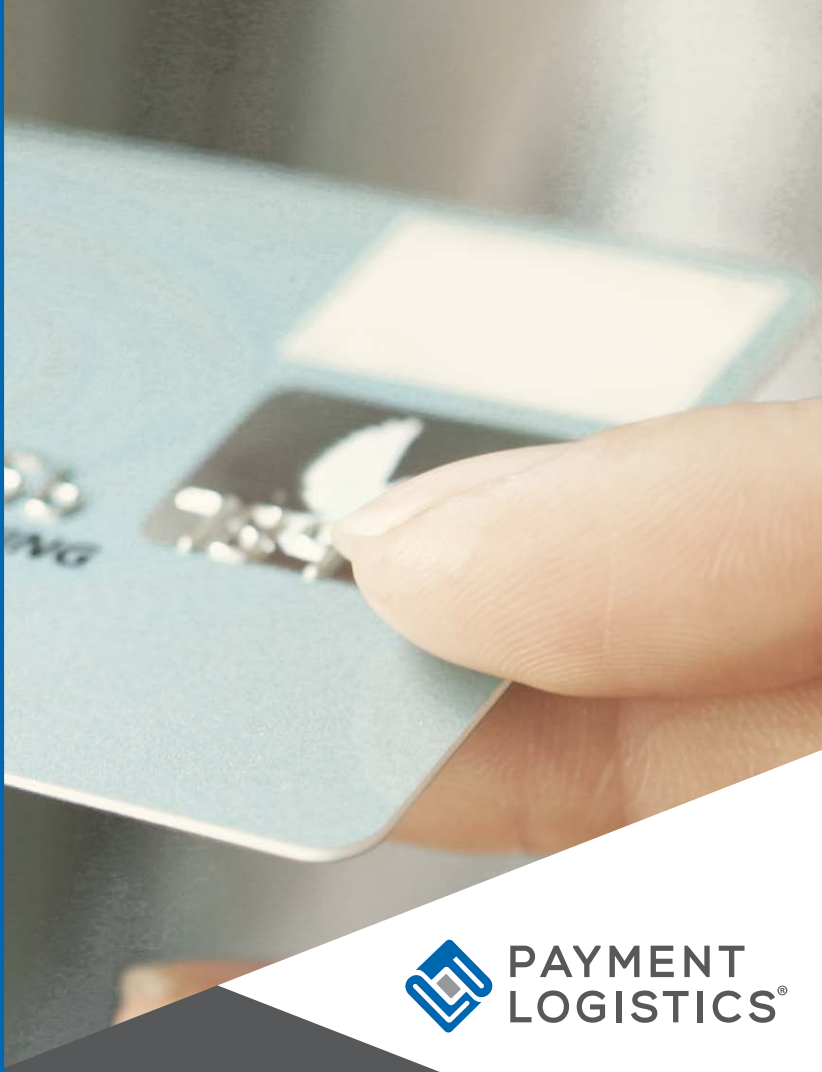


PAYMENT LOGISTICS®

Fraud Awareness & Card Acceptance Training Guide


INTERNATIONAL

Preface

The information provided in this training guide is not intended to be a complete or exhaustive list of procedures to follow. For a complete Payments Acceptance Guide, refer to the Program Guide of your merchant agreement at www.paymentlogistics.com/programguide. Card Organization rules may be available on websites such as:

https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf

https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf

www.americanexpress.com/merchantopguide

In this training guide

Protect Your Business

Be Cautious - Remember, if something seems too good to be true, it probably is. Be wary of customers who purchase big ticket items in quick succession.

Be Vigilant – Be able to identify outlying purchases by knowing your customers and their purchase patterns. Card NOT present transactions entail additional risk, particularly when international shipping is involved. A new customer making a large purchase may not be a financial windfall after all.

Keep your equipment current – With the recent EMV Liability Shift, it is vitally important to make sure your equipment can accept EMV chip cards. By upgrading to an EMV capable payment system, your business will demonstrate your commitment to following best practices for electronic payments acceptance while shielding yourself from costly EMV related chargeback liability.

Understand Your Vulnerabilities – You can be sure that potential fraudsters are aware of your business weaknesses. To prevent fraudsters from exploiting them, assess areas where you might be susceptible to fraud. Also, stay current with new software applications, patches and virus signature updates.

Stay Informed – Knowledge is power. Stay up-to-date by reading important announcements on your monthly statement and subscribing to relevant industry and news publications. Find out if there have been any recent scams in your neighborhood or in nearby areas.

Have an Ace in Your Pocket – Payment Logistics is experienced in detecting and preventing fraudulent activities. Don't hesitate to contact us with any questions or concerns. If you're not sure about a potential purchase, contact us right away. It's better to be safe than sorry.

Chargebacks - The Basics

In the most basic sense, a chargeback is the reversal of a charge to a cardholder's account. A chargeback is typically initiated by the cardholder or the issuing bank when the merchant account is debited and the cardholder's account is credited.

Common cardholder dispute reasons are:

- Counterfeit EMV card
- Card not in possession
- No cardholder authorization
- Goods/services not received
- Goods/services not as described
- Credit/refund not issued

Common card issuer dispute reasons are:

- Counterfeit EMV card
- No valid electronic authorization
- Settlement amount exceeds authorization tolerance limit
- Late presentment

Card Brands

VISA

mastercard

AMERICAN EXPRESS

DISCOVER

EMV & Chargebacks

Digital Wallets & NFC Payments Accepted Here

Pay

pay

SAMSUNG pay

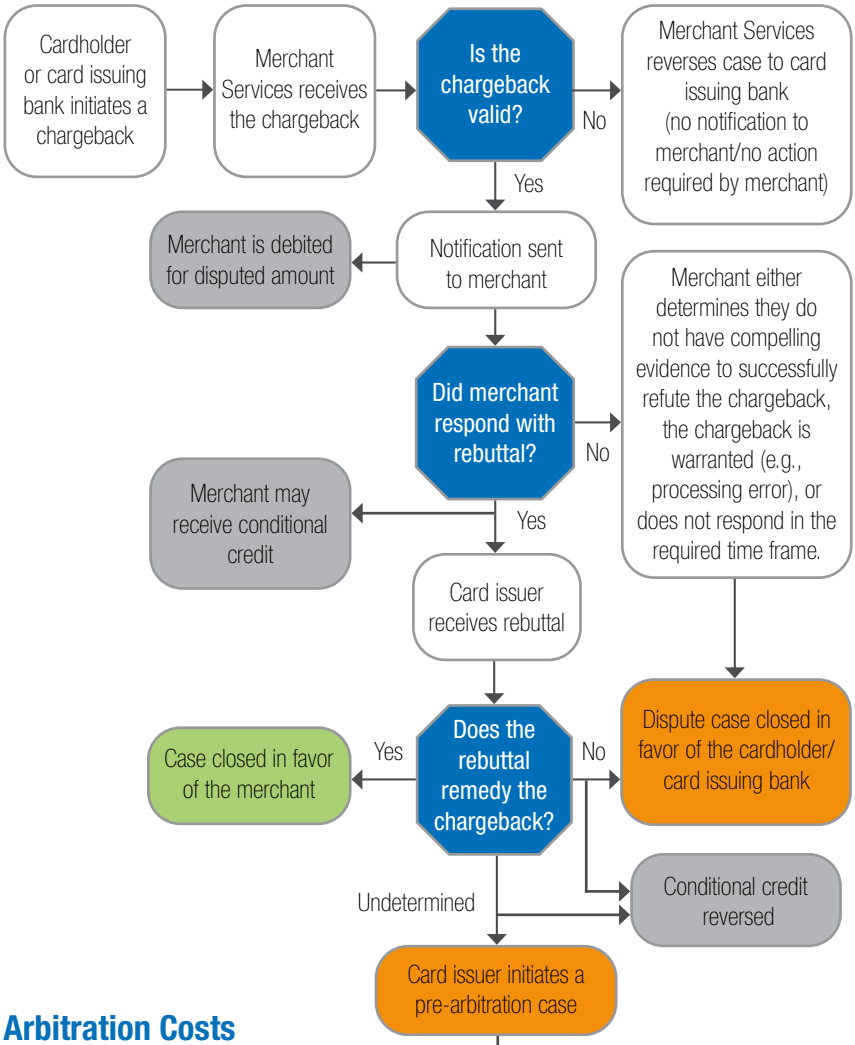
masterpass by mastercard

Visa payWave

To encourage merchants to upgrade their systems to support EMV, the card brands have changed the rules when it comes to who is liable for counterfeit credit and debit card fraud as well as some stolen card fraud. Previously, merchants who unknowingly accepted stolen or counterfeit cards in a card present environment were not liable for those transactions as long as they followed proper procedures. Now, most merchant types are liable for counterfeit card fraud transactions and in some cases stolen card fraud unless they update their systems to support EMV.

Updating your system to support EMV may discourage data security thieves from targeting your business, shield you from EMV related credit and debit card fraud liability and potentially save your business thousands of dollars in chargebacks. In most cases a system update will also simultaneously add support for NFC payments such as Apple Pay®, Android Pay® and other popular digital wallets.

Chargeback Process



Arbitration Costs

Card Organizations charge case filing review fees to merchants for arbitration cases that are ruled in favor of the issuer. The case can be sent to arbitration if you submit a response to a pre-arbitration case. The issuer has the choice to accept your response or pursue arbitration. In many cases, the arbitration fees are more than the disputed transaction amount. For this reason, you should carefully consider whether you should attempt to challenge a pre-arbitration chargeback, as challenging the case could be very costly. Contact us if you have questions about responding to a pre-arbitration case.

Common Fraud Scams - Card Present

Counterfeit Card - Fraudsters program the magnetic stripe of a compromised card onto a seemingly normal card and use it in a retail environment. In this circumstance, the counterfeit card looks and feels just like any card and the cardholder's ID may even match. If you swipe the card and your system prompts you to use the chip reader instead but there is no EMV chip visible, this is a counterfeit card transaction and you must request another form of payment or risk getting stuck with an EMV related chargeback. If you do not have a system capable of reading EMV chip cards, there is little you can do to defend against counterfeit card fraud. One measure would be to enable the last 4 fraud verification method. When doing so, the payment device will prompt you to enter the last 4 digits of the account number that is embossed on the card for every transaction. If the last 4 do not match, it's a counterfeit card transaction and you should request another form of payment. This provides only a small degree of protection compared to utilizing an EMV capable payment system.

Damaged Card - The actual cardholder attempts to utilize a card in a retail environment that has a damaged EMV chip and magnetic stripe. The card can't be read by the payment system and the cardholder has no other card on them so the store clerk is compelled to manually enter the account number into their system. In this scenario, the cardholder can easily commit "friendly fraud" by disputing the transaction and claiming they did not authorize the purchase. You should avoid manually entering account information when the card is present. The best course of action is to request another form of payment or decline to proceed with the sale.

The Cardholder Bully - Customer's card is declined. Customer insists the card is good and uses a cell phone (or even the merchant's phone) to seemingly dial the number on back of the card. Customer speaks to the so-called "bank representative," who clears everything up and then hands the phone to you. The "bank representative" tells you that the card is valid and that you need to run the transaction through as an offline or forced transaction utilizing the six digit approval code provided by them. They may even give you complete instructions on how to run the card based on the payment device you have.

In other scenarios, the merchant will immediately receive a fraudulent phone call after the declined transaction. The caller will identify themselves as an employee of Visa®, MasterCard®, Discover®, American Express® or the card issuing bank. If the cardholder hands you the phone and the caller attempts to clear up the misunderstanding by providing you with an authorization/approval code, this is an attempt to defraud you. Remember, the only valid authorization code is one that you obtain from your payment device or by calling the voice authorization phone numbers we supply to you.


VISA

Card Acceptance Procedures - Card Present

Follow these steps for Card Present Transactions:

EMV: If the customer's credit card is EMV enabled (chip), it must be inserted (i.e. "dipped") in the appropriate chip reader slot on the payment device. It is very important that EMV enabled credit cards are processed appropriately by reading the chip as opposed to the magnetic stripe. In the event that the customer tries to swipe an EMV enabled credit card, the EMV enabled payment device will instruct the user to insert the card into the chip reader. Please make sure to familiarize yourself with your equipment and train your staff accordingly.

NFC: If the customer has an NFC enabled card or device (such as an iPhone with Apple Pay), instruct them to tap the card/device over the NFC reader and hold it until the payment device indicates that it has received the data and is processing the transaction. Remember, for EMV enabled devices always comply with the device prompts.

PIN Bypass with Chip & PIN transactions: Chip and PIN transactions can represent a slight deviation from the norm. Some card issuers (including many foreign banks) issue cards that prefer or require a PIN code to process the transaction. When an EMV payment device prompts for a PIN on a credit card transaction, you can attempt to perform a PIN Bypass if A) your payment device supports it; and B) entering the PIN code is not practical such as in a scenario where the customer doesn't know it or the environment isn't conducive to it (like in a table service restaurant). When performing PIN Bypass (as simple as pressing the green enter key on a PAX device) during the authorization, the payment device tells the card issuer that the PIN is being bypassed and the card issuer gets to make the decision to approve the transaction without a PIN or decline it. If the card issuer approves the transaction, the merchant is protected from stolen card liability. If the card issuer declines the transaction, the merchant has the option of rerunning it and asking the customer to enter their PIN. There may be other ways of handling this scenario that minimize your risk. Please contact Payment Logistics technical support to discuss this further.

Traditional Magnetic Stripe: Swipe the credit card to electronically obtain authorization.

In the event the card fails to run through using an EMV, NFC or magnetic stripe, it is recommended that you request another form of payment. To reduce the risk of card present chargebacks due to fraud, you should avoid manually entering the account information into your electronic authorization device. If another form of payment is not available, you should carefully consider whether or not you want to proceed with the sale. If you do manually enter the account information, it is highly recommended that you also enter the three or four digit verification code. Additionally, you should obtain an imprint and perform a voice authorization by calling the Call Center at 800.228.1122 for Visa, MasterCard, Discover or American Express. For American Express direct accounts, call 800.528.2121. Make sure to record the 6-digit authorization number on the imprinted slip and also run an offline transaction on your payment device. If signature panel is not signed or reads "Check ID," request a state issued identification card and verify signature on ID matches the signature on receipt. **Important:** Not all Card Organizations accept an imprint as a means of verifying cardholder authorization.

1. Maintain possession of the card until after the cardholder has signed the receipt and you have compared the receipt signature against the signature panel on the back of the card. If the customer is using a contactless (NFC) form of payment, skip to Step #4. If signature panel is not signed or reads "Check ID," request a state issued identification card and verify signature on ID matches the signature on receipt.

2. Verify the last four digits on the receipt match the last four digits on card.

3. Request state issued identification, if anything is suspicious.

4. Make sure to retain a signed copy of a legible receipt.

5. If you suspect fraud while in the presence of the cardholder, conduct a code 10 authorization by completing the following:

- Call the Call Center at 800.228.1122 for Visa, MasterCard, Discover or American Express. If you are trying to do an authorization for an American Express direct account, call 800.528.2121.

- Calmly request a code 10 voice authorization.

- Follow the instructions of the operator and under no circumstances should you confront or try to apprehend the cardholder.

Common Fraud Scams - Card NOT Present

Credit Master / Multiple Cards - Customer provides several different card numbers and requests that you try all of them until the transaction goes through or spreads the payments over multiple cards. The card numbers provided typically will be identical except for the last four digits. There is a 99.9% chance that this is fraud.

Baiting - A new customer or one that has a limited purchase history with you may attempt to place one or two orders for $1,000 to build up trust, then proceed to place a $15,000 order. It is imperative you review these purchase patterns closely.

Independent Shipping Carriers / International Shipping - Customer places a large order and wishes to utilize their own shipping carrier (which is not a common carrier). Customer claims that their carrier does not accept credit cards and would like for you to charge their card and send a money order to the carrier. This usually involves international shipping and the "shipping" expense is often more than the cost of the goods being purchased. International shipping is popular for fraudsters because the goods are nearly impossible to track and recover. Visa AVS is not able to validate except in the US, Canada and the United Kingdom. Therefore, be wary of shipping to Ghana, Indonesia, Nigeria and Venezuela.

Stolen Credit Card - Customer places order, transaction is approved and AVS may even match. Shipping could also be to the verified billing address. Typically, customer communication is done through email utilizing a free email service (Hotmail, Yahoo, Gmail, etc) and customer is adamant about receiving a tracking number. The transaction appears legitimate until the package is re-routed mid-delivery and sent to a third party address with no notification to the merchant. This is one of the hardest types of fraud to combat. Be vigilant with customers that are overanxious to get their hands on a tracking number or those who display erratic or abnormal behavior. Utilizing the card security code can be the greatest defense against this type of fraud.

Too Good To Be True - Abnormally large orders of the same item, multiple orders in a short time span or multiple big ticket items are a red flag and should be reviewed closely.

TDD Hearing Impaired Relay - System designed for use by individuals who have impaired auditory senses. Typically, you hear a computerized voice or an operator who identifies themselves as someone who is there to facilitate the transaction. These transactions are almost always fraudulent especially when accompanied by other characteristics of fraud.

First-Time Shopper - Be on the lookout for new customers who ask a lot of questions regarding shipping, how transactions are handled or what forms of payment you accept.

Rush or Overnight Shipping - Crooks want fraudulently obtained items as soon as possible in order to resell them and are not concerned with additional delivery charges.

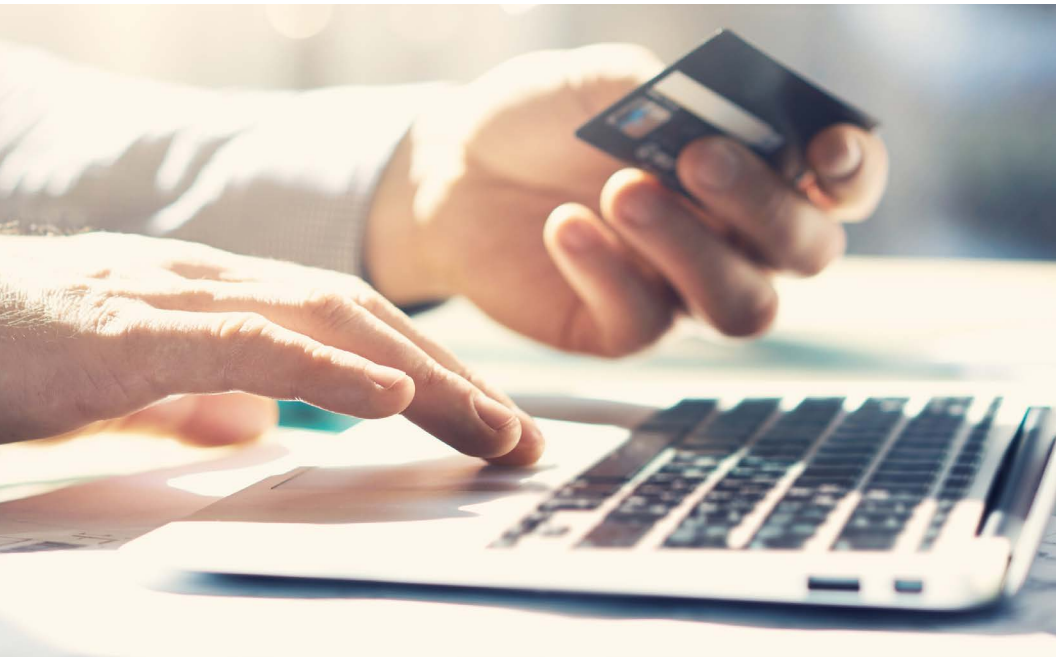
Multiple Cards, One Shipping or IP Address - This could involve an account number generated using special software, or even a batch of stolen cards. If several different cards with different names are being shipped to the same address, be very leery of the order. Multiple cards from one IP address could indicate a fraud scheme, especially when purchases are extravagant or accompany other signs of fraudulent activity.

Multiple Transactions, One Billing Address & Multiple Shipping Addresses - This could represent organized activity, rather than one individual at work. In many instances, shipments will involve PO Boxes or freight forwarding centers.

Multiple Transactions on One Card in a Short Period of Time - This could be an attempt to "run a card" until the account is closed. Fraudsters will continually purchase items, running several small batches of purchases until the card is maxed out.

Ecommerce Card Testing- Fraudsters test stolen credit card numbers by attempting to make small purchases online to determine if the stolen card data can be used to make purchases. Once they receive an approval on a tested card, they will proceed to use the card to make fraudulent purchases or sell the card data on the black market. To help prevent card testing:

- Contact your gateway provider to ensure Velocity Filters are enabled. Filters will limit the amount of times a card can be attempted and the number of times a single IP address (user) can submit a request for an authorization.
- Add a CAPTCHA to your website.



Card Acceptance Procedures - Card NOT Present

Follow these steps for Card NOT Present transactions:

1. Confirm order with customer to ensure there is no confusion. Confirm they understand exactly what they are purchasing and how much they will be charged.
2. Verify you are using the correct payment method for the specific sale.
3. Obtain the following customer information to perform verification with card issuer:
    - Full name as it appears on the card
    - Home telephone number
    - Billing address (Refer to #5 for further information on AVS Verification)
4. Request the Card Verification Value (CVV2) or Card Verification Code (CVC2).
    - Visa / MasterCard / Discover – three digits located on the back of the card at the end of the signature panel after last four digits of the credit card #
    - American Express – four digits located on the front of the card in the top right hand corner
5. AVS Verification
    - Validate AVS to validate billing address and review the response (A = address only, Z = zip only, Y= both match, N = no match, U = AVS unavailable)
6. Perform card security code validation (CVV2, CVC2, etc) and review the response.
7. Whenever possible, ship to the verified billing address and utilize a shipping company that does not permit re-routes of deliveries and requires customer signatures.

If you suspect fraud or would like additional verification:

1. Perform name verification with the card issuing bank
    - Contact the Call Center at 800.228.1122 for Visa, MasterCard, Discover or American Express and select the option to lookup the Bank Telephone number. For American Express direct accounts, call 800.528.2121.
    - Call card issuing bank, select the prompt for security, customer service, or name verification. Tell the Customer Service Agent (CSA) that you are a merchant accepting a transaction from one of their cardholders and that you are performing additional due diligence before you finalize the transaction. Tell them you would like to perform a name verification where you provide all of the information and the CSA simply says “Yes or No” if it matches.
    - You can also ask the bank to say “Yes or No” to the home telephone number, street address and zip code (individually or together).
2. Contact Payment Logistics at 888.972.9564, identify yourself as calling from a client of ours and request assistance with verifying the legitimacy of a transaction.

PCI Compliance

Merchants are required to protect stored data and encrypt transmissions of data across open/public networks, using methods indicated in the Payment Card Industry Data Security Standard (PCI DSS) which is available at www.pcisecuritystandards.org.

Use strong passwords and change default passwords – Change your passwords regularly and do not share passwords. Each employee should have their own login ID and password. Never use the same password for more than one website.

Protect card data – Only store card data that you need. Securely destroy card data that you no longer need. If you need to retain a paper copy with sensitive card data, mark through the sensitive data until it is unreadable and secure the document in a locked drawer or cabinet. Do not accept or send credit card payment details via email.

Protect payment terminals and inspect for tampering – Protect payment terminals by keeping them out of customers' reach when not in use. Look for signs of tampering, or new devices or features that you do not recognize, and only allow repairs from authorized personnel. If you suspect your terminal has been subject to tampering or it needs to be repaired, contact our customer service team right away.

Use trusted business partners – Confirm the security of your service providers to ensure adherence to PCI DSS requirements.

Install patches from your vendors – Follow your vendor and service provider's instructions for installing required patches promptly.

Protect in-house access to your card data – Limit access to payment systems, data, and applications on a business need-to-know basis.

Use anti-virus software – Set your anti-virus software to automatically update and schedule automatic full system scans.

Scan for vulnerabilities and fix issues – Conduct regular vulnerability scans through an approved PCI scanning vendor and correct issues detected by the scan. Contact us for questions about PCI validation or for help correcting detected issues.

Use secure payment terminals and solutions – Use equipment that provides the best security and supports EMV chip. If you utilize a legacy payment integration with your POS system that relies on magnetic stripe reader devices, you are most likely increasing your risk of a cardholder data security breach.

For ecommerce, use a PCI DSS compliant ecommerce service provider to securely process transactions and/or manage your website.

APPENDIX: AVS Response Code Definitions

Code Summary		Value Description	VISA	mastercard	AMERICAN EXPRESS	DISCOVER
X	Match	Street address and 9-digit zip code both match		✓		
Y	Match	Street address and 5-digit zip code both match	✓	✓	✓	✓
A	Partial Match	Street address matches, but both 5-digit and 9-digit zip code do not match	✓	✓	✓	✓
W	Partial Match	Street address does not match, but 9-digit zip code matches		✓		✓
Z	Partial Match	Street address does not match, but 5-digit zip code matches	✓	✓	✓	✓
N	No match	Street address, 9-digit zip code, 5-digit zip code ALL do not match	✓	✓	✓	✓
U	System Unavailable	Address information unavailable. Returned if non-US. AVS is not available or if the AVS in a US bank is not functioning properly.	✓	✓	✓	✓
R	System Unavailable	Retry - Issuer's system unavailable or timed out.	✓	✓	✓	
E	Invalid	AVS data is invalid.	✓			
S	Not supported	US issuing bank does not support AVS.	✓	✓	✓	

APPENDIX: Int'l AVS / CVV2 Response Code Definitions

International AVS Response Code Definitions		
Code/Summary		**Value Description**
D	Match	Street address and postal code match for International transaction
M	Match	Street address and postal code match for International transaction
B	Partial Match	Street address match for International transaction. Postal code not verified due to incompatible formats
P	Partial Match	Postal codes match for International transaction, but street address not verified due to incompatible formats
C	No match	Street address and postal code not verified for international transaction due to incompatible formats
I	No match	Address information not verified by international issuer
G	Not Supported	Non-US Issuer does not participate

Card Verification Value (CVV2) Response Codes	
Code	**Value Description**
M	CVV2 Match
N	CVV2 Not Match
P	Not processed
S	Issuer indicates that CVV2 data should be present on the card, but the merchant has indicated data is not present on the card
U	Issuer has not certified for CVV2 or Issuer has not provided Visa with the CVV2 encryption keys
Empty	Transaction failed because wrong CVV2 number was entered or no CVV2 number was entered

www.paymentlogistics.com
www.pcilogistics.com