards, refer to the following list:

◆ American Express:
  ◆ (800) 528-2121 (provides Approval Codes and verifies names and addresses)
  ◆ (800) 876-9786 (validates consumer information)

◆ Discover Financial Services:
  ◆ (800) 347-3102

WHAT TO DO WITH AN UNAUTHORIZED CARD

If you are informed that the Card has been reported lost or stolen, or is otherwise invalid, do not complete the Transaction. If you are instructed to retain the Card, follow these procedures:

◆ Maintain a record of the Card number in your files.

◆ Cut the Card through the account number lengthwise without damaging the Magnetic Stripe.

◆ Gather the following information:

  ◆ Merchant's name, Merchant Identification Number, telephone number, and address
  ◆ Employee's name, telephone number, and address.
  ◆ Card account number
  ◆ Reason for recovery

◆ Mail the information to:

Exception Processing
ATTN: Card Pick Up
NOVA Information Systems, Inc.
7300 Chapman Highway
Knoxville, TN 37920

NOVA NETWORK

Do not challenge the Card user. Avoid any physical confrontation with anyone who may be using a lost, stolen, or otherwise invalid Card. Do not jeopardize your safety or that of your employees or customers.

Once this person leaves your location, note in writing his or her physical characteristics and any other relevant identification information. Keep in mind that a reward may be offered by the Issuer for the recovery and return of a lost, stolen, or otherwise invalid Card.

NOVA NETWORK

RETRIEVAL REQUESTS AND CHARGEBACKS

A Cardholder or Issuer may dispute a Transaction for any number of reasons, including a billing error, a quality dispute, or non-receipt of goods and/or services. This chapter describes the process for handling disputed Transactions by explaining Retrieval Requests and Chargebacks.

NOTIFICATION OF RETRIEVAL REQUESTS AND CHARGEBACKS

You may elect to receive Retrieval Requests and Chargeback notices by either U.S. mail or Autofax.

To update or change the way you receive a Retrieval Request or Chargeback notification, call Merchant Services or contact the Chargeback department at the toll-free telephone number listed on your notice.

RETRIEVAL REQUESTS

A Retrieval Request is a request from the Issuer, made on behalf of the Cardholder, for a copy of the Transaction Receipt. A Retrieval Request (also known as a Copy Request) most often occurs when a Cardholder:

◆ Loses their copy of the Transaction Receipt
◆ Does not remember the Transaction
◆ Questions the Transaction for any reason

When a copy of a Transaction Receipt is requested, you will receive a Retrieval Request notice to help you identify the Transaction Receipt

for the requested Transaction. The notice will include the following information:

◆ Card number
◆ Dollar amount
◆ Transaction Date

For Transactions charged on foreign Cards, the dollar amount may vary because of currency exchange rates. The Transaction Date listed on the Retrieval Request may also differ a few days from the date of the actual Transaction. If you cannot locate a specific Transaction Receipt in your records for the date specified on the Retrieval Request notice, search your records for three days before and three days after the Transaction Date listed.

Retrieval Request notices do NOT include the Cardholder's name, because this information is not provided by the Issuer.

When you receive a Retrieval Request notice, you are required to provide us with a copy of the applicable Transaction Receipt so we can send it to the Issuer on your behalf. The Transaction Receipt copy must be clear and legible, signed by the Cardholder, and provided within the time frame specified in the notice.

We suggest you maintain Transaction Receipts in chronological order so that you can retrieve them quickly and easily when needed. Records may be stored off site, provided they are secure and readily accessible to the appropriate personnel. Remember, all records must be retained for a minimum of eighteen (18) months.

It is absolutely critical that you respond by the deadline specified in the notice. Failure to respond to a Retrieval Request or failure to provide a Transaction Receipt in a timely manner will result in a Chargeback that cannot be reversed. Your response to a Retrieval Request may be sent by fax or U.S. mail, as outlined in the Retrieval Request notice. Due to possible delays using U.S. mail, we recommend that you fax the response or send it via overnight mail. If you elect to send your response via U.S. mail, make sure you allow sufficient time to meet the deadline.

NOVA NETWORK

If we do not receive your response to the Retrieval Request by the deadline given, a Chargeback will be issued and your DDA will be debited for the amount of the Transaction. Again, this type of Chargeback cannot be reversed. To avoid such Chargebacks, you should make it a priority to respond to Retrieval Request notices as soon as you receive them.

CHARGEBACKS

A Chargeback is a Transaction disputed by the Cardholder or an Issuer. If you receive a Chargeback, we will debit your DDA for the amount of the Transaction including any applicable currency fluctuations.

There are several situations in which Chargebacks may occur. The most common Cardholder-initiated disputes include:

◆ Dissatisfaction with the quality of merchandise or services received
◆ Failure to receive merchandise or services
◆ A questionable Transaction
◆ A processing error by Merchant staff
◆ Unauthorized use of a Card

While it may not be possible to eliminate Chargebacks entirely, you can reduce their occurrence by resolving issues and disputes directly with the Cardholder and by following the proper Authorization and processing procedures. Because Chargebacks can be costly to the Merchant, you should make every effort to prevent them. Generally, you should remember to:

◆ Avoid duplicate processing of a Transaction.
◆ Work with the Cardholder to resolve disputes regarding the quality of merchandise or services rendered.
◆ Refuse to process a Transaction when you receive a Declined Code during Authorization.
◆ Call for Voice Authorization, if needed.
◆ Call for a Code 10 Authorization if you are still suspicious of the Cardholder, Card, or Transaction after receiving an Approval Code.
◆ Follow the procedures for processing Transactions as outlined in Chapter 3, *Settling Daily Transactions.*

◆ Include a description of the goods or services on the Transaction Receipt.

◆ Deliver merchandise or services before charging the Card

◆ Obtain an Authorization Code.

◆ Include the CVV2/CVC2/CID and AVS codes for Card Not Present Transactions, if applicable.

◆ Submit Transaction Receipts on the same day Transactions are authorized.

◆ Make sure an Imprint appears on a manual Transaction Receipt or that the relevant Transaction information appears on the POS Device-generated Transaction Receipt (see *Transaction Receipts* on page 13 for more details).

◆ Never accept expired Cards or Cards having effective dates prior to the date of the Transaction.

◆ Make sure the signature on the Transaction Receipt matches the signature on the back of the Card.

◆ Obtain a signature from the Cardholder when merchandise is delivered.

◆ Be cautious of shipments to an address other than the Cardholder's billing address.

NOTIFICATION OF CHARGEBACKS

If you receive a Chargeback, we will debit your DDA for the amount of the Chargeback and send you a Chargeback notice. This notice includes the details of the Transaction, as well as specific instructions on how to respond.

HOW TO RESPOND TO A CHARGEBACK

A Merchant's written reply to a Chargeback is known as a Chargeback rebuttal.

You must submit your rebuttal to us in a timely manner so we can present it to the Issuer. If you submit a valid rebuttal, we will issue a provisional credit in the amount of the Transaction to your DDA. The Issuer will then review your rebuttal to determine if the Chargeback is remedied. If the Issuer determines that the Chargeback is not remedied, they will initiate a second Chargeback and we will debit your DDA a second time.

You must submit a legible and valid rebuttal within the time frame specified in the Chargeback notice. Failure to do so will delay credit to your DDA and may result in a waiver of your right to rebut the Chargeback.

For more information on rebuttal procedures, contact the Chargeback department.

CHARGEBACKS THAT CANNOT BE REVERSED

There are specific instances when a Chargeback cannot be reversed. In these cases, you are responsible to us for the Transaction amount regardless of the Authorization Code you received. These situations include:

◆ When the Card is present but it is not swiped or manually Imprinted
◆ When the Card is present but you did not have the Cardholder sign the Transaction Receipt
◆ When the signature on the Transaction Receipt does not match the signature of the Cardholder on the back of the Card

DYNAMIC CURRENCY CONVERSION TRANSACTIONS

This section describes how to process Dynamic Currency Conversion (DCC) Transactions for the designated Cards. These guidelines can help you:

◆ Understand your responsibilities for DCC Transactions
◆ Deal with face-to-face transactions
◆ Handle mail order and telephone order transactions
◆ Process Electronic Commerce transactions
◆ Accept Express Service transactions (in limited Travel and Entertainment (T&E) situations)

YOUR RESPONSIBILITIES AND RESTRICTIONS

You have sole responsibility to comply with the Laws and Payment Network Regulations governing DCC Transactions, including all of the following:

1. You must inform the Cardholder that the DCC Transaction is optional and that the Cardholder does not need to do anything additional to have the transaction processed in their local currency. The Cardholder must expressly agree to the DCC Transaction. You are prohibited from using any customer service procedure or contractual language that creates a DCC Transaction for the Cardholder by default.
2. You are prohibited from converting a DCC Transaction in local currency into an amount in a Cardholder's billing currency after the transaction has been completed with the Cardholder but not yet entered into Interchange.

FACE-TO-FACE TRANSACTIONS

In face-to-face transactions, you must ensure that, in addition to the Transaction Receipt requirements discussed in the prior chapters, the Transaction Receipt includes all four of the following information:

1. The price of the goods or services in the Merchant's local currency, accompanied by the currency symbol next to the amount
2. The total price in the Transaction Currency accompanied by the words "Transaction Currency" and the currency symbol next to the amount
3. The exchange rate, including any commission
4. A statement in an area easily seen by the Cardholder stating that the Cardholder was offered a choice of payment in the Merchant's local currency and that the choice of currency is final

MAIL ORDER AND TELEPHONE ORDER (MO/TO) TRANSACTIONS

If you have previously disclosed to us in accordance with Section (C) of the TOS that you will solicit or accept MO/TO Transactions, you must notify the Cardholder of all of the following information prior to initiating a MO/TO DCC Transaction:

1. The price of the goods or services in the Merchant's local currency
2. The exchange rate, including any commission
3. The total price in the Transaction Currency
4. That the Cardholder has a choice of payment, including the Merchant's local currency
5. That the choice of currency is final

In addition to the Transaction Receipt discussed in the prior chapters, the Transaction Receipt for a MO/TO DCC Transaction must include all of the following:

1. Price of the goods or services in the Merchant's local currency accompanied by the currency symbol next to the amount
2. Total price in the Transaction Currency accompanied by the words "Transaction Currency" and the currency symbol next to the amount
3. The exchange rate, including any commission
4. A statement in an area easily seen by the Cardholder stating that the Cardholder was offered a choice of payment in the Merchant's local currency and that the choice of currency is final

ELECTRONIC COMMERCE TRANSACTIONS

If you have previously disclosed to us in accordance with Section (C) of the TOS that you will solicit or accept Electronic Commerce Transactions, you must ensure that the Cardholder confirms receipt of all of the following information by clicking on an "accept" or other affirmative button, ensuring proper disclosure at the time of an Electronic Commerce DCC Transaction:

1. The price of the goods or services in the Merchant's local currency
2. The exchange rate, including any commission
3. The total price in the Transaction Currency
4. That the Cardholder has a choice of payment, including the Merchant's local currency
5. That the choice of currency is final

In addition to the Transaction Receipt requirements discussed in the prior chapters, the Transaction Receipt for an Electronic Commerce DCC Transaction must include all four of the following items:

1. The price of the goods or services in the Merchant's local currency accompanied by the currency symbol next to the amount
2. The total price in the Transaction Currency accompanied by the words "Transaction Currency" and the currency symbol next to the amount
3. The exchange rate, including any commission
4. A statement, in an area easily seen by the Cardholder, that the Cardholder was offered a choice of payment in the Merchant's local currency, and that the choice of currency is final

NOVA NETWORK

EXPRESS SERVICE TRANSACTIONS (LIMITED T&E SITUATIONS)

If you are a T&E hotel, lodging, or car rental Merchant eligible to offer an Express Service Transaction, you must document the terms of the Express Service DCC Transaction in a written agreement. The Cardholder must sign the agreement in advance of a hotel or lodging checkout or a car rental return Transaction. The written agreement must include all of the following information:

1. The specific currency in which the conversion will take place
2. That the Cardholder has been offered a choice of payment, including the Merchant's local currency
3. That the Cardholder understands that a DCC Transaction will take place
4. That the choice of currency is final
5. That the currency conversion rate will be determined at a later time without further Cardholder consultation

In addition to the Transaction Receipt requirements discussed in the prior chapters, the Transaction Receipt for an eligible Express Service DCC Transaction must include all four of the following:

1. The price of the goods or services in the Merchant's local currency accompanied by the currency symbol next to the amount
2. The total price in the Transaction Currency accompanied by the words "Transaction Currency" and the currency symbol next to the amount
3. The exchange rate, including any commission
4. A statement, in an area easily seen by the Cardholder, that the Cardholder was offered a choice of payment in the Merchant's local currency, and that the choice of currency is final

The Merchant shall send the Cardholder a copy of the Transaction Receipt through the postal service within three (3) business days of completing the transaction. The Merchant must process any delayed or amended charges at the same currency conversion rate as the original DCC Transaction.

SUPPLIES

We can provide all of the supplies you need to complete your Visa and MasterCard Transactions. If you are running low, call your service provider or go online to http://www.merchantconnect.com to replenish your stock.

The basic supplies you need are:

◆ Visa and MasterCard Transaction Receipts and Credit Transaction Receipts
◆ Terminal and Imprinter (may be purchased or leased)
◆ Batch Header receipts and envelopes
◆ Merchant plate
◆ Electronic printer paper
◆ Stickers containing Voice Authorization numbers
◆ Visa and MasterCard window decals and cash register signs
◆ Documentation supporting your Terminal or software

We suggest that you check your supplies frequently to ensure you have an adequate quantity on site. Supplies are normally shipped via UPS ground transportation; if you request a "rush" shipment you will incur additional charges.

NOVA NETWORK

ADDITIONAL RESOURCES

To provide you with fast, efficient customer support, we encourage you to access our Web site at http://www.merchantconnect.com. You may retrieve account information, order supplies, and more.

To obtain Issuer-specific information, you can access the following Web sites:

◆ American Express: http://www.americanexpress.com/homepage/merchant.shtml
◆ Discover Financial Services: http://www.novusnet.com
◆ MasterCard: http://www.mastercardintl.com/business
◆ Visa: http://www.usa.visa.com/business/merchants

GLOSSARY

ACH: See *Automated Clearing House*.

ACS: See *Automated Customer Service*.

Address Verification Service (AVS): A fraud-reduction service that allows the Merchant to verify a Cardholder's billing address prior to completing a Card Not Present Transaction.

Agreement: The Terms of Service (TOS), the Merchant Application, this Merchant Operating Guide, any Merchant Agreement or Merchant Processing Agreement, and any other guides or manuals provided to Merchant from time to time, and all additions to, amendments and modifications of, and all replacements to any of them, as applicable.

Approval Code: An Authorization Code indicating that the Transaction is approved and the Card may be honored.

Automated Customer Service (ACS): A desktop application used as a reporting and accounting reconciliation tool for viewing detailed reports of Transaction activity, statement detail, Card type history, and qualification detail.

Authorization: A required procedure by which a Merchant requests approval of a Transaction from the Issuer. See also *Magnetic Swipe Authorization*, *Manual Entry Authorization*, or *Voice Authorization*.

Authorization Code: The code sent by the Issuer in response to an Authorization request that indicates whether the Transaction is approved. Responses may include: "Approved," "Declined," "Declined Pick-Up," or "Referral" ("Call Auth").

Autofax: A program offered to Merchants for receiving Retrieval Request and Chargeback notices via a dedicated 24-hour fax line.

Automated Clearing House (ACH): The funds transfer system governed by the rules of the National Automated Clearing House

NOVA NETWORK

Association. ACH allows financial institutions to clear interbank entries electronically. A Merchant's DDA is debited and credited via ACH.

AVS: See *Address Verification Service*.

Balance: The amount of money owed by the Cardholder to the Issuer for charges on a Credit Card. On a Debit Card this is the amount of money available in the Cardholder's demand deposit or savings account

Bank Identification Number (BIN): The identification number assigned to a Member that is used for Card issuing, Authorization, clearing, and Settlement processing.

Batch: The accumulated Card Transactions stored in the POS Device or Host computer.

Batch Header: A summary, similar to a deposit slip, of a group of Card Transactions accepted by a Merchant who does not process Transactions electronically. It is attached to the Transaction Receipts when they are sent to the paper processor.

BIN: See *Bank Identification Number*.

Card: A plastic card issued by a bank or other financial institution, or by a Card company (e.g., Visa and MasterCard Credit Cards and Debit Cards), that allows a Cardholder to pay for purchases by credit, charge, or debit.

Card Present: The processing environment in which the Card is physically presented to the Merchant by the Cardholder as the form of payment at the time of sale.

Card Not Present: The processing environment in which the Card is not physically presented to the Merchant by the Cardholder as the form of payment at the time of sale. Card Not Present includes Mail Order (MO), Telephone Order (TO), and Electronic Commerce (EC) Transactions.

Cardholder: The person in whose name the Card is issued and who uses the Card for purchasing goods or services, or to obtain a Cash Advance.

Card Identification Number (CID): A Card identification number printed on a Card and used as additional verification for Card Not Present Transactions. For American Express Card types it is a four-

NOVA NETWORK

digit code printed above the Card account number. For Discover Card types it is a three-digit card code value printed on the signature panel of the Card.

Card Imprint: See *Imprint* or *Imprinter*.

Cash Advance: A Transaction in which a Cardholder receives cash from a financial institution or an ATM.

Chargeback: A Transaction disputed by a Cardholder or Issuer pursuant to the Card Rules.

CID: See *Card Identification Number*.

Code 10 Authorization: An Authorization or an "additional verification step" obtained for a suspicious or questionable Transaction, Card, or Cardholder.

Copy Request: See *Retrieval Request*.

Credit Card: A plastic card with a revolving credit limit used to purchase goods and services or to obtain cash advances.

Card Rules: The rules and regulations promulgated by Visa and MasterCard.

Credit Transaction Receipt: A paper or electronic document evidencing a Merchant's refund or price adjustment to be credited to the Cardholder's account and debited from the DDA. This is also known as a credit slip or credit voucher.

CVV2/CVC2: A three-digit value or code printed on the signature panel of a Card and used as additional verification for Card Not Present Transactions.

DBA: See *Doing Business As*.

DCC: See *Dynamic Currency Conversion*.

DDA: See *Demand Deposit Account*.

Debit Card: A Card issued by a financial institution that, when used to make a purchase, results in the immediate withdrawal of funds from the Cardholder's depository account. Debit Cards do not represent a line of credit; they can only be used to the extent the Cardholder has available funds. Debit Cards may be PIN-based, signature-based, or both.

Declined Code: An Authorization Code indicating that the Transaction is declined and the Card is not to be honored.

Declined Pick-Up Code: An Authorization Code indicating that the Transaction is declined and the Card should be retained by the Merchant.

Demand Deposit Account (DDA): A commercial banking account designated by the Merchant through which all Transactions, fees, charges, adjustments, and Chargebacks are processed. In the instance of a Debit Card or ATM Card, this refers to the Cardholder's deposit account.

Discount: A type of fee paid by a Merchant to process its Card Transactions. Discount is calculated by multiplying the Discount rate by the volume of Card Transactions.

Doing Business As (DBA): The trade name of a Merchant that may appear on business signs, customer literature, or other documents.

Dynamic Currency Conversion (DCC): A service that allows merchants to offer international Cardholders in the United States the option at the point-of-sale to pay in their local currency rather than U.S. dollars.

EBT: See *Electronic Benefits Transfer Service*.

ECS: See *Electronic Check Service.*

EGC: See *Electronic Gift Card.*

Electronic Benefits Transfer Service (EBT): A service that allows electronic transfer of government funds to individuals through the use of a plastic debit-like Card and a Personal Identification Number (PIN). The federal government requires all states to distribute food stamps and cash benefits in this manner.

Electronic Check Service (ECS): A product that allows a Merchant to process a paper check electronically. See also the *ECS Merchant Operating Guide (ECS MOG)* for detailed information on processing checks as electronic transactions.

Electronic Commerce: A Transaction that occurs when the Cardholder uses the Internet to make a purchase from a Merchant.

Electronic Gift Card (EGC): A program that allows a Merchant to sell Electronic Gift Cards redeemable for in-store merchandise or services.

NOVA NETWORK

Embossing: The process of printing data on a Card in the form of raised characters so the Card may be used in the imprinting of Transaction Receipts.

Encryption: A security or anti-fraud technique that scrambles data automatically in the POS Device before the data is transmitted. For example, PINs are encrypted when transmitted for Authorization.

Express Service Transaction: A unique Transaction agreement that is required for an eligible T&E Merchant in those limited situations where a Cardholder in advance authorizes a hotel, lodging, or car rental Transaction and chooses to retain their express service options.

Factoring (Laundering): Processing Transactions for another person or business through a Merchant's account.

Hologram: A three-dimensional image included on a Card to discourage counterfeiting.

Host:The central server we use to store Merchant information and to route information between the Merchant and the Issuers.

Imprint: The physical impression made from a Card on the Transaction Receipt, which may be used to prove that the Card was present when the sale was made.

Imprinter: A device used by Merchants to make an Imprint on a Transaction Receipt.

Interchange: The clearing and settlement system for Visa and MasterCard Credit Cards and Debit Cards where data is exchanged between the Servicer and the Issuer.

Interchange Fees: The amount paid by the Servicer to the Issuer on each Transaction. Interchange Fees vary according to the type of Merchant and the method of processing.

Issuer: A financial institution or other entity that issues a Card to a Cardholder.

Laundering: See *Factoring*.

Magnetic Stripe: A stripe of magnetic material affixed to the back of a Card that contains Cardholder account information.

Magnetic Swipe Authorization: An electronic Authorization request generated when a Merchant swipes the Cardholder's Card through the POS Device. The POS Device reads the Cardholder information from

the Magnetic Stripe on the Card and then dials out to the Authorization Center to obtain an Authorization Code.

Manual Entry Authorization: An Authorization request generated when the Merchant key-enters the Cardholder's Card number, expiration date, and sales amount into the POS Device (e.g., when the POS Device is unable to read the Cardholder information from the Magnetic Stripe on the Card). The POS Device then dials out to the appropriate Authorization Center to obtain an Authorization Code.

Member: A financial institution designated by us that is a principal, sponsoring affiliate or other member of Visa or MasterCard.

Merchant: The business entity that provides goods and/or services to Cardholders.

MerchantConnect: A Web-based Transaction reporting and reconciliation system used to manage Transaction data from multiple locations or multiple merchant accounts via any standard Web browser (e.g., Internet Explorer).

Merchant Identification Card: A plastic card issued to the Merchant that contains the Merchant's Identification Number, name, location, and DDA number.

Merchant Identification Number (MID): A unique identification number assigned to a Merchant to identify its business (also referred to as the "Merchant Account").

Merchant Plate: A plastic or metal plate affixed to the Imprinter that contains Merchant information such as the Merchant name, Merchant Identification Number, city and state, and a Discover or American Express account number, if applicable.

Merchant Statement: A monthly summary of activity in a Merchant account.

MO/TO: Mail Order/Telephone Order.

Negative Deposit: When the dollar amount of Credit Transaction Receipts exceeds the dollar amount of Transaction Receipts submitted for processing.

Personal Identification Number (PIN): A number that must be entered by a Cardholder in order to complete certain types of Transactions (e.g., online debit, EBT).

PIN: see *Personal Identification Number*

NOVA NETWORK

POS Device: A terminal or other point-of-sale device, including a Third Party Terminal, at a Merchant location that conforms with the requirements established from time to time by Servicer and the applicable Payment Network.

Pre-authorized Order: A written or electronic authorization by a Cardholder allowing a Merchant to charge their Card at a future date.

Quasi-Cash Transactions: Transactions representing a Merchant's sale of items that are directly convertible to cash.

Recurring Payments: A Transaction charged to the Cardholder (with prior written or electronic permission to a Merchant) on a periodic basis for recurring goods and services (e.g., monthly membership fees, utility bills, subscriptions).

Referral Code: An Authorization Code indicating that the Issuer is requesting that the Merchant call the Voice Authorization Center, which will either provide an Approval Code or ask the Merchant to request additional information from the Cardholder (e.g., mother's maiden name).

Retrieval Request: A request from the Issuer on behalf of the Cardholder for a legible copy of the Cardholder's signed Transaction Receipt.

SCAN[TM]: A check verification service that allows Merchants to decide whether or not to accept a check at the point-of-sale.

Servicer: The entity that processes Transactions on behalf of the Merchant.

Settlement: The process of submitting Transactions to the Servicer for processing.

Split Sale: A prohibited process by which Merchants use multiple Transaction Receipts to avoid Authorization for a single Transaction.

T&E Merchant: A Merchant whose primary function is to provide travel and entertainment related services.

Terminal: A point-of-sale device used by the Merchant to electronically process Card Transactions.

Third Party Terminal: A terminal, other point-of-sale device, or software provided to Merchant by any entity other than Servicer or its authorized designee.

Transaction: Any action between a Cardholder and a Merchant that results in activity on the Cardholder's account (e.g., purchase, refund/return, or debit).

Transaction Currency: The international Cardholder's local currency in a DCC Transaction.

Transaction Date: The date that a Transaction occurs.

Transaction Receipt: The paper or electronic record evidencing the purchase of goods or services from a Merchant by a Cardholder using a Card.

Voice Authorization: An Authorization process whereby a Merchant calls the Voice Authorization Center and provides Cardholder and purchase information over the telephone. The Voice Authorization Center then provides an Authorization Code to the Merchant.

Voice Authorization Center: The center that conducts Voice Authorization for Card Transactions.

NOVA NETWORK