


Your New Merchant Statement

Sample Payment Card Processing Statement



2450 33rd Avenue W. STE 110 Seattle, WA 98199

ACME CORPORATION
1234 MAIN STREET
ANYWHERE, CA 90210

Merchant Statement

Page 1 of 2

Processing Month: 12-2020 **A**

Association Number: 013495

Merchant Number: xxxx-xxxx-xxxx-12

Routing Number: xxxxx1234

Deposit Account Number: xxxxxx1234

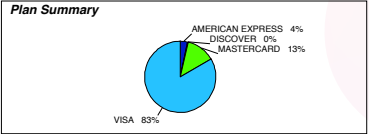
FOR CUSTOMER SERVICE PLEASE CALL (800) 654-9256

D Amount Deducted **C** 2.64

Plan Summary									
Plan Code	Number of Sales	Amount of Sales	Number of Credits	Amount of Credits	Net Sales	Average Ticket	Base P#	Base Rate	Discount Due
VS	1	0.01	0	0.00	0.01	0.01	0.320	0.670	0.32
MC	0	0.00	0	0.00	0.00	0.00	0.320	0.670	0.00
AM	0	0.00	0	0.00	0.00	0.00	0.000	0.000	0.00
DS	0	0.00	0	0.00	0.00	0.00	0.320	0.670	0.00
DB	0	0.00	0	0.00	0.00	0.00	0.000	0.000	0.00
PP	0	0.00	0	0.00	0.00	0.00	0.000	0.670	0.00
**	1	0.01	0	0.00	0.01	0.01	0.01	0.670	0.32

E News For You

Plan Summary



Deposits						
Day	Reference Number	Tran Code	Total Number of Sales	Total Amount of Sales	Total Amount of Credits	Net Deposits
23	90001010003	D	01	0.01	0.00	0.01
Deposit Totals			01	\$0.01	\$0.00	\$0.01

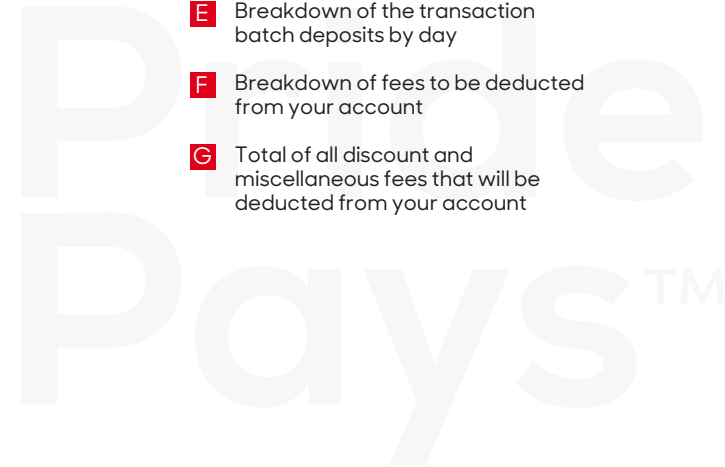
Fees			
Number	Amount	Description	Total
2		FIXED ACQUIRER NETWORK FEE (FANF)	2.00
1		TRANSACTION NETWORK ACCESS FEE	0.06
1		BATCH CLOSE FEE	0.20
1	0.01	ASSOC KILOBYTE/BASE II FEES	0.02
2		VISA ASSOC APF FEE & CREDIT VOUCHER FEE	0.04
TOTAL FEES			2.32

G

Discount	0.32
Fees	2.32
Amount Deducted	2.64

PLAN CODES			TRANSACTION CODES		
VS - VISA	MC - MASTERCARD	DS - DISCOVER	AM - AMERICAN EXPRESS	D - DEPOSIT	
VL - VISA LARGE TICKET	ML - MASTERCARD LARGE TICKET	DL - DISCOVER LARGE TICKET	DB - NETWORK PIN DEBIT	A - ADJUSTMENT	
VB - VISA BUSINESS	MB - MASTERCARD BUSINESS	DZ - DISCOVER BUSINESS	EC - ELECTRONIC CHECK		
VD - VISA DEBIT	MD - MASTERCARD DEBIT	DQ - DISCOVER DEBIT	EB - EBT		
VS - VISA CASH ADV	MS - MASTERCARD CASH ADV	DS - DISCOVER CASH ADV	PP - PAYPAL		

- 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.

Identity theft can be an "inside crime"

Employees who will have access to sensitive cardholder data should be carefully screened before they are hired and periodically thereafter. Unauthorized electronic equipment – such as laptop computers – that can be used to steal or replicate account information should not be allowed in the workplace. Protected cardholder data can lead to higher profits and greater customer loyalty!

PCI Data Security Standards and Compliance

The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements established to ensure that all merchants who process, store or transmit payment card information maintain a secure transaction environment. Importantly, PCI DSS compliance protects both the merchants and their customers. The PCI DSS is administered by the independent Payment Card Industry Security Standards Council, or PCI SSC, which was created by the five major payment card brands – Visa, MasterCard, American Express, Discover and JCB International. The cards covered include any debit, credit or pre-paid cards branded with the association or brand logos of those five participants.

"What are the PCI compliance levels and how are they determined?"

There are four PCI compliance levels and their compliance requirements vary. Merchants are assigned to a level based on their combined transaction volume – including credit, debit and prepaid cards – over a 12-month period. The four levels (from fewest to most transactions) and their requirements are:

- Level 4: Small businesses that process less than 20,000 e-commerce transactions and less than 1 million other transactions annually; Level 4 businesses must complete an annual risk assessment using the appropriate PCI Self-Assessment Questionnaire (SAQ), and quarterly PCI scans, administered by an approved scanning vendor, may also be required.
- Level 3: Mid-sized companies that process between 20,000 and 1 million e-commerce transactions annually; Level 3 companies are required to complete an annual risk assessment using the appropriate SAQ, and quarterly PCI scans, administered by an approved scanning vendor, may also be required.

- Level 2: Companies that process between 1 million and 6 million transactions annually across any sales channel; Level 2 companies are required to undergo a risk assessment every year using the appropriate SAQ, and quarterly PCI scans, administered by an approved scanning vendor, may also be required.
- Level 1: "Big box" stores and major corporations are companies that process a minimum of 6 million transactions per year; in addition to an annual internal audit conducted by a qualified PCI auditor, Level 1 companies may also be required to undergo quarterly PCI scans administered by an approved scanning vendor.

"What are the consequences for noncompliance?"

Your merchant account agreement should outline your specific exposure if you are noncompliant, so check it to make sure you understand your position. Issuing banks and payment card processors can be fined up to \$500,000 for regulatory compliance violations; typically, these fines are passed along to individual merchants in the form of increased transaction fees. In addition to fines, noncompliant businesses that suffer a security breach face card replacement costs, forensic audits and damage to their reputation. Additionally, noncompliant merchants may lose their merchant accounts and languish in the Terminated Merchant File for several years, during which time they cannot accept payment cards.

"Must organizations that use a service provider be compliant?"

Absolutely! As defined by Payment Card Industry (PCI) guidelines, a service provider is a third party that stores, processes or transmits cardholder data on behalf of another entity. While using a service provider may reduce a merchant's risk of exposure and the effort needed to validate compliance, it does not exclude that merchant from PCI compliance.

"Do debit card transactions fall under the scope of PCI compliance?"

Yes, debit cards – along with credit and prepaid cards – that are branded with a logo of one of the five members in PCI SSC (see first paragraph of this topic) are in scope for PCI compliance.

"In terms of PCI compliance, what is a 'merchant'?"

For the purposes of PCI DSS, a merchant is an entity that accepts payment cards (credit, debit or prepaid) with the logo of any of the five members of PCI SSC as payment for goods and/or services. Under the terms of PCI compliance, a merchant is charged with securely storing, processing and transmitting cardholder data.

"In terms of PCI compliance, how is 'cardholder data' defined?"

Cardholder data is the personally identifiable data associated with a cardholder – name, address, account number, expiration date, card verification value (CVV) code, personal identification number (PIN) and Social Security number. This information is embedded in the magnetic stripe on the backs of credit and debit cards or appears on the card itself. Current PCI DSS mandates state that merchant software should never store any of this information permanently.

"Do I need vulnerability scanning to validate my compliance?"

Businesses that electronically store cardholder data post-authorization or that have processing systems connected to the Internet may be required to have a PCI SSC Approved Scanning Vendor (ASV) perform a quarterly scan.

"What is a network security scan?"

A network security scan is performed by an ASV using an automated tool to remotely and non-intrusively check a merchant or service provider's networks and web applications for vulnerabilities in operating systems, services and devices that hackers could use to target the company. Merchants with external-facing Internet Protocol (IP) addresses may be required to pass quarterly scans to validate their PCI compliance.

"How often should a security scan be performed?"

A security scan should be performed quarterly by an ASV. Service providers and merchants should submit their successful scan reports according to the timetable established by their acquirer.

"I run a very small business. Am I really at serious risk of being hacked?"

Unfortunately, yes. In fact, hackers will often target small and home-based businesses precisely because they tend not to take protection seriously. Industry reports say that up to 85 percent of breaches occur in small, Level 4 businesses. It is important to comply with PCI regulations to minimize risk.

"How do I login to begin my Self-Assessment Questionnaire?"

Begin the process by visiting www.Compliance101.com/PCI. Your merchant ID number is your user name (you will find this in the top right-hand corner of your merchant statement) and your initial password is **compliance101** (you will be prompted to create a new password after your first login).

"I have already begun the process of PCI compliance. Do I need to let you know?"

If you have completed or are in the process of determining your business's PCI compliance, you will need to let us know. Please contact your merchant services representative and ask him/her to fax or email you a Merchant PCI Verification Questionnaire. Fill out this form and fax it back to us at 303.482.0347. Once your PCI compliance status is confirmed, you will receive notification of any necessary credits to your account.

"When will I be billed for PCI compliance?"

PCI compliance is billed quarterly through the merchant statement in January, April, July and October. Merchants approved during any of the three months preceding one of these billing months should expect to see the PCI fee on their billing statements during the billing month that follows. Merchants that are not certified as compliant could be subject to more frequent billing of PCI fees.

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 help 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.
- Save electronic copies of receipts in a secure location.
- Regardless of the method used for producing receipts (e.g., email, SMS, or attached printer), the method should mask the PAN [primary account number] in support of applicable laws, regulations, and payment-card brand policies. By policy and practice, the merchant should not permit the use of non-secure channels such as e-mail and SMS to send PAN or SAD [sensitive authentication data].

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

Face-to-Face

The following tips are intended to help 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 card reader and verify that the card number on the mobile device matches the card number on the card.
- When the card will not swipe and you must manually key in the card number to your mobile device, 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 mobile device, call the authorization center and follow their instructions.
- If you receive a "do not honor" or "decline" message through your mobile device, 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.

*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 e-commerce is available.

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

The following tips are intended to help 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. 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 e-commerce 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.).

Merchant Services' 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.
- Entering invoice numbers for corporate cards in order to achieve corporate card rates.
- Entering tax amount and customer code for corporate cards in order to achieve corporate card rates.

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.

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