# Table of Contents

**About This Guide** ................................................................. 1  
  - Background .................................................................. 1  
  - Guide Purpose ............................................................. 1  
  - Who Should Use This Guide .......................................... 1  
  - How This Guide Is Organized ........................................ 2  

**I. Payment Acceptance Basics for Fuel Outlets** .................. 3  
  - Introduction ................................................................... 3  
  - Payment Acceptance and Fuel Retail Outlet Design .......... 3  
  - Outlet Design for Greater Payment Efficiencies .............. 4  
  - How Visa Payment Processing Works – Start to Finish ....... 4  
  - Interchange and Fuel Purchases ..................................... 7  
  - Batch Clearing and Real-Time Processing ....................... 8  

**II. Processing Considerations and Management** ............... 9  
  - Processing Issues and Impacts ....................................... 9  
  - Reducing Risks in Processing ....................................... 10  
  - Streamlining the Purchase Process with Visa’s Real-Time  
    Clearing (RTC) Program ............................................... 11  
  - How RTC Works – From Start to Finish ......................... 11  
  - RTC Benefits ................................................................ 12  
  - Key RTC Considerations .............................................. 12  

**III. Authorization and Clearing** ....................................... 13  
  - Owner/Operator Best Practices ..................................... 13  

**IV. Fraud Management** ................................................. 15  
  - Tools and Controls for Optimal Payment Processing and  
    Reduced Risk ............................................................... 15  
  - Fraud Mitigation – Owner/Operator Best Practices .......... 16  

**V. Chargeback Management** ......................................... 22  
  - The Chargeback Process ............................................... 22  
  - Handling Chargebacks ............................................... 23  
  - Common Retail Fuel Segment Chargebacks and Best  
    Practices ..................................................................... 23  
  - Copy Request Management Best Practices ..................... 25
VI. Interchange Costs Management ..............................................27
    Interchange and Pricing ..................................................27
    Interchange Best Practices ..............................................27

VII. Tender Mix Management ..................................................28
    Facilitating Customer Choice and Preferences ......................28
    Tender Mix Management Best Practices ..............................28

VIII. Quality of Service .........................................................29
    AFD Best Practices .......................................................29
    AVS Best Practices .......................................................29
    Attended and In-Store Service Best Practices .......................29

Glossary of Terms ..............................................................31
About This Guide

Background

Card acceptance is instrumental to success in fuel retailing. More than ever, consumers want convenient, efficient, and easy-to-use services when purchasing fuel. For today’s retail petroleum merchant, card acceptance helps:

- Drive higher purchase sizes,
- Speed up the fueling process for customers, and
- Serve as a valuable means to retain customer loyalty.

In addition to these opportunities in the fuel segment, card acceptance brings with it certain responsibilities and investment decisions, including the need to carefully balance risk and cost mitigation with a positive customer experience.

Guide Purpose

The Visa Payment Acceptance Best Practices for Retail Petroleum Merchants guide provides optimal ways to process card transactions and manage the risks posed by card payments in the fuel segment. The guide offers a set of recommended best practices for establishing transaction amount limits at the automated fuel dispenser, using Visa’s Real-Time Clearing (RTC) program, incorporating system and employee driven fraud controls, managing card acceptance costs, minimizing the risk of loss from chargebacks, and ensuring quality service through programs such as the Visa Easy Payment Service (VEPS).

Who Should Use This Guide

The information contained in the Visa Payment Acceptance Best Practices for Retail Petroleum Merchants guide is geared toward the actions and decisions most pertinent to retail petroleum owners and operators worldwide. It also includes best practices and on-the-job support tools for attending managers and employees.

Key Point to Remember

In this guide, the term automated fuel dispenser refers to an unattended device used to dispense fuel, such as gasoline, propane, or diesel fuel, and which accepts payment cards.

Visa Easy Payment Service (VEPS) is a global program that allows qualifying low value transactions at specific merchants to take place without cardholder verification and without a receipt unless a receipt is requested by the cardholder. Service Stations (MCC 5541) are eligible to participate in VEPS for in-store transactions.

Note: Merchants are solely responsible for their decisions whether and how to implement these recommended best practices. Results from implementing the best practices are not guaranteed, and may differ from merchant to merchant.
This guide is divided into eight sections, each with a different main focus.

- **Section I. Payment Acceptance Basics for Fuel Outlets** offers a general overview of a retail petroleum merchant’s payment acceptance environment.

- **Section II. Processing Considerations and Management** covers a number of principles that are key to achieving fuel transaction processing and funding efficiencies.

- **Section III. Authorization and Clearing** delves into fundamental best practices for ensuring you have a secure and efficient system for processing authorization requests and transaction data.

- **Section IV. Fraud Management** defines the types of tools and controls needed to reduce payment acceptance risk and combat fraud. It offers a set of best practices for owners and operators, as well as managers and employees.

- **Section V. Chargeback Management** describes the chargeback process and the three most common reasons for chargebacks in the retail petroleum environment. The section also includes best practices for avoiding these common chargebacks and handling copy requests.

- **Section VI. Interchange Costs Management** emphasizes the need to process transactions in accordance with rate qualification criteria to avoid interchange downgrades. Best practices are provided to help you control card acceptance costs and monitor qualification levels.

- **Section VII. Tender Mix Management** discusses the trade-offs that must be considered by retail petroleum merchants before making payment acceptance decisions. A set of best practices has been included to help in the preparation of a clear strategy for an overall, appropriate tender mix.

- **Section VIII. Quality of Service** provides a list of best practices/recommendations for creating a retail petroleum environment that successfully meets your customers’ need for speed, efficiency, and ease-of-use.

- A **Glossary of Terms** has also been included to define commonly used terms throughout this guide.
I. Payment Acceptance Basics for Fuel Outlets

**Introduction**

Visa cards offer many tangible benefits to retail petroleum merchants by enabling them to:

- Speed transaction times and serve more customers,
- Reduce opportunities for theft, and
- Maximize the amount of fuel that customers can pump in one visit.

Retail petroleum merchants worldwide have a number of choices when it comes to deciding how a fuel payment transaction should be incorporated into the customer’s broader sales experience. **Outlet set-up options vary by country and are heavily influenced by cost of labor and/or technology considerations, as well as the fuel retailer’s operating environment.**

**Outlet Design Options**

Where and when a customer pays for fuel greatly influences the physical layout of a fuel station and the related costs of that design.

There are several fuel retail outlet designs in relation to payment acceptance, each of which is described below.

- **Single, In-Store Payment** – Many retail outlets still operate with only one stand-alone terminal in the store. This is particularly true for those retailers who are new to acceptance or for retailers who struggle to justify the costs of point-of-sale (POS) hardware in the forecourt. Under such a design, the retailers must determine if they should require their customers to pay before they start filling up at the fuel dispenser, or to trust that they will pay when done fueling.

- **Payment at the Automated Fuel Dispenser with Convenient In-Store Payment** – This design is the optimal choice for offering the quickest and most convenient fuel purchase to the customer. It also saves labor costs by requiring fewer attendants. However, automated fuel dispensers and related payment hardware and software can be expensive relative to other options. Forecourt technology retrofit can also be difficult, particularly if components need to be placed under concrete. Although, wireless technology offers solutions to avoid some construction costs.

- **Payment in the Forecourt with Convenient In-Store Payment** – An unattended payment kiosk or pedestal in the forecourt that supports multiple fuel dispensers can offer many of the advantages of payment at the fuel dispenser, at a lesser cost and construction impact.
Attended Fuel Dispenser - Many countries around the world require an attendant to pump fuel. In low-labor cost countries, the use of attendants simply makes good business sense. Besides managing the fuel dispenser and providing other discrete automotive services, the attendant may accept cards and cash for payment. The location of the POS hardware where attendants authorize and process the transactions can vary, depending on the outlet configuration. Wireless terminals allow the attendant to remain in the forecourt, while reducing opportunities for fraudulent activity; particularly when the POS is integrated with the fuel dispenser.

Outlet Design for Greater Payment Efficiencies

Retail petroleum merchants have a number of factors to consider when laying out their payment operations. On the one hand, there is a desire for greater speed at the POS to increase customer throughput. Automated fuel dispenser payment technology was created to do just this, and by any measure is revolutionary to retail fuel payments. Technology, however, does not come without cost, therefore making the pay-at-the-fuel dispenser design a challenge in many countries. In addition to fueling convenience, retailers must often balance a desire to promote both fuel and in-store sales (where margins tend to be three to five times higher than fuel sales).

Retail petroleum merchants differ in their opinions on the ideal set-up for promoting both fuel and in-store sales. The variation in thinking is often driven by the specific circumstances of the retailer. For example:

- **Smaller retailers** may not have customer queuing challenges, so they can afford to service customers in the store, with the additional benefit of driving store sales. They also tend to lack the fuel sale volumes to support expensive forecourt technology investment.

- **Larger volume retailers** often find, however, that the best way to promote in-store sales is to ensure quick payment at the automated fuel dispenser in order to free up dispensers as soon as possible, and to eliminate the wait time of standing in line in the store. Customers with time constraints do not want to wait and will consequently leave without getting fuel or going into the store. By alleviating lines in the store, customers interested in a quick purchase in the store will be more likely to do so if lines in the store are short or non-existent.

How Visa Payment Processing Works – Start to Finish

Visa operates and maintains VisaNet—the world’s largest consumer payment system. It’s made up of a collection of systems that facilitates the payment transaction process from the time a customer presents a Visa card to a merchant until that transaction ends up on the cardholder’s statement. This is done through:

- An **authorization service** by which Visa card transactions are approved or declined by the card issuer (or by Visa on the issuer’s behalf).

- A **clearing and settlement** service that processes Visa transactions electronically between merchant banks and card issuers to ensure that:
  - Information moves from merchant banks to issuers for posting to cardholder accounts.
  - Payment moves from issuers to merchant banks for Visa transactions.
I. PAYMENT ACCEPTANCE BASICS FOR FUEL OUTLETS

The following illustrations show the lifecycle for a credit, debit, or prepaid transaction at a fuel outlet. The first diagram walks through the authorization process for an automated fuel dispenser; the second depicts the authorization processing steps for an in-store transaction. Please note that the processing events and activities may vary slightly for any one merchant, merchant bank, or card issuer, depending on card and transaction type, and the processing system used.

> AUTHORIZATION AT THE AUTOMATED FUEL DISPENSER

1. Cardholder swipes, inserts, or waves card at the automated fuel dispenser, then enters a PIN or postal code if prompted.
2. The Merchant Bank electronically sends the authorization request for a single unit of currency to VisaNet. This type of authorization request is known as a “status check.”
3. VisaNet passes on the request to the card issuer.
4. Card Issuer approves or declines the transaction.
5. VisaNet forwards the card issuer’s authorization response to the merchant bank.
6. Merchant Bank forwards the response to the merchant.
7. Merchant receives the authorization response. If approved, the cardholder can begin pumping fuel up to the prefixed amount allowed by the terminal.

> AUTHORIZATION IN-STORE

1. Cardholder presents a Visa card to pay for purchases.
2. Merchant swipes the card. For pre-dispense, they enter the estimated transaction amount (or amount requested by cardholder). For post-dispense, the actual amount is entered, and transmits an authorization request to the merchant bank.
3. VisaNet passes on the request to the card issuer.
4. Card Issuer approves or declines the transaction.
5. VisaNet forwards the card issuer’s authorization response to the merchant bank.
6. Merchant Bank forwards the response to the merchant.
7. Merchant receives the authorization response. Whether pre- or post-dispense, the merchant will submit the final amount into clearing.

A Brief Look at Partial Authorization

As an alternative to declining a transaction, an issuer can use a partial authorization to return an approval for a partial amount. This is an amount that is less than the transaction amount requested by the merchant, when the available card balance is not sufficient to approve the transaction in full. Merchants supporting partial authorization allow the cardholder to use up to the available card balance amount.
Clearing and Settlement

Though the terms “Clearing” and “Settlement” are often used to describe the final steps of payment processing, they are two distinct processes.

- **Clearing** occurs when transaction data is delivered from a merchant to a merchant bank, and then subsequently to a card issuer for posting to a cardholder account.

- **Settlement** involves the reporting and transfer of amounts owed by one bank to another as a result of clearing. Visa “net” settles with the merchant banks and card issuers on a daily basis. Through VisaNet, issuers must pay the merchant banks for transactions that have been completed by their cardholders.

**Key Point to Remember**

Settlement does not affect a merchant directly but can affect when the merchant bank makes funds available to the merchant. The merchant bank usually credits the merchant’s account for the amount of the transaction (minus any agreed on merchant fees) within 48 hours of VisaNet settlement.
I. PAYMENT ACCEPTANCE BASICS FOR FUEL OUTLETS

Interchange and Fuel Purchases

Interchange is the transfer rate exchanged between the merchant bank and card issuer each time a Visa payment product is used. Interchange strikes the right economic balance between participants in the payment network. Among other things, it varies by the type of merchant, cost of the sale, payment product type, processing technology the merchant uses and region or country. For example, merchant attributes may require different interchange categories and processing strategies. Similarly, the type of payment product used (e.g., credit, debit, or prepaid) and how that product is used (e.g., face-to-face or over the Internet) affect the interchange rate and processing requirements.

Merchant banks must pay an interchange fee to issuers on all purchase transactions to compensate for the cost and risk of issuing cards. VisaNet then credits the merchant bank for the amount of the transaction minus the Interchange Reimbursement Fee (IRF) amount owed. The merchant bank then pays the merchant the transaction amount minus the Merchant Discount Reimbursement (MDR), which is the IRF plus the merchant bank costs.

Batch Clearing and Real-Time Processing

It is important for retail petroleum merchants to know that there are two data processing methods: batch clearing and real-time processing, and that these processing methods have an impact on how they do business.

- With batch clearing, transaction data is exchanged twice between members. For this reason, it is often called “dual message processing.”
- The authorization message occurs online at the time of the transaction; clearing and is performed later in a second message. Generally, clearing messages are grouped into a “batch,” and cleared as part of “end-of-day” processing. Visa credit, debit, and prepaid transactions can be processed using batch clearing. Fuel purchases typically use batch clearing.
Batch Clearing and Real-Time Processing (continued)

- With **real-time processing**, all transaction data flows online. Where the final amount is known at authorization time, the same online message that carries the authorization request can also provide the issuer with all the information it needs to post the transaction to the cardholder’s account. Thus, real-time processing is often called “single message processing.” However, in fuel retailing, where the final amount is generally not known at time of authorization, a status check is performed. This is followed by a second online clearing message when the final amount is known. Unlike batch clearing, the online clearing messages can be sent as soon as the final amount is known. Fuel retailers wishing to take advantage of real-time processing will typically use the latter form. An alternative process is available under Visa’s Real-Time Clearing (RTC) program, which is discussed later in this document.

For either processing method, where the final amount is not known at the time of authorization, a pre-authorization is performed, normally as a status check (i.e., an authorization for a single unit of currency). An approved status check provides authorization protection up to a specified amount. (Please check with your Visa representative for the amount defined for your market.)
II. PROCESSING CONSIDERATIONS AND MANAGEMENT

II. Processing Considerations and Management

Processing Issues and Impacts

The separation and time lags involved in fuel purchases can be problematic as the retailer typically does not actually know the purchase amount when authorizing transactions in the forecourt, or for pre-dispense amounts in the store. As such, the card issuer, in response to an authorization request, must keep a hold in place on a customer’s funds (debit or prepaid) or line of credit (credit) which often exceeds the amount of fuel purchased.

There are a number of principles important to fuel transaction processing and card acceptance.

- First, the merchant must decide how to process card transactions in the store. In some cases, the retailer may allow the fuel to be dispensed, and then receive payment for the actual amount from the consumer. However, it is more likely that the cardholder will need to come into the store before dispensing the fuel. If performed in-store, the merchant can either obtain an authorization for an estimated amount, or retain a “valuable” against the future payment. This valuable is often the driver’s license or the payment card itself.

- The use of an estimated amount for authorization can be effective, particularly if guided by the customer request to allow a particular amount of fuel to be dispensed. The retailer needs to ensure the dispenser only gives out fuel up to the authorized amount. Also, if less fuel is dispensed than authorized, the difference must be reversed with an authorization reversal. Use of the authorization reversal will also eliminate unnecessary holds on cardholder funds.

- Retaining a valuable will allow the retailer to authorize for the actual amount. However, when the valuable is a driver’s license or payment card, this creates an opportunity for compromise of cardholder information, leading to fraud and identity theft, and significant damage to the relationship with the customer. For this reason, the use of estimated amounts and authorization reversals for the unused portion of the authorized amount, is strongly recommended.

- The merchant must make important decisions about how the customer is prompted to interact with the automated fuel dispenser terminal. For example, the merchant must determine whether to support PIN prompt (particularly important in EMV chip countries). In the U.S., a merchant in a high-fraud area may prompt for a zip or postal code using Visa Address Verification Service (AVS). These decisions are important when it comes to minimizing fraud and for managing acceptance costs.

2 This Visa rule is currently in effect for the U.S., and becomes effective globally as of April 2010.
• Secondly, the merchant and its merchant bank must determine the appropriate amount to authorize and then subsequently the amount of fuel to pump for the customer based on that authorization. It is important for merchants to consider that transactions exceeding the allowable limit for that environment are potentially at risk for chargeback according to Visa operating guidelines. (This chargeback may be limited to the amount exceeding the limit.) This limit is important for both setting transaction amount limits for authorization policy and also for setting limits on fuel dispense.

Reducing Risks in Processing

Issuer holds on account funds during processing. Generally, the hold amount will exceed the fuel purchased. (Either the estimated amount exceeds the actual purchase or the issuer holds amount authorized by status check.) Account holds present risk to all parties involved including the issuer and merchant, as they can restrict future purchases and use of account funds by the consumer. As the customer may blame the merchant for the funds restriction, merchants can help minimize this risk by:

• Setting authorization amounts appropriately, preferably through use of a status check.
• Submitting clearing messages for the final amount as promptly as possible.
• Reversing unused authorizations, or reversing the portion of the authorization that is not used. Effective April 2010, Visa requires that any authorization or portion of authorization that is not used must be reversed using an authorization reversal.

Using the above best practices can reduce the instances of unnecessary holds.

How Unnecessary Holds on Fuel Purchases Can Lead to Customer Service Issues

For Example:

A Visa cardholder has US $75.00 in her deposit access account. When she inserts her debit card into the automated fuel dispenser terminal to get fuel, the merchant requests an authorization status check for a single unit of currency.

The card issuer approves the transaction and places a US $75.00 hold on the cardholder’s available funds.

The actual fuel purchase amount is US $35.00.

The next day, when the cardholder tries to make a US $10.00 purchase using her debit card, the transaction is declined because of insufficient funds.

The concerned cardholder ends up calling the retail petroleum merchant to find out what happened, and then calls the issuer. She learns that the estimated hold amount has reduced her available cash. Now the cardholder is not only concerned, but also unhappy with the purchase situation, affecting her relation with the merchant.

Disparities between the authorized amount and settled amount. This can present some degree of risk when fuel prices are high and large ticket transactions result in settlement amounts exceeding authorized amounts. It can also increase interchange costs and increase chargeback liability.
II. PROCESSING CONSIDERATIONS AND MANAGEMENT

- Merchants should ensure that limits are in place for the fuel dispensed, and that these limits do not exceed the authorized amount.
- As noted above, authorization reversals must be used to reflect the actual transaction amount. Reversals for transactions authorized via status check are required if the transaction is cancelled (no fuel dispensed), but should not be used if any fuel is dispensed.

Visa’s Real-Time Clearing (RTC) program has been designed to help retail petroleum merchants facilitate faster, more affordable, and convenient payment acceptance at the pump. The program has three primary goals:

- Reduce the impact of holds on cardholder accounts/funds.
- Provide greater protections for merchants and merchant banks.
- Speed the flow of funds through the payment system.

To accomplish these goals, the RTC program adds business rules to the real-time processing described earlier. The flow makes use of a pre-authorization, followed by a Sales Completion to finalize the transaction. RTC can also qualify stations’ transactions for better interchange rates at higher ticket amounts, which can lower station owners’ costs.

> TYPICAL RTC PROGRAM FOR FUEL PROCESS FLOW

Here is a high level look at how the RTC program works.

1. Cardholder swipes/inserts/waves his or her card at the automated fuel dispenser. The cardholder may or may not be prompted for a PIN or for a zip or postal code assigned to the card.
2. The merchant submits a pre-authorization request based on an estimated transaction amount. The pre-authorization amount is a good faith estimate based on spending patterns at the merchant and can be up to US $500.
3. The issuer approves or declines the transaction. If approved, the merchant can dispense the fuel.
4. When the fueling is completed, the merchant submits the final amount within two hours, using a real-time message. The transaction completion contains the actual transaction amount (less than the authorized estimated amount). Issuers are required to release the cardholder account hold when the completed transaction is received or within two hours of the pre-authorization request.

Settlement funds are transferred from the issuer to the merchant bank within hours, though settlement conventions to the merchant will vary.

Streamlining the Purchase Process with Visa’s Real-Time Clearing (RTC) Program

Currently, RTC with all program rules is only implemented in the United States.
RTC Benefits

The RTC program provides retail petroleum merchants with a number of core benefits:

- **Greater Merchant Flexibility** – The estimated authorization amounts can be optimized for different business needs, such as using higher amounts for automated fuel dispensers servicing commercial trucks. Using appropriate authorization amounts will result in optimal authorization rates.

- **Greater Chargeback Protection** – The RTC program extends Reason Code 96 (Transaction Exceeds Limited Amount) chargeback protection up to US $500, and Reason Code 72 (No Authorization) chargeback protection up to the estimated amount of the pre-authorization (not to exceed US $500).

- **Automatic Interchange Qualification** – As implemented in the U.S., the retail petroleum merchants’ interchange qualification is automatic. It is not based on the settlement request and/or the qualification of transactions by the merchant bank. Plus, there is no possibility of downgrade.

- **Simplified Clearing** – Online clearing is not subject to batch processing. It is automatic and independent of other transactions, which has the potential for expediting the timing of funding to the merchant.

- **Easier Enhanced Data Processing** – RTC transactions allow for greater richness of enhanced data\(^3\) without the processing hassles. The enhanced data is included with the authorization request and does not need to be retained by the merchant. As a result, merchants are not burdened with Level II and III data storage and/or uploading function responsibilities.

- **Greater Customer Satisfaction Through Reduced Holds** – Under the RTC program, transactions are processed immediately, instead of at the end of the day. This significantly reduces the hold times that issuers place on their cardholders’ accounts. Cardholders receive more accurate balance information—often within hours of the purchase.

Key RTC Considerations

In order for retail petroleum merchants to realize the above RTC program benefits, the following conditions must be met:

- The issuer and merchant bank must participate in RTC. (Issuers in the U.S. are required to support RTC.)

- The merchant bank must support partial authorization. (Only issuers of prepaid cards in the U.S. are required to support partial authorization.)

- The merchant bank must support SMS processing.

---

\(^3\) Enhanced data includes additional summary or line item information about a transaction, and in the fuel industry, is typically used for fleet customers. Level II data includes such things as fuel quantity, sales tax amount, and vehicle or driver ID number, while Level III data includes items such as odometer reading.
III. Authorization and Clearing

**Owner/Operator Best Practices**

- **Authorize purchase transactions.** An authorization protects the merchant, and may also be used to optimize interchange qualification. “Floor limits” define the amount above which authorizations must be performed. In most countries, this floor limit has been set to zero, meaning all fuel transactions must be authorized.
  
  - If the Cardholder does not continue with the Transaction, an authorization reversal must be issued for the full amount.
  
  - If the approved amount is not fully dispensed, an authorization reversal must be issued for the remaining amount. Authorization reversals for remaining amounts are not required when a status check was used. However, if a transaction is cancelled (no fuel dispensed), then an authorization reversal is required.
  
  - If the transaction is cleared for an amount greater than the authorization amount—whether implicit for status checks or explicit for estimated amounts—the issuer has a chargeback right for the amount that exceeds authorization amount.

- **Use “status checks” at automated fuel dispensers.** Authorizations at the automated fuel dispenser are accomplished via a status check for a single unit of currency. This check acts as an implicit authorization of a predefined amount. Use of a status check can also reduce changes to the dispenser software when the implicit amount is updated by Visa to reflect market conditions. Note that a status check is always an online authorization, even in chip countries.

  Authorizations for in-store transactions may also be for an estimated amount. However, this can lead to an impact to open-to-buy for the customer, unless paired with authorization reversals for any unused portion of the authorization.

- **Consult with your merchant bank to determine the optimal authorization levels for your operation.** Retail petroleum merchants and their banks will work together to determine authorization amount limits. Optimal amounts, however, tend to be highly influenced by the rules set forth by Visa and other card networks related to chargeback liabilities and interchange qualification. This amount varies around the world based on local fuel price dynamics, environment (in-store vs. automated fuel dispenser), and card product (Fleet cards may have higher optimal authorization amounts).

- **Work with your merchant bank to clear transactions in a timely manner.** This can improve your merchant payment timeframe, and reduce the window for operational issues that can lead to chargebacks.

---

4 Usually the equivalent of US $75 for magnetic-stripe transactions or US $100 for chip transactions
• **Where applicable, support partial authorization.** By enabling the partial authorization processing functionality, you are able to turn what would otherwise be a decline into an approval, thus increasing sales and generating revenue. An issuer can use a partial authorization to return an approval for an amount that is less than the transaction amount requested by the merchant, when the available card balance is not sufficient to approve the transaction in full.

  - Participating retail petroleum merchants must be able to set the fuel dispenser to only pump fuel up to the amount approved by the issuer.
  - Merchant banks must submit the authorized amount from the partial authorization response message as the “Authorized Amount” in the clearing transaction, not the single unit of currency status check from the authorization request. The amount of fuel pumped is submitted as the settlement amount in the “Source Amount” field in the clearing transaction.
  - If approved amount is not fully dispensed, an authorization reversal must be issued for the remaining amount.
  - If a transaction is cleared for an amount greater than the authorized amount in the partial authorization response message, the issuer has a chargeback right for the amount that exceeds the partial authorization amount.
IV. Fraud Management

Payment card fraud continues to be a concern for retail petroleum merchants. Unattended fuel dispensers are easy to access for the fraudster who wishes to remain anonymous and relatively more attractive for fraudulent activity. The fraudster may wish to attack the fuel dispenser as a point-of-compromise, attempting to capture payment or PIN data, or as a means to check fraudulent cards. Attended forecourts also have exposure, particularly when the attendants participate in fraudulent activities. As fuel itself is a desirable commodity, the fuel purchases, whether in-store or at an automated fuel dispenser, can also be an attractive target for fraud. A fraudulent fuel purchases has a direct impact on the retailer. While attacks on the fuel dispenser to obtain payment or PIN data may not directly affect the retailer, they provide opportunities for other fraudulent activities that can ultimately have an impact on all parties in the payment system.

Most merchant banks work very closely with their retailers in the fuel segment to define the appropriate types of tools and controls they need to actively manage payment system risk and limit related exposures.

Tools and controls that can help retailers reduce risk and better combat fraud include the following:

- **The Payment Card Industry (PCI) Data Security Standard (DSS)** is a comprehensive set of international security requirements for protecting cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. **PCI DSS compliance protects the merchant from being a point-of-compromise.**

- All Visa acquirers and issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit Visa account numbers. This program applies to all payment channels including card present, mail/telephone order, and e-commerce.

- **The PCI PIN Encrypting Device (PED) and PCI PIN Security Requirements** are intended to protect Visa cardholder PINs both in the POS and in the transporting networks. Visa requires both PCI PED and PCI PIN compliance for all PIN entry. This compliance includes mandates to use Triple DES to protect PIN data. Once an authorization is sent, PIN data should be erased to eliminate any opportunity for subsequent exposure of PIN data.
Tools and Controls for Optimal Payment Processing and Reduced Risk (continued)

- **Fraud Screening programs** can be used to suspend processing if a transaction:
  - Matches data stored in the merchant's internal negative files.
  - Exceeds velocity limits and controls.
  - Generates an Address Verification Service (AVS) mismatch.
  - Matches other high risk attributes customized by the merchant.

- **AVS** verifies the credit card billing address and/or zip or postal code of the customer who is paying with a Visa card (Fuel retailers typically verify only the zip or postal code). The merchant includes an AVS request with the transaction authorization and receives a result code (separate from the authorization response code) that indicates whether the address given by the cardholder matches the address in the issuer’s file. A partial or no-match response may indicate fraud risk. **Currently, AVS can only be used to confirm zip or postal codes for card present transactions in the United States.**

Fraud Mitigation – Owner/Operator Best Practices

Retail petroleum owners and operators can help reduce fraud exposure by implementing proper security controls and utilizing the following risk management best practices.

- **Set and communicate payment card policies and procedures that can help mitigate automated fuel dispenser fraud.** Establishing card acceptance policies, including risk management policies and procedures, and communicating those policies across the retail enterprise is the single-most important action that can be taken.

- **Minimize opportunities for attendants to engage in fraudulent behavior.**
  - Stay current on trends regarding attended fraud, such as pump attendants who accept cash while using fraudulent cards to activate the dispenser.
  - Ensure the POS communicates authorized amounts directly to the pump for dispensing.
  - Have all pump attendants enter an identification code whenever using the POS.
  - To avoid card compromise, use wireless POS so that the cardholder never loses sight of the card (or preferably, retains possession of the card).

- **Maintain velocity checking programs to monitor the frequency of transactions on the same card.** Visa recommends merchants monitor card transactions by location, and preferably by region and/or enterprise. The “Two-and-In” is a good rule of thumb to apply here; that is, two transactions for the same PAN within 24 hours will cause the third attempt to be directed into the store. Remember that the velocity checking database must be PCI DSS compliant.

- **Create a negative database that is PCI DSS compliant and implement it within your authorization system.** When a payment card matches the negative database, instruct cardholder to “See Cashier” for additional assistance.
Fraud Mitigation - Owner/Operator Best Practices (continued)

- **Set a delay time between authorization requests to help prevent automated fuel dispenser card testing.** Setting delays between authorization requests may make it less convenient for fraudsters to test stolen or re-encoded cards.

- **Monitor quantity of key-entered transactions by location, point of sale terminal and clerk ID.** A high number of key-entered transactions can be indicative of internal/external fraud or equipment maintenance issues.

- **Clearly communicate to managers and employees the potential for automated fuel dispenser fraud, as well as security measures and procedures they can employ to minimize fraud exposure.** Consider distributing the recommended best practices quick reference tools that follow.

- **If operating in EMV chip and PIN countries, provide support for PIN prompting both in-store and at the dispenser.** PIN will provide optimal protection against lost and stolen card use. In many chip countries, PIN support is required for full liability protection.

- **If operating in non-chip and non-PIN countries, closely inspect signatures for in-store transactions.**

- **In the U.S., use the Visa AVS at high fraud locations.** Visa recommends that merchants operating automated fuel dispensers:
  - To prevent shoulder surfers, mask the zip or postal code digits as they are input by the cardholder (e.g., ****7).
  - If the cardholder does not correctly input their current billing statement zip code within two attempts, instruct the cardholder to “See Cashier” to complete the transaction.
  - “Approve” the following AVS results codes: Z, P, Y.
  - “Decline” all other result codes and instruct the cardholder to “See Cashier” for additional assistance.
Quick Reference — Automated Fuel Dispenser Fraud Prevention

Manager/Employee
Best Practices

- **Monitor suspicious activity at automated fuel dispensers.** Managers and employees should be continually on the lookout for the warning signs of automated fuel dispenser fraud, which can include:
  - A single customer activating multiple automated fuel dispensers.
  - Filling multiple vehicles from one automated fuel dispenser transaction.
  - Filling large non-vehicle containers.
  - Fueling several times a day (system wide and location specific).
  - Card testing (inserting payment card for authorization without pumping).
  - Island surfing (persons walking around offering to pump fuel with their payment card in exchange for cash).

- **Routinely inspect automated fuel dispensers to ensure skimming devices and foreign hardware/software are not present.**

- **Eliminate “church key” access to mitigate automated fuel dispenser tampering.** Some older automated fuel dispensers share common keys that allow service station employees and service technicians to easily gain access to the dispenser’s interior. Unfortunately, fraudsters have exploited this ease-of-entry feature, using copies of the keys to gain unauthorized access.

- **Routinely walk around automated fuel dispensers to spot suspicious activity.**

- **Apply system offline (authorization system not available) procedures as needed.**
  - Alert owner/operator headquarters of all offline issues.
  - Verify transmission is not blocked or purposely interrupted.
  - Temporarily have dispensers direct cardholders to “See Attendant” for all transactions.
  - Call the Visa Authorization Center for authorization requests that exceed predetermined transaction amount (set lower limits at high-risk locations).
  - Make sure to imprint front of card for all manually authorized transactions.
  - For manually authorized transactions, retain card while receiving authorization and verify card security features.
  - Obtain cardholder signature and compare to back of card.
### Quick Reference — Attended and In-Store Fraud Prevention

#### Manager/Employee

**Best Practices**

- Always get a signature or PIN for all in-store transactions, except when the transaction is processed under the Visa Easy Payment Service (VEPS).
- Compare and match the account number. If your terminal does not prompt for key entry of the last four digits, compare the number on the Visa card to the number shown on the POS terminal display or the sales receipt. If the numbers do not match, you may have a counterfeit card. (This recommendation does not apply to multi-application EMV chip cards.)
- Take appropriate action based on the authorization message response.

<table>
<thead>
<tr>
<th>RESPONSE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Ask the customer to sign the sales receipt and compare signatures.</td>
</tr>
<tr>
<td>Declined</td>
<td>Return the card to customer and ask for another Visa card.</td>
</tr>
<tr>
<td>Call</td>
<td>Call your authorization center and tell them you received a “call” message. Be prepared to answer questions. The operator may ask to speak with the cardholder.</td>
</tr>
<tr>
<td>Pick Up</td>
<td>Keep the card if you can do so peacefully.</td>
</tr>
</tbody>
</table>

- For all key-entered and manually authorized transactions (Unable to process authorization using card-swipe):
  - Imprint payment card after receiving issuer authorization, add all required data elements and verify Visa card security features.
  - Obtain cardholder’s signature on transaction receipt and compare it to the signature panel located on back of the Visa card.
- While processing a transaction, always check the card security features. Any sign of tampering may mean that you have been given a counterfeit card.
- Be aware of suspicious activity at the counter.
  - Individual buying an unusual amount of convenience store items.
  - Limited or no eye contact from customer and/or they are acting “strangely.”
  - Buying large amounts of alcohol, cigarettes, and phone cards/gift cards.
  - Buying money orders and/or lottery tickets with credit card.
  - Attempting to bribe the cashier.
  - Requesting large amounts of cash back on small purchases.
- Monitor levels of key-entered transactions. Managers of multiple stores should monitor the number of key-entered transactions for unusual activity. While higher than normal levels of key-entered transactions may indicate a faulty card-reader (which may impact the MDR), they may also indicate an attempt at fraudulent activity by store personnel.
Quick Reference — Attended and In-Store Fraud Prevention

**Visa Card Security Features**

**Visa Brand Mark Card Security Features**

- The Signature Panel must appear on the back of the card and contain an ultraviolet element that repeats the word “Visa.” The panel will look like this one, or have a custom design. It may vary in length.
- The words “Authorized Signature” and “Not Valid Unless Signed” must appear above, below, or beside the signature panel.
- If someone has tried to erase the signature panel, the word “VOID” will be displayed.
- The Magnetic Stripe is encoded with the card’s identifying information.
- Card Verification Value (CVV) is a unique three-digit code that is encoded on the magnetic stripe of all valid cards. CVV is used to detect a counterfeit card.
- Card Verification Value 2 (CVV2) is a three-digit code that appears either on or in a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-not-present transactions to verify that customer is in possession of a valid Visa card at the time of the sale.
- Embossed/Unembossed or Printed Account Number on valid cards begins with “4.” All digits must be even, straight, and the same size.
- Four-Digit Bank Identification Number (BIN) must be printed directly below the account number. This number must match exactly with the first four digits of the account number.
- Expiration or “Good Thru” date should appear below the account number.
- Visa Brand Mark must appear in blue and gold on a white background in either the bottom right, top left, or top-right corner.
- Ultraviolet “V” is visible over the Visa Brand Mark when placed under an ultraviolet light.

**Visa Logo Card Security Features**

- The magnetic stripe is encoded with the card’s account number, expiration date, and other identifying information.
- Card Verification Value (CVV) is a unique three-digit code that is encoded on the magnetic stripe of all valid cards. CVV is used to detect a counterfeit card.
- Card Verification Value 2 (CVV2) is a three-digit code that appears on the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-not-present transactions to verify that customer is in possession of a valid Visa card at the time of the sale.
- Embossed/Printed Account Number begins with “4.” All digits must be even, even, straight, and the same size/shape.
- Four-Digit Bank Identification Number (BIN) must be printed directly below the embossed/printed account number. This number must match exactly with the first four digits of the account number.
- Expiration or “Good Thru” date should appear below the account number.
- Flying “V” is an embossed security character beside the “Good Thru” date. This character is not a required security feature and may or may not appear on the card.
- Ultraviolet-Sensitive Dove is visible in the face of the card when the card is placed under an ultraviolet light.

* June 30, 2011 - Visa cards displaying the flag will no longer be in circulation.
IV. FRAUD MANAGEMENT

Quick Reference — Attended and In-Store Fraud Prevention

**Visa Card Security Features**

**Unembossed Visa Card Acceptance**

The new unembossed Visa card may look and feel different, but it is a valid card that can be accepted at any Visa merchant location which has an electronic terminal. Unlike an embossed Visa card with raised numbers, letters, and symbols, the unembossed card has a smooth, flat surface. From a merchant perspective, the processing of an unembossed card at the point-of-sale should be seamless. There’s no need for new software, special hardware, or modified terminal procedures. You simply swipe the unembossed card just as you would an embossed card, then wait for an authorization and obtain the cardholder’s signature. Because of the unembossed card’s flat surface, it cannot be used for transactions that require a card imprint.

**Visa Chip Card**

Visa Chip cards are embedded with a chip; this chip communicates information to a point-of-sale terminal. At this time, chip cards are primarily issued outside the U.S.

**Visa Electron Card**

Visa Electron cards feel flat; all information is printed or engraved, not embossed or raised. Some unembossed Visa cards may have only a partial account number printed on the card. The Visa Dove Design Hologram may or may not appear on Visa Electron cards.
V. Chargeback Management

The Chargeback Process

A “chargeback” provides a card issuer with a way to return a disputed transaction.

When a chargeback right applies, the issuer sends the transaction back to the merchant bank and charges back the amount of the disputed sale. The merchant bank then researches the transaction. If the merchant cannot remedy the chargeback, it is the merchant’s loss. If the chargeback is valid, the merchant bank deducts the amount of the chargeback from the merchant account.

Example Flow for Cardholder Dispute

Cardholder
- Disputes transaction.
- Contacts card issuer with disputed information.

Card Issuer
- Reviews eligibility of transaction for chargeback. If appropriate, returns transaction (charges it back) to merchant bank through Visa electronically.

Visa
- Electronically screens representment for technical criteria compliance.
- If appropriate, forwards representment to card issuer electronically.

Merchant Bank
- Forwards represented item to Visa.

Merchant
- Receives chargeback.
- If appropriate, and under certain conditions, can represent chargeback to its merchant bank.
- If conditions aren’t met, merchant may have to accept chargeback.

Arbitration

If the card issuer disputes a representment from the merchant bank, the card issuer may file for arbitration with Visa. In arbitration, Visa decides which party is responsible for the disputed transaction. In most cases, Visa’s decision is final and must be accepted by both the card issuer and the merchant bank.
Handling Chargebacks

- **Cardholder disputes.** Customer disputes are one of the most common reasons for chargebacks. Besides the most obvious causes, these chargebacks may also indicate customer dissatisfaction—and the potential for lost sales in the future. For both financial and customer service reasons, petroleum merchants should address the underlying cause of disputes as part of their customer service policies.

There are many reasons for chargebacks—the ones which typically occur in the fuel segment include the following:

- **Reason Code 72: No Authorization** – A merchant did not obtain authorization for a transaction. (This will also apply if the cleared transaction amount exceeds the authorized amount.)
- **Reason Code 81: Fraudulent Transaction – Card-Present Environment** – Merchant processed a transaction in a card-present environment and did not obtain both a card imprint and cardholder signature (or PIN).

Listed below are the most common causes for these three reason codes, as well as best practices for chargeback avoidance.

**Reason Code 72: No Authorization**

**Common Cause for Reason Code 72:**

The merchant did not obtain an authorization for a transaction on the transaction date, or the authorization was obtained using invalid/incorrect transaction data as specified in the VisaNet manuals. *Note: For automated fuel dispenser transactions, the chargeback is not valid if an authorization status check for a single unit of currency was obtained and the amount did not exceed the allowable limit for that environment.*

**Chargeback Avoidance Best Practices:**

- Obtain an authorization using the correct transaction data before completing the transaction. This can include, but is not limited to making sure the following data is correct:
  - Transaction date,
  - MCC,
  - Indicator for the merchant or transaction type, and
  - Country code or special condition indicator.

- If unable to get an authorization because terminal isn’t working or because the card’s magnetic stripe cannot be read, request an authorization by key-entering the transaction or calling your voice authorization center. If the transaction is approved, write the approval code on the sales receipt in the appropriate space, and imprint the card’s embossed information onto the receipt, using a manual imprinter. *NOTE: Unembossed cards are not eligible for key entry or for voice authorizations. If you are unable to obtain an electronic authorization for an unembossed card, ask for another Visa card.*
V. CHARGEBACK MANAGEMENT

Common Retail Fuel Segment Chargebacks and Best Practices (continued)

- **If a transaction is declined, do not accept it.** Immediately stop the transaction, and ask the customer for another Visa card.
- **Do not dispense fuel in excess of authorized amount.** Establish fuel dispenser threshold values. Visa’s threshold values vary based on card product. Threshold values may also be set based on merchant-determined metrics.

**Reason Code 81: Fraudulent Transaction – Card-Present Environment**

*Common Causes for Reason Code 81:*

- The card was not swiped through a magnetic-stripe reader or dipped into a chip reader, and a manual imprint of the card was not taken.
- For in-store sales, the cardholder’s signature was not captured on the sales receipt or a PIN was not taken.
- The cardholder denies participating in the transaction and the signature or PIN was not obtained, and/or an imprint was not taken; usually indicating a lost of stolen card situation.

*Chargeback Avoidance Best Practices:*

- **Authorize online transactions using best practices described in Section III of this guide.** Make use of voice authorizations when online authorizations are not possible.
- For in-store transactions, always get a signature and imprint.
- **Diligently apply fraud mitigation.** For further information, refer to Section IV of this guide.
- To help minimize employee fraud, restrict employee access to card numbers.
- At the automated fuel dispenser, make use of the “See Cashier Inside” messaging when transactions trigger suspicion. While customers certainly enjoy the convenience of paying at the pump, they are often equally concerned about fraud and are willing to take basic measures to help combat potential fraud.
- **Follow the referral process when you receive an authorization response of “CALL.”**
- Do not accept expired cards.
- **Monitor and quickly diagnose problems leading to offline status of POS systems.** Have a clear set of policies for card acceptance when your system is offline.
- **If you are receiving a high volume of Reason Code 81 chargebacks, investigate.** Examine the sales receipts related to the chargebacks to check which POS terminals and sales staff were involved in these transactions.
Reason Code 96: Transaction Exceeds Limited Amount Terminal

Common Cause for Reason Code 96:
An automated fuel dispenser and transaction exceeded the allowable limit for that environment. For these transactions, the amount of the issuer chargeback is limited to the amount that exceeds the specified limit amount.

Chargeback Avoidance Best Practices:

- **Ensure automated fuel dispenser terminals are consistently set at proper transaction amount limits.** Reason Code 96 chargebacks typically result from a merchant electing not to enforce automated fuel dispenser limits. Consider limiting fuel distribution to Visa's allowable amount. Complying with Visa's allowable limits will reduce your exposure to a Reason Code 96 chargeback. Your merchant bank can assist you in determining Visa limits.

- **Work with your merchant bank to optimize the process for responding to a Reason Code 96 chargeback in a timely manner and re-presenting, when appropriate.**

Copy Request Management Best Practices

When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the merchant bank. Once the issuer receives this documentation, the first step is for the issuer to determine whether a chargeback situation exists. Merchants who keep copy requests to a minimum are also more likely to have lower chargeback rates and higher profitability.

- **Make sure customers can recognize your name on their bills.** Cardholders must be able to look at their bank statements and recognize transactions that occurred at your establishment. Check with your merchant bank to be sure it has correct information on your “Doing Business As” (DBA) name, city, and state. You can check this information yourself by purchasing an item on your Visa card at each of your outlets and looking at the merchant name and location on your monthly Visa statement. Is your business name recognizable? Can your customers identify the transactions made at your establishment?

- **Avoid illegible transaction receipts.** This is key to minimizing copy requests and chargebacks. When responding to a copy request, merchants usually photocopy or scan the transaction receipt before mailing or electronically sending it to your merchant bank. If the receipt is not legible to begin with, the copy that the bank receives and then sends to the issuer may not be useful in resolving the cardholder’s question. If this occurs, the transaction may be returned to the merchant as a chargeback for an illegible copy. At this point, since transaction receipt readability can’t be improved, the merchant may end up taking a loss on the transaction.
• Make sure your business name is legible on receipts. Your company’s name should be accurately and legibly printed on transaction receipts. The location, size, or color of this information should not interfere with transaction detail. Similarly, you should make sure that any company logos or marketing messages on receipts are positioned away from transaction information.

• Train attendants. With proper transaction processing, many copy requests can be prevented at the point of sale. Attendants should:
  – Follow proper POS card acceptance procedures.
  – Review each transaction receipt for accuracy and completeness.
  – Ensure the transaction receipt is readable. If it is not, reprint the receipt and request a new signature.
  – Give the cardholder the customer copy of the transaction receipt, and keep the original, signed copy.

• Clearly communicate to managers and employees the best practices they can apply to help avoid illegible transaction receipts. Consider distributing the recommended best practices quick reference tool below.

Quick Reference — Avoiding Illegible Transaction Receipts

Manager/Employee
Best Practices

The following best practices are recommended to avoid illegible transaction receipts.

■ Change point-of-sale printer cartridge routinely. Faded, barely visible ink on sales drafts is the #1 cause of illegible sales draft copies. Make sure the printing is clear and dark on every sales draft. Check readability on all POS printers daily.

■ Handle carbonless paper and carbon/silver-backed paper carefully. Silver-backed paper appears black when copied. Any pressure on carbonless and carbon-backed paper during handling and storage causes black blotches, making copies illegible. Always handle this type of paper with care!

■ Change POS printer paper when colored streak first appears. The colored streak down the center or the edges of printer paper indicates the end of the paper roll. It also diminishes the legibility of transaction information. Change the printer paper as soon as this colored warning streak appears.

■ Keep white copy of sales draft receipt—give customers colored copy. Keep the white copy of sales draft; color won’t matter to your customers. Since colored paper does not copy as clearly as white paper, it can result in illegible copies.
VI. Interchange Costs Management

Interchange and Pricing

Payment acceptance has associated costs which need to be closely monitored and managed. An important component of this cost is the IRF paid by the merchant bank to the card issuer and often passed through to the merchant. Interchange rates are determined based on the type of merchant, type of card product, and the manner in which the transaction is processed. If a transaction is not processed in accordance with rate qualification criteria, it may be downgraded to a more expensive interchange rate. In controlling card acceptance costs, therefore, it is imperative that retail petroleum merchants control interchange downgrades.

Interchange Best Practices

- **Use VEPS for appropriate in-store transactions.** VEPS also applies to lower value transactions in an attended forecourt.
- **Avoid downgrades that result from miscoded transaction files.** Consider the following:
  - Carefully test initial deployment and any subsequent changes to the POS system.
  - Ensure that each POS is coded to the proper Merchant Category Code (MCC), which can include “petrol”, “service station”, “AFD”, etc.
  - Conduct root cause analysis of downgrades, sensitive to the likelihood that the POS may be miscoding transactions.
- **Use the appropriate MCC.** The MCC 5542 must be used for all automated fuel dispenser transactions. MCC 5541 is used for in-store and attended forecourt fuel purchases. Non-fuel purchases must be coded with the correct MCC.
- **Ensure that transaction clearing batches are transmitted to the merchant bank at least once a day.**
- **Work with your merchant bank to ensure correct interchange assigned to all transactions.** Merchant banks should be capable of providing the underlying volume by the rate category detail that is needed to monitor qualification levels.
- **In conjunction with your merchant bank, use peer benchmarks and historical patterns to identify anomalies in qualification patterns.** Conduct root-cause-analysis in order to understand the causes of downgrades (such as failed PIN pads, break-downs in telecommunications technology, misprogrammed POS software, etc.).
VII. Tender Mix Management

Facilitating Customer Choice and Preferences

The competitive and financial success of retail petroleum merchants can be greatly enhanced by their willingness and ability to accept payment types which are most preferred by the customers. However, while the facilitation of customer choice and preferences should be first priority, different payment types do indeed carry different costs and benefits to customers. Merchants need to consider the trade-offs carefully before making their payment acceptance decisions.

Tender Mix Management Best Practices

• **Examine the advantages of cards vs. cash.** Cash is more or less universally accepted and is an important component of an overall tender mix strategy. However, though often perceived as the least costly payment form, cash carries with it a number of limitations including smaller ticket sizes, concerns about security, employee theft, cash management costs, opportunity costs of lost sales (particularly in the store), and less convenience in a pay-in-the-forecourt environment. Cash is not free and its costs tend to be underestimated.

• **Examine the advantages of cards vs. checks or accounts.** Checks carry many of the same costs as cash, as well as the risk of non-sufficient funds. Similarly, these costs tend to be underestimated. Visa cards protect the merchant from credit risks, unlike the exposure of extending account credit to customers.

• **Use a strategic approach to prepaid cards, which have great potential in the fuel segment.** Prepaid cards have proven highly effective as a means for customers without bankcards to benefit from the convenience of cards, as well as a useful and easy mechanism for transferring fuel purchase capability.

• **Discuss a co-brand strategy with your merchant bank or with other Visa issuers to determine the optimal product design and approach to distribution.** Understand and use the payment process as a valuable point of interaction to provide customer loyalty. Branded card programs (such as co-branded Visa cards or prepaid/gift cards) are a proven method to drive customer loyalty and incremental purchases. They also provide a means to lower acceptance costs. Retail petroleum merchants can promote branded cards using a variety of tactics, including customer rewards for using the branded card, recognizing cardholders with personal prompts at the automated fuel dispenser, and reminding customers about the programs using promotion at the outlet.

• **Discuss a prepaid strategy with your merchant bank or with other Visa issuers to determine the optimal prepaid product design and approach to distribution.** Prepaid cards can be used as a means to reward motorists for purchasing other products. At a minimum, retailers should have a clear strategy for profiting from distribution and acceptance of prepaid cards, and optimally, to aggressively distribute prepaid cards to generate stand-alone card profitability and incremental fuel purchases.
VIII. Quality of Service

It doesn’t matter if a customer is paying for fuel, and/or buying a few items in-store at a retail outlet. They all expect the same thing when it comes to quality service—speed, efficiency, and ease-of-use. It is up to the retail petroleum manager to establish the proper framework for service success and customer satisfaction.

AFD Best Practices

- Ensure automated fuel dispenser key pads are functioning properly (e.g., the key pad does not stick) to expedite transactions.
- Use intercom systems to offer customer assistance.
- Communicate transaction amount limits to your customers. To ensure that the amount limit does not come as a surprise or disruption to the customer, post information at the pump or POS that describes the limit and the customer’s alternatives, such as conducting a second transaction or going inside first to pay for fuel.

AVS Best Practices

- Wherever Visa AVS is being used:
  - Provide signage to international cardholders that either allows them to bypass a zip or postal code entry (using the Clear/Cancel key) or instructs the cardholder to “See Cashier” to complete the transaction.
  - In the event of a zip or postal code input error, provide a “Clear/Cancel” key.
  - Provide signage to mitigate cardholder phishing fears. For example, stickers or video screen content, explaining the point of sale is requesting the cardholder’s Visa billing statement zip or postal code for security purposes.

Attended and In-Store Service Best Practices

- Use VEPS to make payment processing faster and easier while increasing sales. VEPS is a global program that allows qualifying low value transactions\(^5\) at specific merchants to take place without cardholder verification and without a receipt, unless a receipt is requested by the cardholder. VEPS makes the Visa payment process faster and easier for both merchants and customers. This is especially beneficial to high-volume merchants such as quick service restaurants (QSRs) and supermarkets since it allows merchants to serve more customers and reduces customer time spent in line (queuing).
  - Service Stations (MCC 5541) are eligible to participate in VEPS for attended and in-store transactions.
  - Merchants do not need to register for VEPS. If you are eligible to participate, contact your merchant bank or processor.

---

\(^5\) The default value is US $25 (or local equivalent), but can vary by country.
- Merchants are not obliged to respond to issuer requests for copy for eligible transactions – meaning merchants do not need to store receipts for VEPS-qualified transactions.
- Merchants are protected from chargeback against receipt and signature related chargebacks for VEPS-qualified transactions.

• To learn more about VEPS and/or order a copy of the Visa Easy Payment Service (VEPS) brochure, contact your merchant bank or processor, or Visa representative.
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Number</td>
<td>The 16-digit account number that appears on the front of all valid Visa cards. The number is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td>Address Verification System (AVS)</td>
<td>A risk management tool that enables a merchant to verify the billing address of a customer presenting a Visa card for payment. The merchant includes an AVS request with the transaction authorization and receives a result code indicating whether the address given by the cardholder matches the address in the issuer’s file. A “Partial” or “No Match” may indicate fraud risk.</td>
</tr>
<tr>
<td>Authorization</td>
<td>A process by which a transaction for a specified amount is approved by an issuer for a merchant.</td>
</tr>
<tr>
<td>Authorization Center</td>
<td>Facilities established by members in-house or by third party processors to respond to merchants’ or other members’ requests for authorizations for transactions or cash advances. Authorization centers may also respond to referrals.</td>
</tr>
<tr>
<td>Authorization Monitoring</td>
<td>Electronic systems used by members to screen authorized transactions over a given period of time (e.g., a day, week or month) for evidence of potential fraud.</td>
</tr>
<tr>
<td>Automated Fuel Dispenser (AFD)</td>
<td>A Self-Service Terminal or Automated Dispensing Machine that dispenses fuel such as gasoline, diesel fuel, or propane.</td>
</tr>
<tr>
<td>Card Security Features</td>
<td>Alphanumeric, pictorial, and other design and functional elements on bankcards. The exact physical dimensions and placement of these features are specified by the Visa International Operating Regulations and are difficult to copy exactly. Card security features are checked by merchants at the point of sale to ensure the card is valid.</td>
</tr>
<tr>
<td>Card Verification Value (CVV)</td>
<td>A unique three-digit “check number” encoded on the magnetic-stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information and is verified online at the same time a transaction is authorized.</td>
</tr>
<tr>
<td>Cardholder</td>
<td>The person or entity whose name is embossed on the face of a card or encoded on the magnetic-stripe.</td>
</tr>
<tr>
<td>Cash-Back</td>
<td>Cash obtained from a Visa or Visa Electron Merchant through the use of a Visa or Visa Electron Card, in conjunction with, and processed as, a retail transaction.</td>
</tr>
<tr>
<td>Chargeback</td>
<td>A formal process that allows an issuer to charge the amount of sale back to the merchant bank, because the merchant has not complied with requirements.</td>
</tr>
<tr>
<td>Counterfeit Card</td>
<td>A payment device which has been fraudulently printed, embossed and/or encoded to be used as a valid card.</td>
</tr>
</tbody>
</table>
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Embossed Account Number</strong></td>
<td>The 16-digit account number that may appear in raised print on the front of valid Visa cards. The embossed number is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td><strong>Expired Card</strong></td>
<td>A card on which the expiration date embossed and/or encoded by the issuer has expired.</td>
</tr>
<tr>
<td><strong>Face-to-Face Transactions</strong></td>
<td>Transactions in which both the cardholder and the card are present at the point of sale.</td>
</tr>
<tr>
<td><strong>“Flying V” (For Visa Flag Logo cards only)</strong></td>
<td>The stylized, embossed “V” located to the right of the Good Thru date on all valid Visa Flag Logo cards. The “flying V” is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td><strong>Interchange</strong></td>
<td>Interchange is the transfer rate exchanged between the merchant’s and cardholder’s financial institutions each time a Visa payment product is used. Its primary role is to create the right balance of incentives between cardholders’ financial institutions—which promote and issue Visa cards to consumers—and merchants’ financial institutions—which enroll and process Visa transactions for merchants.</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>A financial institution that issues Visa cards.</td>
</tr>
<tr>
<td><strong>Magnetic Stripe (Mag Stripe)</strong></td>
<td>A strip of magnetic tape on the back of all bankcards. The stripe is encoded with identifying account information as specified in the Visa International Operating Regulations. On a valid card, the account information on the magnetic stripe matches similar embossed information on the front of the card.</td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td>A principal or entity entering into a card acceptance agreement with a Visa member financial institution.</td>
</tr>
<tr>
<td><strong>Merchant Bank</strong></td>
<td>Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services.</td>
</tr>
<tr>
<td><strong>Merchant Discount Reimbursement (MDR)</strong></td>
<td>The fee charged to the merchant by the merchant bank for processing services that enable the merchant to accept payment cards. It is the Interchange Reimbursement Fee (IRF), plus agreed upon merchant bank costs.</td>
</tr>
<tr>
<td><strong>Mini-Dove Hologram (May appear on the back of Visa Brand Mark cards)</strong></td>
<td>The Visa mini-dove hologram design may appear on the back of a Visa Brand Mark card within a specific outlined area. When the card is tilted back and forth, the dove should appear to “fly.”</td>
</tr>
<tr>
<td><strong>Payment Card Industry Data Security Standard (PCI DSS)</strong></td>
<td>A set of requirements established by the Payment Card Industry to protect cardholder data. These requirements apply to all members, merchants, and agents that store, process, or transmit cardholder data.</td>
</tr>
<tr>
<td><strong>Personal Identification Number (PIN)</strong></td>
<td>An alphabetic and/or numeric code which may be used as a means of cardholder identification.</td>
</tr>
</tbody>
</table>

---

5 The default value is US $25 (or local equivalent), but can vary by country.
<table>
<thead>
<tr>
<th>Glossary of Terms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point of Sale (POS)</td>
<td>The location at which the sale/transaction takes place.</td>
</tr>
<tr>
<td>Printed Account Number</td>
<td>The 16-digit account number that may appear in print on the front of valid Visa cards. The printed number is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td>Printed Number</td>
<td>A four-digit number that is printed below the first four digits of the printed or embossed account number on all valid Visa cards. The four-digit printed number should begin with a “4,” and be the same as the first four digits of the account number above it. The printed four-digit number is one of the card security features that merchants should check to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td>Referral Messages</td>
<td>A “call” or “call center” response to a merchant’s or member’s request for an authorization. A referral message indicates that the issuer needs more information about the transaction or cardholder before an approval can be issued.</td>
</tr>
<tr>
<td>Sales Transaction Receipt</td>
<td>A paper or electronic record of a sale which the merchant presents to the bank for processing. The cardholder’s card account can then be debited and the merchant account may be credited (also referred to as draft or sales draft).</td>
</tr>
<tr>
<td>Skimming</td>
<td>The replication of account information encoded on the magnetic stripe of a valid card and its subsequent use for fraudulent transactions in which a valid authorization occurs. Full-track data is captured from a valid card and then re-encoded on a counterfeit card. The term “skimming” is also used to refer to any situation in which electronically transmitted or stored account data is replicated, and then re-encoded on counterfeit cards or used in some other way for fraudulent transactions.</td>
</tr>
<tr>
<td>Signature panel (Appears on the back of all Visa Flag Logo cards)</td>
<td>The panel for cardholders’ signatures on the back of all valid Visa Flag Logo cards. Valid panels are white with the repeated word “Visa” printed at an angle in blue and gold. It may also contain the full or truncated account number and the three-digit CVV2, printed in reverse italics. The words “Not Valid Without Signature” or “Authorized signature” should also appear below or to the side of the panel on most Visa cards. The signature panel is one of the card security features merchants should check to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td>Signature panel (Appears on the back of all Visa Brand Mark cards)</td>
<td>The panel for cardholders’ signatures on the back of all valid Visa Brand Mark cards. A valid panel contains an ultraviolet element that either repeats the word “Visa” or has a custom design. The signature panel is one of the card security features merchants should check to ensure that a card-present transaction is valid.</td>
</tr>
<tr>
<td>Transaction</td>
<td>The act between the cardholder and merchant or cardholder and financial institution which results in the sale of goods or services.</td>
</tr>
<tr>
<td>Visa Easy Payment Service (VEPS)</td>
<td>A global program that allows qualifying low value transactions at specific merchants to take place without cardholder verification and without a receipt, unless a receipt is requested.</td>
</tr>
</tbody>
</table>

---

6 The default value is US $25 (or local equivalent), but can vary by country.