Pace Payment Systems Card Acceptance Guide

As a Pace Payment Systems merchant, it is important to:

- Read, understand and abide by the Merchant Agreement and this Card Acceptance Guide.
- Take all necessary steps to prevent fraud.
- Follow best practices in accepting electronic payment methods.
- Advise Pace Payment Systems of any changes related to the merchant's business, such as changes in status, changes in business structure, address or contact information, or cancellations.
- Notify Pace Payment Systems upon cancelling or returning equipment.
- Keep up-to-date on all industry news and policy changes
- Advise Pace Payment Systems of any changes to merchant payment application, hardware or software.

Best Practices for Processing Payment Card Transactions

Processing face-to-face card present Transactions

Never Honor a Card when:

- The customer does not have the actual card.
- The card appears to have been altered or tampered with.
- Authorization is declined or merchant is instructed to pick up the card.
- The signatures do not match
- The merchant is suspicious – if suspicious Call the Voice Authorization Center and request a Code 10 authorization.

Processing key-entered transactions when the mag-stripe or chip cannot be read:

- Be sure the card hasn't expired
- Get a manual imprint
- Have the customer sign the imprinted sales draft
- Be sure the signature on the draft matches the signature on the card
- Make sure the AVS and CVV2 verifies
- Get customers contact information and bank name

Mail/Phone/Card-not Present Transactions

An authorization for a phone order, mail order, fax or Internet transaction does not guarantee against chargebacks. Shipments to an address different from the address verified as the cardholder's may result in an increase of chargebacks. You can verify the billing address of the cardholder when processing the sale through your POS device, with the Voice Authorization Center or by contacting the cardholder's bank. Our Customer Service team can provide the number of the cardholder's bank, if necessary Businesses that run card-not-present transactions are at a higher risk of receiving a chargeback and should require/retain all of the following items as applicable:

- Manual imprint the card
- Check customer identification to validate they are the cardholder
- Positive AVS and CVV response
- Verify with card issuer bank directly
- Retain proof of delivery
- Provide receipt of purchase to customer
- Be sure customer is aware of return/cancellation policy

Voice Authorization Instructions: Visa/MasterCard/ Discover/AMEX

If you need to call the Voice Authorization Center follow the steps below:

1. Dial 800-944-1111
2. Press 1 to authorize a card
3. Enter Bank ID number____________, then press # (number found on your terminal)
4. Enter Terminal ID number found on your terminal (even though it asks for the Merchant ID) _, then press #
5. Press 1 for a retail transaction 0r Press 3 for a MOTO transaction
6. Enter Card Number, Press#
7. Enter Exp. Date in MMYY format, Press #
8. Enter amount of charge, press #
   System will repeat charge entered. Press # if correct.
   If incorrect, press *, you will be asked to re-enter the amount
9. The system will give one of two responses:
   "Approved" followed by a 6-digit approval code. Write this code on the imprinter slip. The funds are now being held for you.
   OR
   "Do Not Honor" This means the card was NOT approved, it may be a lack of funds, a bad card etc. If you press zero to speak to a representative, they may be able to provide more information. If you receive a Do Not Honor response, request another form of payment.
10. There are three options to choose from at the end of the transaction:
    Press 1 to run another transaction of the same type
    Press 2 to run a transaction of a different type Press
    3 to end the call.

Important: If you are calling the voice authorization center because your POS device is not working, be sure to take an imprint of the card or write down the cardholder information including the card number, expiration date and the Authorization Code to **finalize and capture the sale once your terminal is operational**

Merchant Website

If you have a website, be sure the following information is included on your site:

- Merchant outlet address
- Merchant outlet country and country of domicile must be disclosed prior to the cardholder accessing payment instructions
- Complete description of the goods or services offered
- Merchandise return and refund policy clearly displayed on the checkout screen. Policy must be displayed on checkout screen and cannot take cardholder to a separate screen
- Consumer data privacy policy and method of transaction security used during the ordering and payment process
- Customer service contact including e-mail and /or telephone number
- Transaction currency (e.g. U.S> dollars, Canadian dollars)
- Export or legal restrictions (if known)
- Delivery policy
- Card acceptance brand marks in full color

Suspicious Activity

If you are suspicious or suspect fraud when processing a payment card transaction, contact the voice authorization center and request a Code 10 authorization. Some indicators of possible fraud are:

- Multiple orders on the same card
- Large ticket items
- Rush shipping
- Shipping to an international address

- Orders made on multiple cards/ shipping addresses

Retention of Sales Drafts

Keep complete records for all transactions in case of a chargeback event. Keep all sales drafts in a secure location with restricted access. When discarding any sales drafts, do so in a secure manner to ensure no data can be compromised. This information should be kept in case of chargeback.

Securing Sensitive Data

Sensitive data is any personally identifiable information that can be traced back to an individual. It is important that all customer information is kept as secure as their credit card data. For an ecommerce merchant you want to be sure to use a check out page that is hosted by a PCI-compliant provider. For all other merchants you will want to be sure that your system is set up to encrypt card numbers.

PCI Compliance

The Payment Card Industry (PCI) Data Security Standards are a set of rules that are regulated and mandated by the major credit card associations (Visa, MasterCard, Discover Card and American Express). These rules are passed on to the consumers, as well as all companies in the processing chain. To reduce the risk of lost, stolen or otherwise exposed sensitive cardholder data, this compliance is required to be upheld for all entities that accept credit cards. All merchants who accept credit cards as a form of payment for services or goods must have a program in place at the merchant level and at the processor's level. Both entities must abide by the regulations set by the card associations to assure that all cardholder data is always in a secure environment.

We have partnered with a 3rd party vendor to assist in providing an easy to use tool for higher success in achieving PCI compliance. Our PCI Compliance Program partner is ControlScan, an Approved Scanning Vendor (ASV) by the PCI DSS Council. They are a leading ASV provider of PCI Compliance solutions for small and medium-sized merchants. Their easy-to-use Smart SAQ Tools make achieving compliance less complicated. To access and validate your account please visit www.mycontrolscan.com. Login with the username and password provided in the notification you received or contact us.

- **PCI Protection Plan from Pace Payment Systems**
- **PCI Security Standards Council**
- **Visa**
- **MasterCard**
- **Discover**
- **American Express**
- **PABP List**
- **Glossary**
- **QSA List**

Data Compromise Incident

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS).

If you become aware that there may have been an occurrence that resulted in the unauthorized access to or disclosure of account data within your systems, you must notify us immediately.

FAQ's

What is a merchant account?

An account issued by Pace Payment Systems that allows a business to accept credit and debit cards. If you have questions on your account please call Customer Service, it is most helpful to have this number available. See Figure 3.

What is the transaction process?

See Figure 3

What is the difference between online debit and offline debit?

Online debit transactions require customer to use their PIN at the time of the transaction and causes the transaction to be routed through a debit network. Offline transactions require customers to sign a sales receipt and causes the transaction to be routed through Visa, MasterCard or Discover's network.

What is EMV?

EMV is a technology that is meant to help in preventing fraudulent activity for card-present transactions. The credit/debit card will be embedded with a smart chip, which will then be inserted into the terminal at the time of the transaction. In addition to the security chip, EMV also verifies the customer's identity with the use of a PIN or signature.

What is PCI DSS compliance?

PCI DDS is a set of requirements meant to ensure that all companies handle credit card information securely in order to prevent fraud.

What is a retrieval request?

A retrieval request is initiated when the issuing bank is requesting to verify that a transaction has actually taken place; typically, a copy of the sales draft or invoice showing what was purchased needs to be provided. These requests are time sensitive and should be provided within 15 days of the request date.

When will I receive my statement?

Statements are sent out within the first few business days of the month following the processing activity.

What is the difference between a refund/return and a void?

A refund, or a return, is when the merchant must run a transaction that returns the money back to the customer's credit/debit card. If the batch has not yet been settled, then the merchant can void out the transaction rather than issue a refund.

What is a batch?

When a merchant batches out it is grouping together all of the authorized transactions into one lump sum. Merchants typically batch at the end of each business day.

What is a chargeback?

A transaction that is disputed by the cardholder or card issuing bank and returned to the acquirer for processing back to the merchant. Cardholders may dispute charges for various reasons or the card issuer may initiate a chargeback because the merchant did not follow proper processing procedures. Some reasons for a cardholder dispute include the customer stating he did not receive the goods or services, didn't place an order or make the purchase, was not happy with the quality of the goods/services received and has been unable to resolve with the merchant. The issuing bank will initiate a chargeback when this happens, after which the merchant will need to validate and defend the purchase. The issuing bank can also initiate a chargeback if the merchant did not follow all the proper procedures, including obtaining a valid authorization for the transaction

What is the difference between Signature Debit vs. PIN Debit?

Debit cards, which are linked to customers' checking accounts at banks, come in two forms: signature-based and PIN-based. Both capabilities typically reside on the same card. Signature-based debit transactions (also known as "offline debit") are typically routed through either MasterCard or Visa, much like a credit card transaction.

PIN-based debit (also known as "online debit") requires the consumer to enter a personal identification number at the point of sale (POS); the transaction is then routed through electronic-funds-transfer (EFT) networks such as STAR®, Pulse®, NYCE®, and Jeanie®. These debit networks all require users to enter a PIN for both ATM and POS transactions. PIN transactions also can be run through EFT networks at MasterCard (Maestro®) and Visa (Interlink®).

Glossary

Address Verification System (AVS):
A security feature that requires merchants to supply address information for the cardholder in card-not-present transactions. The system verifies that the address entered matches the one the bank has on file and then confirms whether the information is valid or not. See Figure 2.

Authorization:
The initial request a merchant makes for a customer's bank to release funds for payment.

Approval Code:
A six-digit code that indicates approval of a transaction.

Batch:
A group of authorized transactions, typically used by the merchant at the close of business each day.

Cardholder:
The authorized user of a credit or debit card.

Cardholder Verification Value (CVV2):
A three- or four-digit number that is printed on a card to verify its authenticity. The "2" refers to the printed code on the card. (CVV1 is encoded on the magnetic stripe of the card). See Figure 1.

Chargeback:
A transaction that is disputed by the cardholder or card issuing bank and returned to the acquirer for processing back to the merchant. Cardholder's may dispute charges for various reasons or the card issuer may initiate a chargeback because the merchant did not follow proper processing procedures. You will be sent a chargeback notification directly or the debit from your bank account will serve as notice of the chargeback. If you disagree with the chargeback, be sure to submit your response by the given "respond by" date.

Some reasons for a cardholder dispute include the customer stating he did not receive the goods or services, didn't place an order or make the purchase, was not happy with the quality of the goods/services received and has been unable to resolve with the merchant. The issuing bank will initiate a chargeback when this happens, after which the merchant will need to validate and defend the purchase. The issuing bank can also initiate a chargeback if the merchant did not follow all the proper procedures, including obtaining a valid authorization for the transaction

Compliance:
Merchants that accept credit card transactions must meet or exceed regulations set by the local government, federal government, the card associations, and the Payment Card Industry Security Standards Council (PCI SSC).

Decline:
A response from the card issuer denying the use of the card for the attempted transaction. If a request for approval is declined, the merchant must ask the cardholder for another form of payment.

EMV:
EMV is a smart chip technology that offers an additional step for authentication beyond the traditional magnetic stripe card payment for card-present transactions (commonly called Chip and PIN or smart

cards). In addition to the security chip, which is placed inside of a reader during a transaction, EMV also verifies the cardholder’s identity with the use of a PIN or signature.

Fraud:
Any prohibited method used to access or use another person’s cardholder data.

Issuer:
A term used to define who issues the credit or debit card. The issuer bears the risk, essentially vouching for the creditworthiness of the customer.

Magnetic Stripe:
A type of card, sometimes called a mag stripe, capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card.

Merchant Acquirer:
Either a bank, a processor or independent sales organization (ISO) handling the merchant’s card acceptance. A processor or ISO will work with an acquiring bank, which is needed to officially accept payment on behalf of the merchant.

Merchant Identification Number (MID):
An identification number that represents a merchant’s point-of-sale terminal for the purpose of processing and tracking credit card transactions.

NFC:
Formally known as near field communication, NFC is a set of close-range wireless technologies that enable a connection for processing mobile payments.

Processor:
A company (often a third party) that handles credit card transactions for merchant banks and is usually paid per transaction. They are usually broken down into two types: front-end and back-end.

Refund:
A transaction returning money back to a customer’s credit or debit card that should be processed on the same card as the original transaction, after that transaction has settled. (Before settlement, see **Void**)

Retrieval Request:
A request sent by the issuing bank for a merchant to verify that a transaction has taken place. A customer has a 60-day window during which they may dispute a given charge. Merchants are charged by their merchant services provider (MSP) for each retrieval request. If the merchant does not respond in a timely basis, they can be charged an additional timeliness fee or lose the transaction completely.

Settlement:
This is the process merchants must complete at the end of the day in order to be paid for their transactions.

Voice Authorization:
A security measure used to ensure that a particular purchase is being authorized by the actual card-holding customer.

Void:
A credit card transaction that has been deleted before settlement. (After settlement, see **Refund**)
.

Figure 1

The CVV- CID is required on all keyed transactions. It can be found on the signature line on the back of a Visa, MasterCard, and Discover card and is 3 digits in length. The CID code is found on the front of an Amex card and is 4 digits in length. The responses are listed below:

CVV RESPONSES	
CVV2 Response	***Code***
CVV - CID Matches	M
CVV - CID Does Not Match	N
CVV- CID Not Processed	P
CVV- CID Should be on card, but the merchant has indicated that CVV2 is not present.	S
Issuer is not Certified	U

Figure 2

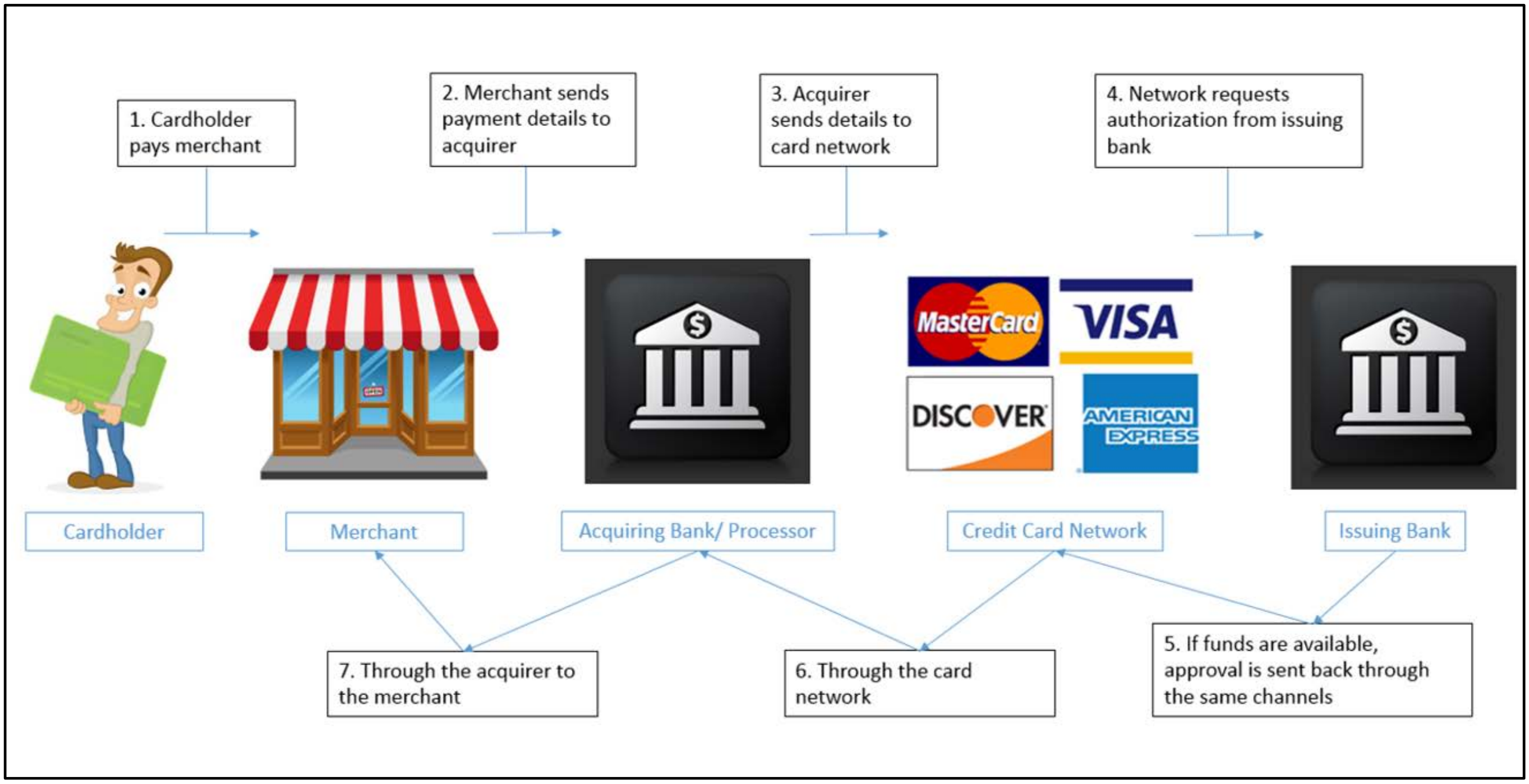
When entering the Address Verification Data, you must enter the street address in numeric format using the cardholder's billing street address in compressed format. See below for some examples:

COMPRESSED ADDRESS FORMAT	
Actual Address	***Compressed Format***
One Elm Street	1
123 First Street	1231
89 25th Street	8925
22 Walnut Street #23	2223
P.O. Box 12345	12345

AVS RESPONSE CODES			
Code	***Description***		***Action***
A	Address: Address matches, ZIP does not match		Verify Zip Code. Accept at your discretion.
B	Street address match. Postal code not verified because of incompatible formats.	Visa Only	Accept at your discretion.
C	Street address match. Postal code not verified because of incompatible formats.	Visa Only	Accept at your discretion.
D	Street address and postal code match for international transaction.	Visa Only	No Action Required.
E	Edit Error: Address information failed edit check.		Accept at your discretion.
G	Global- Non-AVS Participant. Address information not verified for international transaction.	Visa Only	Accept at your own discretion.
N	NO: Address and ZIP do not match.		Verify address and zip. Accept at your discretion.
M	Street addresses and postal codes match.	Visa Only	No Action Required.

P	Postal codes match. Street address not verified because of incompatible formats.	Visa Only	Accept at your own discretion.
R	Retry: System unavailable or time-out.		Accept at your discretion.
U	Unavailable: Address information is unavailable.		Accept at your discretion.
W	Whole ZIP: 9-digit zip match.		Verify address. Accept at your discretion.
X	Exact: Address and 9-digit ZIP match.		No Action Required.
Y	Yes: Address and 5-digit match.		No Action Required.
Z	ZIP: 5-digit ZIP matches, address does not match.		Verify address. Accept at your discretion.

Figure 3


1. Cardholder pays merchant
2. Merchant sends payment details to acquirer
3. Acquirer sends details to card network
4. Network requests authorization from issuing bank
MasterCard
VISA
DISCOVER
AMERICAN EXPRESS
Cardholder
Merchant
Acquiring Bank/ Processor
Credit Card Network
Issuing Bank
7. Through the acquirer to the merchant
6. Through the card network
5. If funds are available, approval is sent back through the same channels