Merchant Services Payment Card Processing Setup Kit

Tools to increase your revenue stream

Welcome

Welcome to Merchant Services. We are pleased that you have chosen us as your payment card processing provider. We pledge to provide you with outstanding customer service. Our Customer Relations department is available 24 hours a day, 7 days a week, by calling 1-800-654-9256.

Included with this letter are the training materials you will need to process your payment card transactions. You may also be contacted in the next few days by one of our merchant trainers, who will schedule a time to train you on your new payment card system.

Funding of your daily deposits generally occurs from one to two business days based on the time the batch is closed. This schedule may vary due to bank holidays and other specific criteria related to your account.

You will be automatically charged for your discount and fees on the 10th of each month. You will receive a statement at the beginning of the month, itemizing these fees.

Again, we at Merchant Services look forward to assisting you with all of your payment card processing needs.

Thank you,
Merchant Services

Getting Set Up

Setting up your new payment card processing terminal with Merchant Services is easy. Your deployment kit contains instructions to help your installation process run smoothly before, during and after your call with a Merchant Services training representative. In addition to setup instructions, this kit contains valuable tips to help reduce your risk of fraud and chargebacks, terminal reference information and contact information should you need assistance at any time. We recommend keeping this manual in a handy location for easy reference in the future. The following items should be included in your Merchant Services Customer Deployment Kit:

3	Installation Tips
4	Digital vs. Analog Phone Line Policy
5	Sample Payment Card Processing Statement
6-7	Data Security – It's Everyone's Business
7-10	PCI Data Security Standards and Compliance
11	New IRS Regulations and How They May Impact You
12-18	Tips to Prevent Fraud and Avoid Chargebacks
19-20	Frequently Asked Account Questions
21	Merchant Information Resources

Other Items Included:

- Terminal Key Overlay Card
- Visa®, MasterCard®, American Express®, Discover® and PayPal™ Sticker
- Merchant Services Voice Authorization Sticker
- Quick Reference Guide

Installation Tips

Before your pre-scheduled training and installation call with a Merchant Services representative, please take advantage of the following information:

1. Payment card processing terminals work best with a dedicated analog line, which is a telephone line that has its own telephone number, much like a fax machine.
2. The telephone line from the terminal into the telephone wall jack should not be on a splitter and should instead be plugged directly into the wall jack.
3. If your new Merchant Services terminal will share a line with the telephone that will be used during the training call, you may want to have a cell phone available during the training. Please be sure to give us this information when we contact you, and provide the cell phone number that the training representative may call.
4. If your telephone system requires an access number to dial out (for example 9 or 8), please be sure to let us know when you are contacted to schedule your training appointment.

Digital vs. Analog Phone Line Policy

Overview

High-speed connectivity – such as digital subscriber lines (DSL), broadband cable Internet for business and associated communications technologies such as Voice-over-Internet Protocol (VoIP) – is commonplace today. Many telecommunication companies offer only VoIP telephone services. VoIP converts analog audio signals into digital data that can be transmitted over the Internet. Since VoIP is intended to be transparent to the user, using a dial-up, point-of-sale terminal to process transactions over this connection is not only difficult to identify, but it is also difficult to support and may not be secure.

Issues — Insecure data transfer with VoIP:

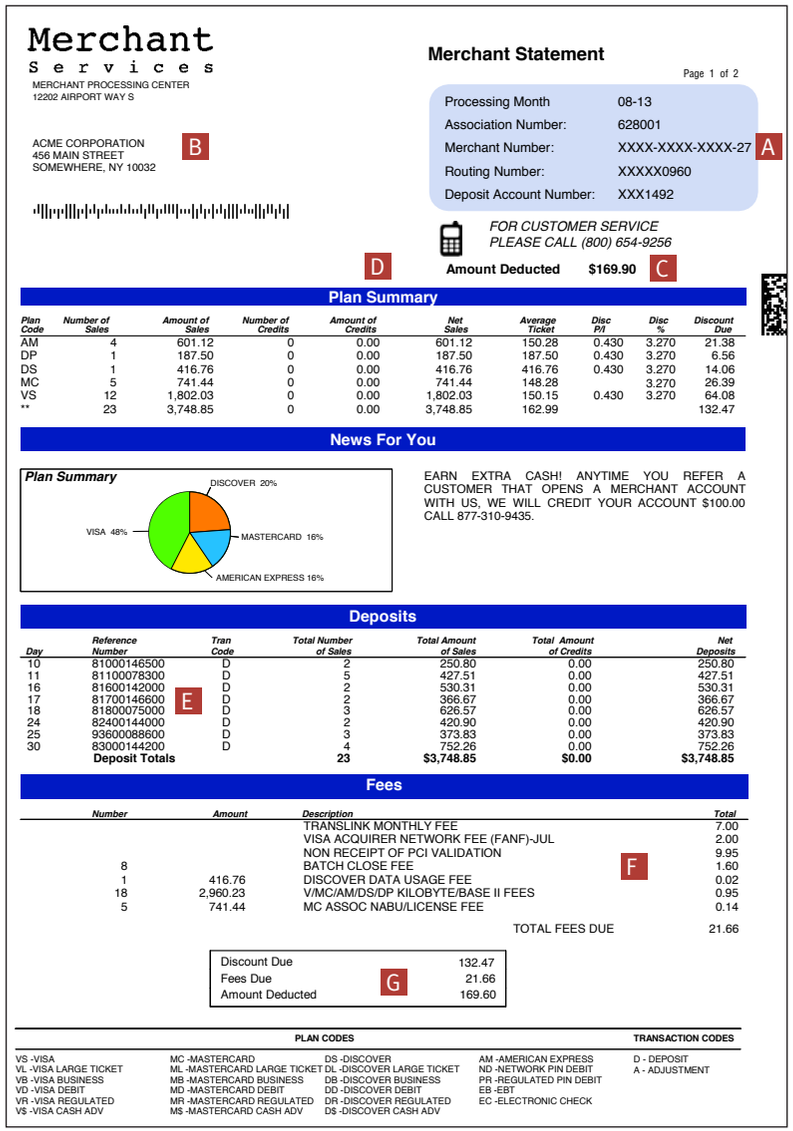
VoIP service in lieu of an analog service line can leave transactions unsecured and vulnerable to fraudulent activity. Sending dial transactions over a VoIP line does not provide protection with Secure Sockets Layer (SSL) encryption, and can result in data capture, card/merchant number theft, etc., especially if the VoIP carrier uses the public Internet as transport. These scenarios are outside the guidelines for secure transaction processing set forth by the card associations and the Payment Card Industry (PCI) standards.

Solutions

Digital services, including VoIP, are cheaper alternatives to a dial-up business line, both in lower monthly fees and in the elimination of usage fees; and are attractive telecom solutions for small businesses. However, as it stands today, these services can create an environment that prevents verification of secure transactions, and are therefore prohibited by Merchant Services. Some solutions are:

- You may use your existing dial-up terminal with an analog dial line for secure point-to-point transaction processing.
- You may upgrade your device to an IP or dual communication terminal.

Your New Merchant Statement



Merchant Services

MERCHANT PROCESSING CENTER
12202 AIRPORT WAY S

ACME CORPORATION
456 MAIN STREET
SOMEWHERE, NY 10032

Merchant Statement

Page 1 of 2

Processing Month	08-13
Association Number:	628001
Merchant Number:	XXXX-XXXX-XXXX-27
Routing Number:	XXXXX0960
Deposit Account Number:	XXX1492

FOR CUSTOMER SERVICE
PLEASE CALL (800) 654-9256

Amount Deducted $169.90

Plan Summary

Plan Code	Number of Sales	Amount of Sales	Number of Credits	Amount of Credits	Net Sales	Average Ticket	Disc P/I	Disc %	Discount Due
AM	4	601.12	0	0.00	601.12	150.28	0.430	3.270	21.38
DP	1	187.50	0	0.00	187.50	187.50	0.430	3.270	6.56
DS	1	416.76	0	0.00	416.76	416.76	0.430	3.270	14.06
MC	5	741.44	0	0.00	741.44	148.28		3.270	26.39
VS	12	1,802.03	0	0.00	1,802.03	150.15	0.430	3.270	64.08
**	23	3,748.85	0	0.00	3,748.85	162.99			132.47

News For You

Plan Summary

DISCOVER 20%
VISA 48%
MASTERCARD 16%
AMERICAN EXPRESS 16%

EARN EXTRA CASH! ANYTIME YOU REFER A CUSTOMER THAT OPENS A MERCHANT ACCOUNT WITH US, WE WILL CREDIT YOUR ACCOUNT $100.00 CALL 877-310-9435.

Deposits

Day	Reference Number	Tran Code	Total Number of Sales	Total Amount of Sales	Total Amount of Credits	Net Deposits
10	81000146500	D	2	250.80	0.00	250.80
11	81100078300	D	5	427.51	0.00	427.51
16	81600142000	D	2	530.31	0.00	530.31
17	81700146600	D	2	366.67	0.00	366.67
18	81800075000	D	3	626.57	0.00	626.57
24	82400144000	D	2	420.90	0.00	420.90
25	93600088600	D	3	373.83	0.00	373.83
30	83000144200	D	4	752.26	0.00	752.26
	Deposit Totals		**23**	**$3,748.85**	**$0.00**	**$3,748.85**

Fees

Number	Amount	Description	Total
		TRANSLINK MONTHLY FEE	7.00
		VISA ACQUIRER NETWORK FEE (FANF)-JUL	2.00
		NON RECEIPT OF PCI VALIDATION	9.95
8		BATCH CLOSE FEE	1.60
1	416.76	DISCOVER DATA USAGE FEE	0.02
18	2,960.23	V/MC/AM/DS/DP KILOBYTE/BASE II FEES	0.95
5	741.44	MC ASSOC NABU/LICENSE FEE	0.14
		TOTAL FEES DUE	21.66

Discount Due	132.47
Fees Due	21.66
Amount Deducted	169.60

PLAN CODES

VS -VISA
VL -VISA LARGE TICKET
VB -VISA BUSINESS
VD -VISA DEBIT
VR -VISA REGULATED
VS -VISA CASH ADV

MC -MASTERCARD
ML -MASTERCARD LARGE TICKET
MB -MASTERCARD BUSINESS
MD -MASTERCARD DEBIT
MR -MASTERCARD REGULATED
MS -MASTERCARD CASH ADV

DS -DISCOVER
DL -DISCOVER LARGE TICKET
DB -DISCOVER BUSINESS
DD -DISCOVER DEBIT
DR -DISCOVER REGULATED
DS -DISCOVER CASH ADV

AM -AMERICAN EXPRESS
ND -NETWORK PIN DEBIT
PR -REGULATED PIN DEBIT
EB -EBT
EC -ELECTRONIC CHECK

TRANSACTION CODES

D - DEPOSIT
A - ADJUSTMENT

Sample Payment Card Processing Statement

- **A** Merchant-specific account details
- **B** Merchant name and address information
- **C** Total amount due, to be deducted on the 10th of the month
- **D** Summary of processing by card type
- **E** Breakdown of the transaction batch deposits by day
- **F** Breakdown of fees to be deducted from your account
- **G** Total of all discount and miscellaneous fees that will be deducted from your account

Data Security – It's Everyone's Business

Protect your good reputation and keep your customers happy

With the explosive growth of identity theft, data security has become more than just important – it's mandatory. Visa®, MasterCard®, American Express®, Discover® and PayPal™ Operating Regulations now require merchants to store cardholder account information in a secure manner to prevent it from being accessible to criminals.

Identity theft is a topic about which most consumers are well-informed. They know it can be devastating to their credit. Media reports about hackers and stolen payment card information have consumers on high alert. They want assurance that their card information is safe with businesses they choose to shop at.

In the "brick and mortar" world

If you need to check a cardholder's identification, you shouldn't write down any information such as a driver's license number or Social Security number. This type of data could be used to commit identity theft. Unless directed to do so by the voice authorization center, there is no need to check a customer's ID as long as the card is signed.

The CARDHOLDER copy of your electronic sales receipts should only display the last four digits of the account number. Industry Operating Regulations mandate that all but the last four digits of the cardholder account number, and the entire expiration date, be suppressed on the cardholder copy of all transaction receipts generated from electronic terminals. Please contact us if you need your software or equipment updated or upgraded to comply with these regulations.
Keep the MERCHANT copy of your receipts in a secure location, and limit their access to select members of your organization. Merchant copies will still display the full card account number in many cases, plus the card expiration date and the cardholder's signature. Information of this nature cannot be allowed to fall into the wrong hands!

New IRS Regulations and How They May Impact You

IRS Section 6050W went into effect at the beginning of 2011 and significantly impacts the payment card industry. Under this mandate, all payment settlement entities — including merchant services providers — are required to report their merchants' annual gross credit, debit and third-party network payment card transactions to the IRS on Form 1099-K. We will send you a copy of this form on or before January 31 for all activity in the previous year, and will also send it to the IRS to comply with the mandate.

What this means for merchants

In order to comply with the mandate, we will need to have up-to-date records of your legal business name, address and taxpayer identification number (TIN). This information must match your filed tax forms in order to be valid. Please keep in mind that merchants who fail to provide their taxpayer ID number could be subject to a backup withholding equal to 28% of their gross payment card transactions.

As a merchant services provider, we are responsible for complying with IRS Section 6050W.

We have taken several steps to make it easy and convenient for you to understand the mandate and how it impacts you. For example:

- We have assembled a team of professionals with expertise in tax regulations to ensure that necessary steps are taken by Merchant Services to comply with the mandate
- We have already begun submitting merchant information to the IRS via its secure electronic service
- If we currently do not have your updated information on file, we will contact you with instructions on how you can provide it to us.

If you have additional questions regarding this new regulation and how it may impact you and your business, please seek advice from your own tax professional.

Preventing Fraud and Avoiding Chargebacks

Payment card processing has the potential to help you increase your revenue stream as well as offer more convenience to your customers. To ensure that your Payment card processing transactions go as smoothly as possible, we've included some tips on avoiding chargebacks and fraudulent and/or criminal activity. For your own protection, please read the following pages thoroughly and keep this manual handy for future reference and training.

Recognizing Fraudulent Behavior when Conducting Business Face to Face with Your Customer

Certain customer behavior could point to payment card fraud, but remember, it does not necessarily indicate criminal activity. In particular, watch for customers who:

- Purchase several of the same items or purchase very expensive items and do not ask any questions about the items.
- Purchase a lot of merchandise without regard to size, color or price.
- Try to distract or rush you during the sale.
- Make purchases, leave the store and return to make additional purchases.
- Make purchases right at opening or at the last minute when the store is closing.

Recognizing Fraudulent Behavior when Conducting Business via Telephone Orders, Mail Orders or Over the Internet with Your Customer

Because the payment card and cardholder are not present, you, the merchant, often take the loss from a bad transaction. There are people that intend to obtain products and services by deceptive practices. By using lost or stolen cards, or card numbers generated by fraud schemes, they order goods and have them shipped to an address to be

picked up by themselves or someone they call a "runner." When the charge appears on the true cardholder's statement, they will request a copy of the draft or it will be charged back right away. If this is an order made over the telephone, through the mail or via the Internet, these chargebacks are very hard to fight because there is no imprint or signature.

There are characteristics that may indicate that the transaction may not be legitimate. Individually, these characteristics are seldom cause for alarm; rather, it is when several of these factors characterize a transaction that there may be a problem. In particular, watch for customers who:

- Place orders that are larger than normal when you are not familiar with the customer.
- Purchase several of the same item or very expensive items.
- Want orders shipped "rush" or "overnight."
- Have orders shipped to an international address, as they cannot be verified by an Address Verification Service and are very risky unless you know your customer very well.
- Have orders shipped to the same address that were purchased on different cards.
- Place orders from Internet addresses using free e-mail services.
- Charge transactions to account numbers that are sequential.
- Provide multiple card numbers from a single Internet address.
- Charge multiple transactions to one card over a very short period of time.

Avoiding Chargebacks and Dealing with Retrieval Requests

A chargeback is the reversal of a sales transaction previously processed by your business. Your customer or your customer's bank can initiate a chargeback and the amount of the transaction is deducted from your account. Whether it is for tax purposes, fraud or any variety of reasons, if you receive a "retrieval request" from a cardholder or the cardholder's bank requesting a copy of a sales draft or mail order form, DO NOT ignore these requests. Failure to comply promptly could result in a non-recourse chargeback.

There are some basic steps you can take to prevent some of the most common errors that may result in unnecessary chargebacks:

Receipts and Documentation

- Change printer cartridge routinely to avoid faded, barely visible ink on sales drafts. **Visa/MasterCard/American Express/Discover/PayPal state this is a leading cause of illegible sales draft copies.**
- Check readability of all sales drafts daily.
- Position company logo or marketing messages away from the transaction information, as these can make imaged sales draft copies illegible.
- Always use white non-patterned paper for transaction information, since colored or patterned paper can render an imaged document illegible.
- Always provide documentation in original-size format. Reduced images result in illegible/blurred documents.
- Handle carbonless paper and carbon/silver-backed paper carefully, as excessive heat or any pressure during the handling/storage process causes black blotches, making copies illegible.
- Change printer paper when colored streak indicates the end of the roll. The streak diminishes the legibility of transaction information.
- Return policies must be disclosed on the sales draft in close proximity to the customer signature.
- Save all sales drafts for 18 months and store the sales draft in a secure place by payment card number and approximate transaction date only (not by cardholder name). We will not be able to give you the customer's name, because cardholder names are not provided to us.

What You Can Do to Prevent Fraud and Chargebacks when Conducting Business Face-to-Face

The following tips are intended to keep you from being the victim of fraud and will help you avoid chargebacks when conducting in-store transactions.

- Never accept an expired payment card.
- Always inspect the card. Keep the card throughout the transaction. Never accept a card that appears to have been altered.
- Whenever possible, obtain a swipe of the card through the terminal and verify that the card number on the terminal matches the card number on the card.
- When the card will not swipe and you must manually key in the card number to your terminal, you MUST also get an imprint of the card using an imprinter with your merchant plate and have the customer sign the imprinted sales draft.
- In addition, if you are handwriting a sales draft, you need to fill out the draft completely with the transaction date and items purchased.
- Compare the name printed on the electronic sales receipt to the name embossed on the card.
- The embossing on the card should be clear and straight and the hologram should be smooth with the card and three-dimensional.
- Make sure the signature panel has not been tampered with.
- Compare the signature on the sales draft and the back of the card. The card must be signed. If the card is not signed, have the customer sign the card in front of you, and then check the signature on a picture ID. If the signature on the back of the card does not match the signature on the sales draft, do not continue with the sale.
- Use account number–verifying terminals or visually compare the last four digits of the embossed account number to the four digits printed on the sales receipt to determine they are the same numbers in the same sequence.
- Also compare the four digits printed on the card with the first four numbers embossed on the card. The first four numbers should always match. If they do not, do not complete the transaction and notify the authorization center.

- Obtain an authorization for the full amount of the sale (hotels may authorize within 15% of the total).
- If you receive a “call center” or “pick up card” message through your terminal, call the authorization center and follow their instructions.
- If you receive a “do not honor” or “decline” message through your terminal, do not proceed with the transaction. **DO NOT** try again for an authorization; there is no protection for a transaction after you have received a “decline” or “do not honor” message, even if you receive an approval code on a second attempt.

If you are suspicious of a sale, ask for a **Code 10 authorization**. A separate phone call to your authorization center asking for a Code 10 authorization lets the center know you have concerns about a transaction. A Code 10 is a universal code that provides merchants with a way to alert the authorization center that a suspicious transaction is occurring. The Code 10 operator asks a series of questions that can be answered with yes or no responses; just follow the operator’s instructions, and **NEVER** put your life in danger.

REMINDER: Although an authorization code is required on all transactions, it does not guarantee that it is a valid sale made by the legitimate cardholder! An authorization code means that the account is open and has the available credit at that time, but it is not a guarantee of payment.

What You Can Do to Prevent Fraud and Chargebacks when Conducting Business via Telephone Orders, Mail Orders or Over the Internet

The following tips are intended to keep you from being the victim of fraud and will help you avoid chargebacks when conducting Card-Not-Present business. However, Merchant Services is not always able to prevent chargebacks affiliated with doing business in mail, phone or e-commerce environments.

The following information is required on EVERY mail, phone or e-commerce invoice and sales draft:

- The cardholder's payment card number and the expiration date.
- The name that appears on the front of the payment card.
- The cardholder's billing address and phone number.
- Description of merchandise and/or services rendered.

Additionally, the following steps should be taken for every transaction:

- Use an Address Verification Service (AVS) during authorization to verify the cardholder's billing address. Address Verification compares the shipping address given to the merchant with the customer's billing address with their issuing bank. **If the addresses do not match, do not ship the merchandise. You are putting yourself at risk of taking a loss.**
- To verify the card's authenticity, ask for the CVV 2 code on the back of the card if it is a Visa, the CVC 2 code if it is a MasterCard, or the CID code on the front if it is an American Express or on the back if it is a Discover or PayPal* card. This information is frequently missing on fraudulent payment cards, and it would be unavailable in the case of compromised card numbers or generated account number schemes. This three-digit number is found on the back of the card on the signature panel after the card number. While this code does not provide protection against fraud, it does allow the merchant an additional level of security in processing the transaction.

*The account number will not be embossed on the PayPal card. The PayPal Card can only be used for mag stripe read, point-of-sale transactions. No key-entered and no card-not-present ecommerce is available.

- Ask the customer for additional information. For example, ask for a day and evening phone number, and call the customer back later.
- Ask for the bank name on the front of the card, and the bank's customer service number from the back of the card.
- Separately confirm the order with the customer. If you do not use an AVS, send a note via the billing address, rather than the "ship to" address, before shipping the order.
- When you ship the merchandise, ship only to the cardholder's billing address; NEVER ship to any other address that the customer may request.
- You may want a certified signature as proof that the merchandise was delivered.
- Merchants who ship merchandise outside the United States have a greater risk of payment card fraud because the AVS service will only verify addresses within the United States.
- Ask Merchant Services to include your customer service telephone number in the billing name that appears on your customer's payment card statement. This allows your customers the ability to contact you directly if they have questions regarding the sale.
- Provide cardholder name and merchant contact details in the sales transaction data.
- Clearly link credits and refunds you have issued with the original sale information. Include invoice number and settlement information.
- If you have a VERY unusual mail, phone or Internet transaction to be shipped, and are uneasy about the transaction, you can call Merchant Services Support. We will try to assist you in verifying the transaction with the issuing bank BEFORE you ship the merchandise.

Now that you've read these helpful tips, we recommend reading them again and having any company employees who will be handling payment card transactions study them carefully as well. Following these precautions can help to greatly reduce chargebacks and lower your risk of fraudulent charges. If you have questions regarding this information, please contact Merchant Services Support.

Frequently Asked Account Questions

What is “interchange” and how does it affect my fees?

Interchange is the largest portion of your Discount Rate. Interchange is the fee charged by the card issuer to reimburse them for the expense of processing the transaction through their settlement systems. Visa, MasterCard, Discover and PayPal have more than 100 different interchange pricing levels. The qualification requirements for each level vary depending on the card type (consumer, business, purchasing, international, rewards, etc.), the merchant type (retail, hospitality, fuel, etc.) and how the card was presented and processed by the merchant (swiped, key entered, Internet, etc.).

TransFirst’s statement billing to merchants for American Express Cards is based on fees from American Express to processor. These fees are tiered by the merchant’s industry classification and transaction amount. Other fees that may apply include card not swiped, network, inbound and access charges billed by American Express to the processor. American Express does not have or charge interchange.

Discount Rate

For retail merchants, the Discount Rate charged on your merchant statement assumes that qualification requirements are met. The requirements include:

- The payment card is swiped for authorization.
- The cardholder signs the receipt.
- The transaction is batched out (settled) within 24 hours.
- The authorization amount and settlement amount are equal.
- The payment card is a consumer card without a reward program.

A consumer card has the cardholder's name instead of a business name, does not have “purchasing” or “business” on the front, and is associated with an individual instead of a company.

When a card does not meet the requirements of the minimum Discount Rate criteria, it may be processed at a higher rate. These fees are captured in the line item on your statement and may be labeled several things, including “Non-Qualified”.

Non-Qualified Transaction Fees:

Transactions that fail to meet the Discount Rate requirements may be settled at a Non-Qualified rate*. This “downgrade” in qualifications can be caused by any combination of reasons. Merchants that have a portion of their transactions qualifying as Non-Qual should make sure that they are:

- Swiping cards instead of hand-keying in the card number.
- Entering AVS (address information) for the billing address.
- Settling (closing) the batch in a timely manner, usually within 24 hours.
- Not over-settling transactions. Over-settling means that a merchant obtains an authorization for $5.00 and settles the transaction for $10.00. This practice is most common with mail order merchants that charge shipping “after the fact.” These merchants should re-authorize the card for the appropriate amount.
- Entering invoice numbers when prompted.
- Entering tax amount and customer code when prompted.

When will I receive the money from the batch deposits made through my point of sale unit?

Funding generally occurs anywhere from one to five business days based on the time the batch is closed and the specific setup of your account.

What information is required when I call Merchant Support for service?

You should have your Merchant ID number readily available to expedite your service. If this is not available, you should be prepared to answer questions specific to your account establishment for security purposes.

How are PIN-based debit refunds handled?

PIN-based transactions cannot be voided at the POS. If a PIN-based transaction is voided, the cardholder will not receive their money back because of the void. The void/refund should be corrected with cash at the time of the transaction. This does not apply to signature debit, only transactions in which a PIN number was entered. If a PIN-based debit transaction has been inadvertently voided please contact technical support.

*American Express Card transactions are only downgraded based on size of ticket. Merchant pricing structure is determined by TransFirst.

Merchant Information Resources

Phone numbers you may need:

Merchant Support: 800.654.9256

Voice Authorization: 800.291.4840

Please note, you will need to provide your MID, DBA and ZIP code.

For card decals and other promotional items, visit:
www.transfirst.com/support/decals-and-signage

For PayPal In-Store Acceptance Program:

The account number will not be embossed on the PayPal card. The PayPal Card can only be used for mag stripe read, point-of-sale transactions. No key-entered and no card-not-present ecommerce is available.

Merchant Services
12202 Airport Way, Suite 100
Broomfield, CO 80021

TF2166