Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants

DECEMBER 2018

Important Information on Confidentiality and Copyright

Notice: This information is proprietary and CONFIDENTIAL to Visa. It is distributed to Visa participants for use exclusively in managing their Visa programs. It must not be duplicated, published, distributed or disclosed, in whole or in part, to merchants, cardholders or any other person without prior written permission from Visa.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Note: This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules*. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

Contents

About This Guide

Background

Card acceptance is instrumental in operating a successful fuel retailing business. 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.

KEY POINT TO REMEMBER

In this guide, the term Automated Fuel Dispenser (AFD) refers to an unattended device used to dispense fuel, such as gasoline, propane, or diesel fuel, and which accepts payment cards.

Visa Card Benefits

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 in the U.S. 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. This guide showcases the decisions and options required to operate a successful business.

Who Should Use This Guide

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

Guide Purpose

The *Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants* guide provides optimal ways to process card transactions and manage the risks posed by card payments in the fuel segment.[1]

The guide offers a set of recommended best practices for:

- Handling in-store and AFD acceptance procedures
- Processing authorization requests and transaction data for in-store and AFD environments
- Achieving fuel transaction processing and funding efficiencies
- Understanding interchange and controlling downgrades
- Diagnosing and dealing with higher than acceptable key-entry or fallback rates
- Applying fraud mitigation tools for both in-store and AFD transactions
- Using Visa's Real-Time Clearing (RTC) program
- Processing Fleet Card transactions
- Minimizing risk of loss from disputes
- Ensuring compliance with Payment Card Industry Data Security Standards (PCI DSS)
- Implementing EMV Chip

Guide Focus

Given the zero floor limit in the U.S. payment environment, the majority of transactions are authorized online. This guide focuses solely on the implementation requirements relating to online-only configured terminals and does not include offline functionality.

[1] **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.

How This Guide Is Organized

The guide is divided into nine sections.

- **Section I. General Authorization and Clearing Overview** offers a general overview of a retail petroleum merchants' payment acceptance environment.
- **Section II. In-Store Transactions** deals exclusively with the in-store (or inside) environment. It covers authorization transaction flow, acceptance procedures, VEPS, partial authorization, CPS retail program qualification; fraud and dispute mitigation.
- **Section III. AFD Transactions** deals exclusively with the AFD (or outside) environment. It addresses transaction flows and explains real-time clearing (RTC) benefits and key considerations for adoption. It identifies best practices for customer satisfaction, CPS credit or debit program qualification, fraud prevention and dispute mitigation.
- **Section IV. Processing Considerations and Management** covers principles that are key to achieving fuel transaction processing and funding efficiencies.
- **Section V. Accepting Visa Fleet Card Payments** outlines merchant considerations and best practices for ensuring proper Visa Fleet card payment acceptance in the retail petroleum environment.
- **Section VI. Interchange Costs Management** emphasizes the need to process transactions in accordance with rate qualification criteria to avoid interchange downgrades.
- **Section VII. Cardholder Data Security** addresses the tools and controls to safeguard sensitive cardholder data.
- **Section VIII. Chip Implementation** identifies terminal configuration, testing and AID requirements. All other specific chip best practices and procedures are detailed as they relate to the other sections of this guide.
- **Additional Resources** provides guidance for EMV Chip implementation
- A **Glossary of Terms** includes commonly defined terms used throughout this guide.

Note: Because there are different practices and procedures for in-store versus AFD environments, Sections II and III deal exclusively with transactions handled in these environments respectively.

All other sections provide pertinent information that applies to both the in-store and the AFD environment.

I. General Authorization and Clearing Overview

Introduction

The General Authorization and Clearing Overview section offers a general overview of a retail petroleum merchants' payment acceptance environment.

How Visa Payment Processing Works – Start to Finish

Visa operates and maintains VisaNet—the world's largest consumer payment system. It is comprised 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 appears on the cardholder's statement.

This is accomplished through:

- An authorization service where 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.

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. VisaNet settles with the merchant banks and card issuers on a daily basis. Through VisaNet, issuers pay the merchant banks for transactions that have been completed by their cardholders.

Note: We will cover authorization, clearing and settlement in detail for in-store and at AFDs in their respective sections.

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.

II. In-Store Transactions – Service Stations and Convenience Stores (Typically Use MCC 5541)

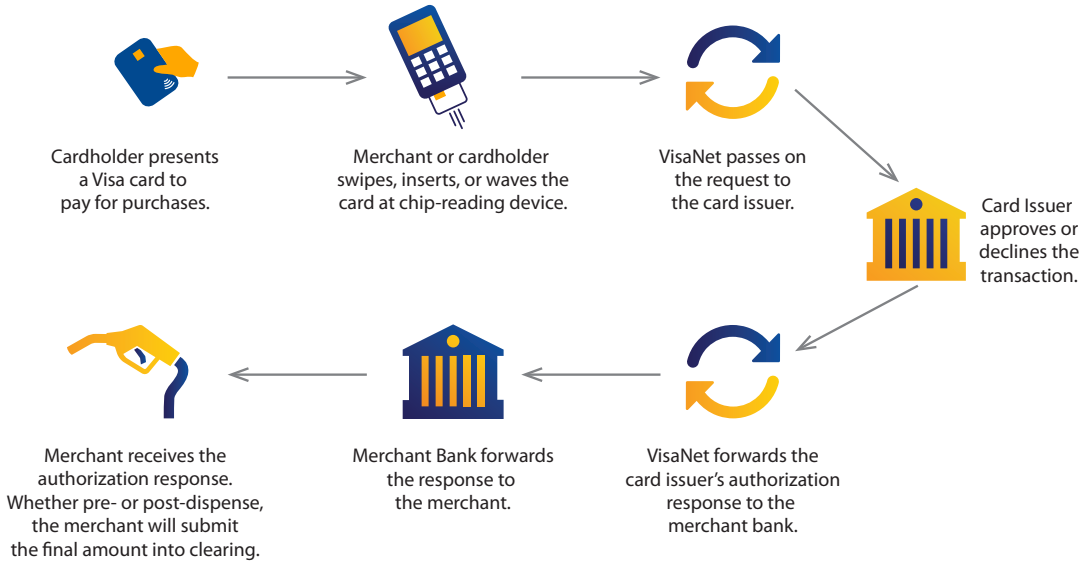
Introduction

The In-Store Transactions section deals exclusively with transactions that take place in an in-store (or inside) environment. It covers authorization transaction flow; acceptance procedures; fraud and dispute mitigation.

Authorization Processing Steps

The following illustration shows the authorization processing steps for an in-store transaction. It depicts the lifecycle for a credit, debit, or prepaid 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. The transaction flows represent EMV contact chip, Visa payWave or magnetic stripe.

Authorization In-Store



Clearing and Settlement

Merchant deposits the transaction receipt with merchant bank for the final transaction amount.

Merchant Bank credits the merchant's account and electronically submits the transaction to Visa for settlement.

VisaNet

- Facilitates settlement by paying the merchant bank for the transaction amount and debiting the card issuer account
- Sends the transaction to the card issuer

Card Issuer:

- Posts the transaction to the cardholder account
- Sends the monthly statement to the cardholder

Cardholder receives the statement

Manager/Employee Best Practices

The following best practices apply for in-store acceptance:

- Always get a signature or PIN for all in-store transactions, except when the transaction is processed under VEPS (Visa Easy Payment Service) or if the POS terminal is not EMV Chip enabled. A signature is optional if the POS terminal is chip enabled.
- Take appropriate action based on the authorization message response.

Authorization Response	Meaning
Approved	Card issuer approves the transaction. This is the most common response. When a transaction is approved, the POS terminal automatically prints a sales receipt.
Declined or Card Not Accepted	Card issuer does not approve the transaction. The transaction should not be completed. When a negative or alert message is received, the response is displayed on the POS terminal, and no sales receipt is printed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account. Remember to always treat the customer courteously.
Pick Up	Card issuer wants to recover the card. Do not complete the transaction. Inform the customer that you have been instructed to keep the card, and ask for an alternative form of payment. If you feel uncomfortable, simply return the card to the cardholder.

Always request authorization on an expired card.

Smart Phone In-App In-Store Transaction Processing

Merchants who allow their customers to conduct in-store purchases using smart phone applications need to ensure the authorization messages contain the proper data elements to reflect these types of purchases. Below is a chart of authorization message fields impacted by smart phone in-app purchases and the required data elements.

Authorization	inApp Service Station Transaction Values
Field 18 (Merchant Category Code)	5541
Field 22 (Point of Sale Entry Mode)	01 (Manual Key Entry) or 10 (Credential On File)
Field 25 (Point of Sale Condition Code)	59 (eCommerce)
Field 60.1 (Terminal Type)	0 (Unspecified)
Field 60.8 (Electronic Commerce Indicator)	Varies by authentication type

In-Store Fraud Mitigation for High Risk Items

Fuel merchants who have not implemented EMV chip acceptance technology will face an increasing threat of counterfeit fraud and resulting associated dispute liability for service station transactions.

Two best practices to help reduce counterfeit fraud for service station transactions are the:

- Read and Compare Verification method
- Check ID on Service Station Transactions

Read and Compare Verification Method Best Practices

Implement the Read and Compare Verification method when:

- Processing transactions over a specific dollar amount
- Purchases involve items known to be associated with high fraud (e.g., prepaid cards, tobacco products, alcohol)
- The transaction is suspicious

The Read and Compare Verification method can be performed either manually or through your POS device.

Manual Read and Compare Method

After swiping the card:

1. Read the last four (4) digits of the account number on the **physical card**

2. Compare them to the last four digits appearing on the **receipt**.

This method is most effective when sales associates confirm the last four card digits on their own rather than asking the customer to read the numbers aloud.

Automated Read and Compare Method Through Your POS Device

If the necessary software modifications have been made to the POS device, implement the automated Read and Compare Verification method. When prompted, input the last 4 digits of the account number. The device will perform the Read and Compare verification:

If the numbers:	
Match	Complete the transaction
Do not match	Cancel the transaction, and ask for another form of payment

Check ID on Service Station Transactions Best Practice

If suspicious of the transaction, ask the cardholder for a government issued ID. If the cardholder's name on the Visa card provided does not match the name on the cardholder's government-issued identification, you may decline the sale and ask for another form of payment. For more information, contact your acquiring bank, processor or Visa representative.

Additional Fraud Prevention Best Practice

Monitor quantity of fallback of chip card transactions for both magnetic-stripe read and key-entered transactions by location, POS terminal, and clerk ID. A high number of key-entered transactions can be indicative of internal/external fraud or equipment maintenance issues.

In-Store Transaction Dispute Mitigation

For in-store dispute mitigation, follow these guidelines when dealing with authorization related, fraud and duplicate processing disputes.

Authorization Related Disputes (Dispute Condition 11.3)

This dispute applies to transactions that were not authorized (possibly, due to systems being down). After downtime, reauthorize all stored transactions versus forwarding directly into settlement to prevent:

- No-authorization disputes
- Zero-floor limit misuse fees
- Transaction interchange downgrade
- Debit Transaction Integrity Fees (TIF)

Fraud Disputes (Dispute Condition 10.3)

This dispute is related to fraudulent transactions:

- Ensure all transactions are electronically authorized.
- If the transaction was key-entered, capture an imprint and signature.

For key-entered transactions, an issuer dispute (Dispute Condition 10.3) is valid unless the merchant can provide an imprint for domestic and international transactions.

Duplicate Processing Disputes (Dispute Condition 12.6)

This dispute results when "a single transaction" was processed more than once on the same account number. Ensure that your:

- POS systems are not submitting duplicate transactions to the acquirer.
- Staff are properly trained to void duplicate transactions.

III. AFD Transactions

Introduction

The AFD Transactions section deals exclusively with transactions handled in the automated fuel dispenser (outside) environment.

It covers best practices to ensure customer satisfaction. This section addresses key transaction flows and explains real-time clearing (RTC) benefits and considerations for adoption. It also details best practices for fraud prevention and dispute mitigation.

Authorization

Three Ways to Authorize an AFD Transaction

There are three ways to process AFD authorizations depending on the situations detailed below:

Situation: Before Pumping, the cardholder:	Use:
Identifies the exact amount of money to purchase gasoline	Authorization for the exact amount
Does not know how much the gasoline will cost	$1.00 status check procedure
Does not know how much the gasoline will cost AND your processor participates in Visa's Real-Time Clearing (RTC) program.	Real-time processing estimated authorization amount

On the next pages, each of these authorization process flows are detailed and the corresponding clearing and settlement process flows.

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.

The transaction flow represents EMV contact chip, Visa payWave or magnetic-stripe read card.

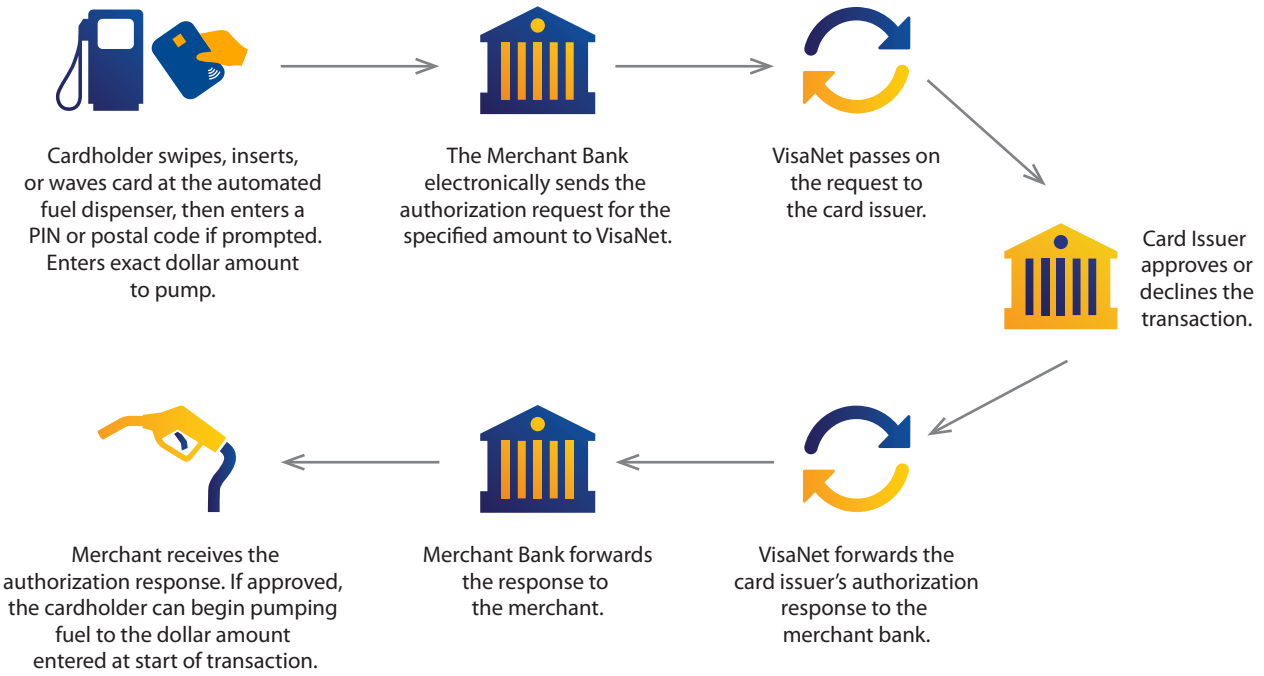
Visa does not require a signature or PIN for AFD transactions. For chip transactions, the chip cryptogram amount should be whatever amount is contained in the authorization message. No chip data is required in the clearing/advice or the final amount notification from the dispenser as long as the transaction is online authorized.

A new MCC of 5552 will be added October 2019* for charging stations for electric vehicles.
** Date subject to change*

Obtaining Authorization for Exact Amount

The following illustration walks through the authorization process for an automated fuel dispenser for an exact amount. It shows the lifecycle for a credit, debit, or prepaid transaction.

Exact Amount Authorization at the Automated Fuel Dispenser



Exact Amount Clearing and Settlement

Merchant deposits the transaction receipt with merchant bank for the final transaction amount.

Merchant Bank credits the merchant's account and electronically submits the transaction to Visa for settlement.

VisaNet

- Facilitates settlement by paying the merchant bank for the transaction amount and debiting the card issuer account
- Sends the transaction to the card issuer

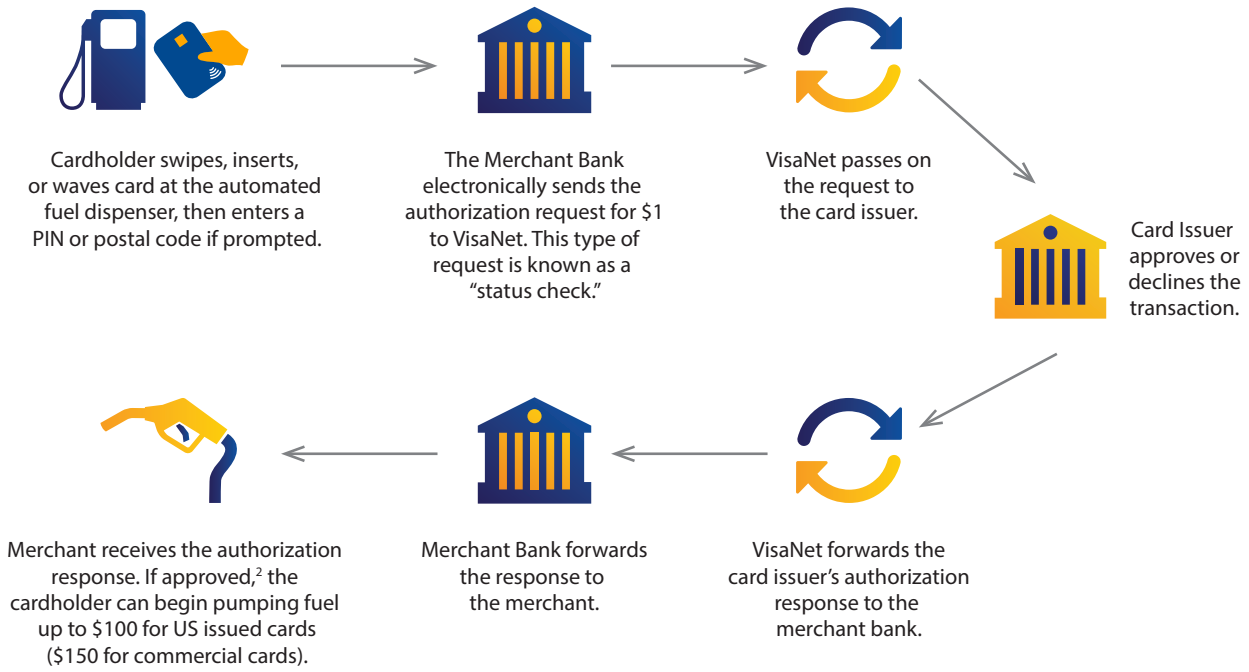
Card Issuer:

- Posts the transaction to the cardholder account
- Sends the monthly statement to the cardholder

Cardholder receives the statement

Authorization Process Flow $1.00 Status Check Procedure

On this page details the process flow when performing a $1.00 status check. On the next page shows the process flow for the confirmation advice sent within two hours of the transaction.



Note: The authorization dispute protection for AFD terminals performing $1.00 status checks is U.S. $100.00 for U.S. issued Visa Business, Visa Corporate, Visa Purchasing, and consumer cards. For non-U.S. issued cards the amount is $75.

The authorization dispute protection for AFD terminals performing $1.00 status checks for Visa Fleet cards is U.S. $150.00.

If an authorization Dispute Condition 11.3 is submitted, then the dispute amount is limited to the amount that exceeded the approved authorization amount.

[2] For chip cards, the cardholder can remove the card as soon status check is completed and approved. It is recommended to add a beep to remind customer to pull out card before fuel dispenses.

AFD Confirmation Advice

Visa Core Rules and Visa Product and Service Rules require U.S. automated fuel dispenser merchants that perform $1 status checks to submit Acquirer Confirmation Advices (0120 non-financial messages) within two hours of the status check authorization.

These advices inform participating issuers of the final automated fuel dispenser transaction amounts, which in turn, provide more timely information so that they can effectively manage their Visa cardholder accounts and enhance their purchase experience at the pump.

Upon receipt of the authorization holds, participating issuers must release any holds exceeding the final transaction amount specified in the advice.

This requirement also benefits merchants, as they may receive fewer customer complaints regarding hold amounts that are greater than the final transaction amount.

Within two hours of transaction merchant sends online confirmation advice message indicating final amount of transaction to merchant bank.

Merchant Bank sends confirmation advice message to Visa.

VisaNet sends the confirmation advice message to the card issuer.

Card issuer releases the cardholder account hold when the confirmation advice message is received.

Clearing and Settlement $1.00 Status Check Flow

The following diagram illustrates the $1 status check authorization flow for clearing and settlement:

Merchant deposits the transaction receipt with merchant bank for the final transaction amount.

Merchant Bank credits the merchant's account and electronically submits the transaction to Visa for settlement.

VisaNet

- Facilitates settlement by paying the merchant bank for the transaction amount and debiting the card issuer account
- Sends the transaction to the card issuer

Card Issuer:

- Posts the transaction to the cardholder account
- Sends the monthly statement to the cardholder

Cardholder receives the statement

Purchase Process with Visa's Real-Time Clearing (RTC) Program

Visa's Real-Time Clearing (RTC) program has been designed to help retail petroleum merchants facilitate more flexible payment acceptance at the pump.

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 dispute protection
  The RTC program extends Dispute Condition 11.3 dispute protection up to the estimated amount of the pre-authorization (not to exceed U.S. $500).
- Automatic interchange qualification
  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. This 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.

How RTC Works – From Start to Finish

The following diagrams provide a high level look at how the RTC program works.

[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. Refer to Section VII: Accepting Fleet Card Payments in this guide for more detailed information.

Real Time Clearing AFD Transaction Authorization

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.

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.

The issuer approves or declines the transaction.

If approved, the merchant can dispense fuel to the cardholder.

Real Time Clearing AFD Transaction Clearing & Settlement

When the fueling is completed, the merchant submits the final amount within two hours, using a real-time completion message.

The transaction completion message contains the actual transaction amount (less than the authorized estimated amount).

Merchant Bank credits the merchant's account and electronically submits the transaction completion message to Visa for settlement.

VisaNet

- Facilitates settlement by paying the merchant bank for the transaction amount and debiting the card issuer account
- Sends the transaction to the card issuer

Card Issuer:

- Is required to release the cardholder account hold when the transaction completion message is received or within two hours of the pre-authorization request
- Posts the transaction to the cardholder account.
- Sends the monthly statement to the cardholder

Cardholder receives the statement

Key RTC Considerations

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

The merchant bank must support:

- Partial authorization.
- Single Message System (SMS) processing.

Smart Phone In-App Transaction Processing

Merchants who allow their customers to conduct AFD purchases using smart phone applications need to ensure the authorization messages contain the proper data elements to reflect these types of purchases. Below is a chart of authorization message fields impacted by smart phone in-app purchases and the required data elements.

Authorization Fields	Change from Card Present AFD Transaction Values	inApp AFD Transaction Values
Field 18 (Merchant Category Code)	No	5542
Field 22 (Point of Sale Entry Mode)	Yes	01 (Manual Key Entry) or 10 (Credential On File)
Field 25 (Point of Sale Condition Code)	Yes	59 (E-Commerce)
Field 60.1 (Terminal Type)	Yes	0 (Unspecified)
Field 60.8 (Electronic Commerce Indicator)	Yes	Varies by authentication type

AFD Fraud Prevention Best Practices

AFD best practices to mitigate fraud loss follow:

- 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 (swiping, inserting, or waving payment card for authorization without pumping).
  - Island surfing (individuals 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.
- 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).

- 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.
- 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.

Tools to Reduce AFD Fraud Risk

To help reduce AFD fraud, use the following tools and strategies:

- Visa Transaction Advisor (VTA)
- Address Verification Service (AVS)
- Velocity checking

Visa Transaction Advisor (VTA)

Visa Transaction Advisor (VTA) allows merchants to identify transactions with a higher risk of fraud and perform further cardholder authentication before gas is dispensed.

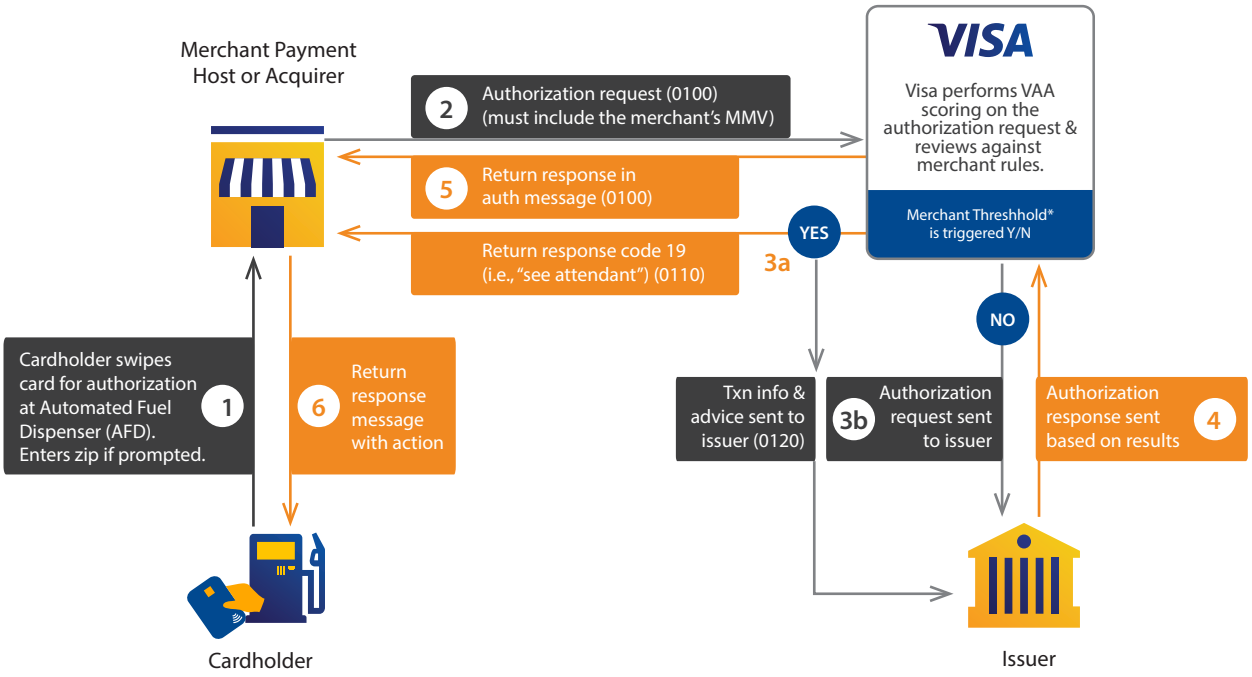
VTA works as follows: After a cardholder inserts the card at the pump, Visa analyzes multiple data sets, such as past transactions, whether the account has been involved in a data compromise, and nearly 500 other pieces of data to create a risk score for each fuel pump transaction.

If an AFD transaction exceeds a fraud score threshold set by the merchant, Visa sends the merchant a response code of '19' which the fuel pump translates to "See attendant."

This fraud management solution operates invisibly to the cardholder, helping to ensure a positive customer experience.

Visa Transaction Advisor also leverages existing payment processes, thus requiring minimal or no new investments in infrastructure changes.

Visa Transaction Advisor for AFDs – Process Flow



* Note: Visa sets a merchant approved, VTA rule based on VAA score. For the small number of bans over the score threshold, a Field 39 response code "19" would be sent to the merchant indicating the txn needs to be sent inside.

For more information, contact your acquiring bank, processor or Visa representative or email VTA@visa.com.

Address Verification Service (AVS)

Address Verification Service (AVS) verifies the five-digit billing statement postal code of the customer who is paying with a Visa card at an AFD. The postal code is included in the authorization request message to Visa.

The response message back will contain an AVS result code (separate from the authorization response code) that indicates whether the postal code given by the customer matches the postal code, on file, with the card issuer.

If:	Then:
There is a "no match" response	It may indicate fraud. He/she should be instructed to go inside to complete the fuel purchase transaction.
The cardholder does not correctly input his/her current billing statement postal code within two attempts	He/she should be instructed to go inside to complete the fuel purchase transaction

Note: Currently, AVS can only be used to confirm postal codes for cards issued in the United States and Canada.

Canadian Postal Codes

Canadian customers who travel to the U.S. can participate in AVS when prompted for a 5-digit numeric ZIP code at the pump, by doing the following:

Take the three numbers from the Canadian postal code.		Add two zeros to the end.		This is the number a Canadian cardholder can use when asked for a U.S. ZIP code.
FOR EXAMPLE:				
A2B 3C4	**+**	**00**		**23400**

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.
- Use the Visa AVS at high fraud locations. Visa recommends that merchants operating automated fuel dispensers take the following actions:
  - 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.
  - If the transaction is approved by the Issuer but the transaction is not completed due to an AVS "no match" response, the authorization approval must be reversed.

Velocity Checking

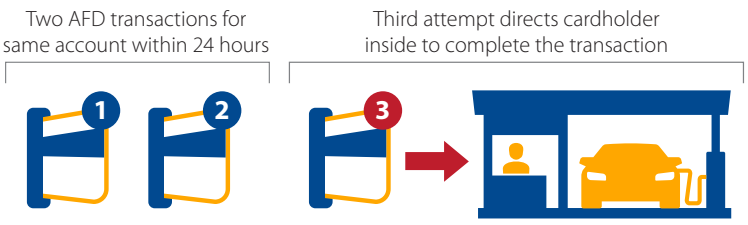
Velocity checking monitors the frequency of transactions on the same card. Visa recommends maintaining velocity checking programs that monitor card usage by each location as well as across all locations for the merchant brand.

Remember the velocity checking database must be PCI DSS compliant.

Two and In Strategy

The "Two-and-In" strategy is a good policy to apply for velocity checking. It works, as follows:

Two AFD transactions for the same account number within a 24-hour period at the same location, or across the brand, will cause the third attempt to be directed into the store to complete the fuel purchase transaction.



Visa Fraud Monitoring Program

The Visa Fraud Monitoring Program will be enhanced to identify AFD merchant outlets that generate excessive counterfeit fraud ("VFMP-AFD"). Acquirers will be subject to counterfeit fraud disputes for AFD merchant outlets identified in the enforcement period of the VFMP-AFD.

Visa is making this enhancement to protect U.S. issuers, cardholders, acquirers and fuel merchants from potential migration of counterfeit fraud to AFDs during the Extension Period. The VFMP-AFD program described in this VBN will be effective starting with the July 2017 VFMP-AFD program cycle for the Standard Program Timeline. The VFMP-AFD program related to the Excessive Program Timeline will take effect starting with the November 2017 VFMP-AFD program cycle. After the October 2020 VFMP-AFD program cycle concludes, U.S. acquired AFDs will be monitored under the terms of the existing VFMP defined in the Visa Rules along with all other U.S. acquired merchants.

The VFMP-AFD will leverage the existing VFMP program timelines and threshold structure. The program thresholds are tailored for counterfeit fraud activity at U.S. AFDs at both the Standard and Excessive Thresholds. Acquirers of AFD merchant outlets identified in the VFMP-AFD will not be subject to Non-Compliance Assessments.

Visa will notify U.S. acquirers of all the AFD merchant outlets in their portfolio which are identified in the VFMP-AFD through the Visa Risk Performance Tracking (VRPT) tool available on Visa Online.

Visa encourages all U.S. acquirers to review the fraud performance and risk controls for all of their AFD merchant outlets prior to the July 2017 VFMP-AFD program cycle. For any AFD merchant outlets which exceed the VFMP-AFD program thresholds, U.S. acquirers should work with their AFD merchants to identify solutions which could be implemented prior to the VFMP-AFD start date. Examples of potential risk controls include the Address Verification Service, Transaction Velocity Controls, Visa Transaction Advisor, etc.

To facilitate early identification of these AFD merchant outlets, Visa will provide advisory reports for each Acquirer BID starting with the March 2017 program cycle. These reports will be available through the VRPT. Acquirers should contact the Brand Protection team or their Visa Account Manager if they require assistance with these reports.

The VFMP-AFD program described in this VBN impacts only U.S. acquired AFDs for domestic U.S. transactions. The VFMP will continue to operate as currently defined in the Visa Rules for all U.S. non-AFD merchant types.

Updated Program Thresholds for U.S. AFDs

The enhanced VFMP will review the prior calendar month's domestic counterfeit fraud dollar totals and the domestic counterfeit fraud-to-sales ratio for all U.S. acquired AFDs.

U.S. acquired AFD Merchant Outlets will be identified on the VFMP-AFD "Standard Program Timeline" on a monthly basis if they meet or exceed the program's "Standard Threshold":

- $10,000 in domestic counterfeit fraud and
- 0.20% domestic counterfeit fraud amount to domestic sales amount ratio

U.S. acquired AFD Merchant Outlets will be identified on the VFMP-AFD "Excessive Program Timeline" on a monthly basis if they meet or exceed the program's "Excessive Threshold":

- $10,000 in domestic counterfeit fraud and
- 2.00% domestic counterfeit fraud amount to domestic sales amount ratio

Once a U.S. acquired AFD merchant outlet is over the Excessive Program Threshold, it will remain on the Excessive Program Timeline until it remediates out of the program.

Visa may escalate a U.S. acquired AFD merchant outlet from the Standard Program Timeline to the Excessive Program Timeline if it determines the merchant causes undue harm to the goodwill of the Visa payment system.

To address any cases of recidivism, Visa will escalate all U.S. acquired AFD merchant outlets to the Excessive Program Timeline that re-enter the VFMP-AFD within 12 months of completing their remediation.

Visa reserves the right to review and adjust either the Standard or Excessive Thresholds as needed.

VFMP – AFD Program Timelines

Tables 1 (Standard Program Timeline) and 2 (Excessive Program Timeline) show the acquirer obligations for each VFMP-AFD program month.

Table 1 - VFMP Standard Program Timeline

Program Status	Acquirer Actions/Provisions
Month 1 – Notification	Visa Inc. notifies the Acquirer their Merchant has been entered into the program. The Acquirer must review their Merchant's activity and take appropriate mitigating steps.
Month 2 to 4 – Workout Period	Acquirers must implement actions to reduce fraud levels at identified Merchants. Upon request, Acquirers must provide Visa Inc., with a remediation plan to address the fraud issue(s) starting with Month 2. Acquirers will provide updates to the remediation plan from Month 3 onwards.
Month 5 to 11 – Enforcement Period	• Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification. • The Acquirer must continue to implement their reduction plan, adjusting it as necessary to effectively reduce fraud. • The Acquirer must notify their Merchant they may lose Visa acceptance privileges if they remain in the program.
Month 12 – Enforcement Period	• Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification. • The Merchant is eligible for disqualification.

Table 2 - VFMP Excessive Program Timeline

Program Status	Acquirer Actions/Provisions
Month 1 – Enforcement Period	• Visa notifies the Acquirer their Merchant has been entered into the program. The Acquirer must review their Merchant's activity and take appropriate mitigating steps. Acquirers must implement actions to reduce fraud levels at identified Merchants. Upon request, Acquirers must provide Visa Inc., with a remediation plan to address the fraud issue(s). • Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification.
Month 2 to 5 – Enforcement Period	• Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification. • Acquirers must continue to implement actions to reduce fraud at identified Merchants and, upon request, provide Visa with updates to the remediation plan from Month 2 onwards.
Month 6 to 11 – Enforcement Period	• Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification. • Acquirers must continue to provide written updates to Visa detailing how the plan is effectively reducing fraud levels. • The Acquirer must notify their Merchant they may lose Visa acceptance privileges if they remain in the program
Month 12 – Enforcement Period	• The Merchant is eligible for disqualification. • Visa Fraud Monitoring Program (Dispute Condition 10.5) window will be opened to enable Issuers to recover counterfeit fraud losses associated with the current program identification.

As shown in Tables 1 and 2, Dispute Condition 10.5 applies to counterfeit fraud transactions associated with the respective "Enforcement Period" program months in VFMP. Dispute Condition 10.5 chargeback windows will not be opened until Program Month 5 in the Standard Timeline. In the Excessive Program Timeline, Dispute Condition 10.5 windows will open starting from Month 1. Note that Member Appeal Rights do not apply to Dispute Condition 10.5 disputes.

Remediation for Identified Merchants

For both Standard and Excessive program timelines in the enhanced VFMP, remediation will be considered successful if the merchant is able to remain below at least one of the listed performance thresholds for three consecutive months ("remediation period"). For example, VFMP remediation is successful if the U.S. acquired AFD merchant outlet remains below the $10,000 counterfeit fraud threshold for three consecutive months.

Merchants that have not completed the remediation period will continue to progress through the program timeline for each identification. If a U.S. acquired AFD merchant is identified in the enhanced VFMP at a new U.S. acquirer without completing the remediation period, their program status will be aligned with the other program case(s) and the merchant will continue in the program timeline where they left off. If an AFD merchant goes to an offshore acquirer, they will be subject to the EMV liability shift disputes as the other Visa markets already have the EMV liability shift in place.

In cases with egregious fraud or dispute activity, Visa may require the immediate termination of the merchant agreement or impose Member Risk Reduction Requirements on the acquirer to expedite remediation efforts as permitted by the Visa Rules.

Chip Lost and Stolen Liability for AFD Transactions

Effective 1 April 2014 issuers are financially liable for lost and stolen fraud for all online-authorized chip (contact and contactless) AFD transactions, regardless of the Cardholder Verification Method (CVM) used.

While the transaction does not need to contain a PIN, the chip on the card (contact or contactless) must be read by the terminal.

Differences between Magnetic-Stripe and Chip Card Acceptance

Ensure sales staff know the procedural differences between magnetic-stripe and chip card acceptance:

- Chip cards are inserted into the reader and must remain inserted until the transaction is completed. Early removal of the card from the reader will terminate the transaction.
  - This differs from the magnetic-stripe method where the merchant swipes the card and immediately removes it in a single motion.
  - As terminal messages vary, any message that signals when a transaction is completed should be clearly identified. Merchants and their customers should be educated to remove the card from the terminal only after seeing this message.
- Merchant staff should prompt cardholders to insert the card into the chip reader rather than swiping the magnetic-stripe.
  - This will make the transaction process faster and mitigate the potential problem where an issuer may have incorrectly personalized the card with a service code that does not correspond to the chip card.

Dispute Mitigation for AFD Transactions

For dispute mitigation, follow these guidelines when dealing with authorization related, fraud and duplicate processing disputes.

[7] If the use of the terminal's manual override feature is allowed

Authorization Related Disputes (Dispute Condition 11.3)

This dispute applies to transactions that were not authorized (possibly due to systems being down). Stop the pump at the $100 limit ($150 for Fleet Cards) for $1 status check authorizations.

After downtime, reauthorize all stored transactions versus forwarding directly into settlement to prevent:

- No-authorization disputes
- Zero-floor limit misuse fees
- Transaction interchange downgrade
- Debit Transaction Integrity Fees (TIF)

Fraud Disputes (Dispute Condition 10.3)

This dispute is related to fraudulent transactions.

- Ensure all transactions are electronically authorized.
- Use Visa Transaction Advisor, Address Verification Service and Velocity Checking together to avoid fraudulent transactions.

Duplicate Processing Disputes (Dispute Condition 12.6)

This dispute is because "a single transaction" was processed more than once on the same account number.

- Ensure that your POS systems are not submitting duplicate transactions to the acquirer.

Invalid Disputes (Dispute Condition 13.3 and 13.6)

Disputes 13.3 – Defective Merchandise and 13.6 Credit Not Processed are invalid for AFD transactions. If received they should be sent back to the issuer.

Authorization Related Disputes (Dispute Condition 11.3)

This dispute applies to transactions that were not authorized (possibly due to systems being down).

Stop the pump at the $100 limit for $1 status check authorizations.

After downtime, reauthorize all stored transactions versus forwarding directly into settlement to prevent:

- No-authorization disputes
- Zero-floor limit misuse fees
- Transaction interchange downgrade
- Debit Transaction Integrity Fees (TIF)

Fraud Disputes (Dispute Condition 10.3)

This dispute is related to fraudulent transactions.

- Ensure all transactions are electronically authorized.
- Use Visa Transaction Advisor, Address Verification Service and Velocity Checking to avoid fraudulent transactions.

Duplicate Processing Disputes (Dispute Condition 12.6)

This dispute is because "a single transaction" was processed more than once on the same account number.

- Ensure that your POS systems are not submitting duplicate transactions to the acquirer.

IV. Processing Considerations and Management

Introduction

The Processing Considerations and Management section covers principles that are key to achieving fuel transaction processing and funding efficiencies.

Owner/Operator Authorization Best Practices

An authorization protects the merchant, and may also be used to optimize interchange qualification. In the U.S., the floor limit has been set to zero, meaning all fuel transactions must be online authorized.

Best practices for retail petroleum owners and operators include the following:

- Authorize all purchase transactions.
- If the cardholder does not continue with the transaction, an authorization reversal must be issued for the full amount.
- For transactions conducted in the service station if the approved amount is not fully dispensed an authorization reversal must be issued for the remaining amount.
- For AFD transactions when a $1 status check authorization is used, merchants must send an AFD confirmation advice message.
- 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 an authorization dispute right for the amount that exceeds the authorization amount.

Note: When supporting chip, there are requirements for reversals.

Contact your acquirer and refer to the Transaction Acceptance Device Guide (TADG) and the U.S. Acquirer Implementation Guide (AIG) for more information visit:

TADG: https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/visa-emv-merchant-tadg.pdf

AIG: https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/visa-emv-merchant-aig.pdf

Ensuring Customer Satisfaction Best Practices

Customers expect 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.

The following are best practices to help ensure customer satisfaction:

- Check automated fuel dispenser key pads to make sure they 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 make sure 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.

Principles

There are several principles important to fuel transaction processing and card acceptance. They are, as follows:

1. **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 a specified 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 a specified 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 provides 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.

       This can result in 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.
2. **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.
   - A merchant in a high-fraud area should prompt for a ZIP or postal code using AVS (Address Verification Service).
   - These decisions are important when it comes to minimizing fraud and for managing acceptance costs.
3. **The merchant and its merchant bank must determine the appropriate method to authorize and then subsequently allow the amount of fuel to be pumped per customer based on the approved authorization.**
   - It is important for merchants to consider that transactions exceeding the allowable limit from the approved authorization are potentially at risk for no authorization disputes according to Visa operating guidelines. (This dispute is be limited to the amount exceeding the limit.)
   - This limit is important for both setting authorization transaction amount and for setting the limit on the amount of fuel dispensed at the pump.

Deferred or Delayed Authorizations

Deferred or delayed authorizations may occur when the device does not have online capability (i.e., during outages or downtime for AFDs) and the online authorization is performed after the card is no longer available.

Merchants performing this type of authorization should complete it within 24 hours of the transaction.

When authorization processing is back on-line, the merchant should request an authorization and only submit approved transactions for clearing and settlement.

Because the U.S. has a zero floor limit, a merchant who supports the completion of transactions when authorization systems are offline will have several other considerations and requirements; this practice is not recommended.

Prior to submitting transactions for settlement, acquirers or merchants who do not obtain online approval do so at their own liability. Also, it is important to note that this practice is against Visa Rules. Consult your acquirer for more information.

Account Holds Best Practices

Fuel purchases are unique 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.

Account holds present risk to all parties involved including the issuer and merchant, as they can restrict the use of account funds and can prevent other purchases by the consumer.

As the customer may blame the merchant for the funds restriction, merchants can help minimize this risk by following these best practices:

- Set estimated authorization amounts appropriately or through use of a status check authorization.
- Submit AFD confirmation advice messages as soon as possible after the fuel has been pumped.
- Submit clearing messages for the final amount as promptly as possible.
- Reverse unused authorizations or reverse the portion of authorization that is not used for service station transactions.

Visa Easy Payment Service (VEPS)

Visa Easy Payment Service (VEPS) is a global program that allows qualifying low-value transactions of $25 or less at specific merchants to take place without cardholder verification. A receipt is not required unless requested by the cardholder.

Service Stations (MCC 5541) are eligible to participate in VEPS for in-store and attended transactions if the POS terminal is not EMV Chip enabled.

Use VEPS to make payment processing faster and easier for both merchants and customers while increasing sales.

This is especially beneficial to high-volume merchants since it allows merchants to serve more customers and reduces customer time spent in-line.

As part of the VEPS program, merchants:

- Do not need to register for VEPS. If you are eligible to participate, contact your merchant bank or processor.
- 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.
- Are protected from illegible fulfillment such as: Transaction not recognized, and Fraud-Card Present disputes.

Partial Authorization

Merchants are encouraged to participate in the Visa Partial Authorization. Visa Partial Authorization enables participating merchants to receive an approval for a partial amount of an in-store or AFD transaction (i.e., the amount available on the card) when the amount in the original authorization request exceeds the available card balance.

The issuer is able to return an authorization response with an approval for a portion of the original amount requested. This enables the transaction to be capped at the partial authorized amount. If the merchant wishes to dispense above the amount returned in the partial authorization response, the remainder of the transaction amount can be paid by other means using split tender functionality, where applicable.

This service provides an alternative to receiving a decline when the available card balance is not sufficient to approve a transaction in-full and can result in increased sales for the merchant.

U.S. merchants who do not support partial authorizations for AFD transactions are assessed a fee of $0.01 per transaction.

Disparities Between the Authorized Amount and Settled Amount

Disparities 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 dispute liability.

- Merchants should ensure that limits are in place for the fuel dispensed, and that these limits do not exceed the authorized amount.
- Authorization 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. They are also required on approved authorizations where the merchant elects not to complete the transaction because of a "no match" AVS response.

Visa's Global Point of Sale (POS) Counterfeit Liability Shift

Visa's global point of sale (POS) counterfeit liability shift is important to all key stakeholders in the payment industry because it encourages a "chip-on-chip" transaction (i.e., a chip card read by a chip terminal) that provides dynamic authentication data.

This, in turn, helps to better protect all parties. With this Liability Shift comes a set of rules for determining who holds the liability for a counterfeit point-of-sale transaction.

Under these new rules, the party that is the cause of a chip transaction not occurring, either the issuer or acquirer, will be held financially responsible for any resulting card-present counterfeit fraud losses.

- Issuers assume counterfeit fraud-related liability if a non-chip card is presented at a chip-capable terminal.
- Acquirers assume counterfeit fraud-related liability if a counterfeit chip card is presented at a non-chip-capable terminal.

The 1 October 2015 EMV liability shift applies to all issuers and acquirers in the U.S. with the exception of transactions at AFDs and ATMs.

Effective 1 October 2017 transactions made at AFDs for non-U.S. issued cards will be included in the EMV liability shift.

Effective 1 October 2020, transactions made at AFDs for U..S. issued cards will be included in the EMV liability shift.

Change in Value After Transaction Was Pre-Authorized for Chip Cards

After pre-authorization, there can be a change in value (above or below) for the total transaction involving chip cards.

Some examples include:

- More fuel dispensed than was pre-authorized
- Card-based discounts when as EMV payment card triggers a discount. In these cases, the discount is applied in clearing – not in authorization.
- Dual cards where loyalty and payment are on the same card. This may reduce the value of the transaction.

Process these chip cards transactions in the same way you would process a magnetic-stripe transaction.

Note: The transaction amount may not match the cryptogram amount. The merchant must not compare or change the amount authorized in tag 9F02 to the actual transaction amount.

Fallback If the Terminal Cannot Read the Chip

If the chip-reading device cannot read the chip on the card, the terminal should first fallback to magnetic stripe. If the magnetic stripe cannot be read, only then should key-entered take place. Key-entered transactions should always be the last option. **Effective April 2017** key-entered acceptance is optional for EMV chip enabled merchants.

Because the fallback transaction is either swiped or keyed, the normal rules of transaction processing for zero floor limit transactions will come into play, as applicable:

For	Requirement
Swiped transactions	A signature is required, without an option to capture a PIN.
Key-entered transactions	A manual imprint is required.

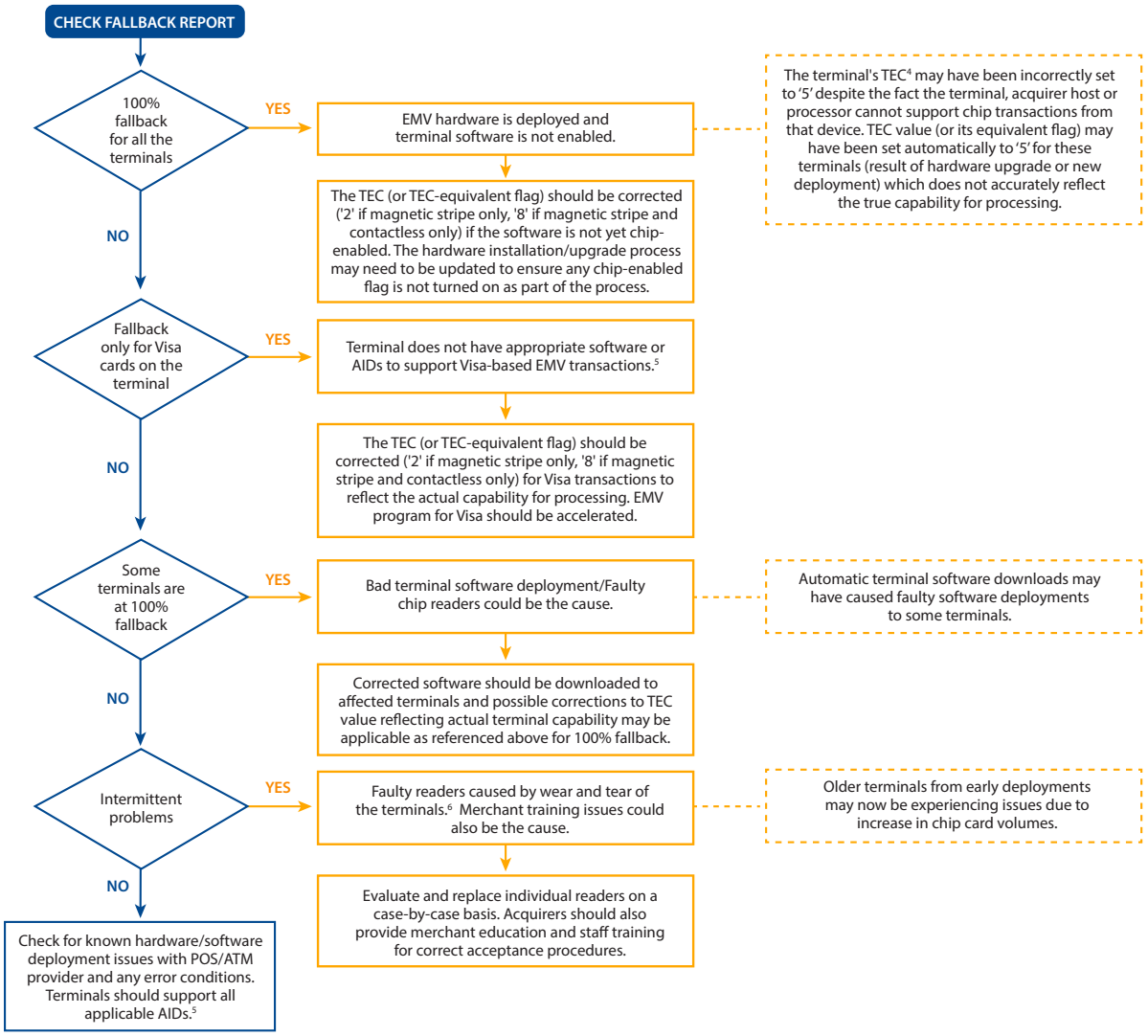
Merchants should not force a fallback to magnetic stripe or key-entry, as they are more likely to see higher levels of authorization declines for these transactions from issuers than for valid chip transactions.

Visa strongly recommends that all card-present transactions be initiated with an electronic read. Electronically-read data provides valuable risk management information to the issuer and appropriate protection to the merchant.

Major Causes of Fallback

There are number of reasons for fallback ranging from data quality issues to faulty devices. It is essential that monitoring procedures are followed to ensure fallback levels are kept to a minimum.

The following flowchart outlines the major causes of fallback and the suggested recommendations to minimize it. The best way to minimize fallback is to analyze and monitor fallback reporting as well as check for potential issues based on trends discovered from reporting.



Ensure staff are trained to follow the prompts on the terminal to avoid higher levels of key-entered transactions.

The liability shift does not impact key-entered rules as the counterfeit liability remains with the party that has not invested in chip technology.

[4] TEC (Terminal Entry Capability) is a one-digit value that identifies a terminal's ability to electronically read account data from Visa cards or mobile devices. Value of 2 indicates the terminal can read only magnetic-stripe cards, 5 indicates the terminal can read contact chip cards and possible contactless chip form factors/mobile device or magnetic-stripe cards.

[5] Terminals must support the applicable AIDs to minimize fallback transactions. All POS terminals must support Visa AID and Visa Electron AID; ATM terminals must support Visa AID, Visa Electron AID and Plus AID. To support Interlink acceptance, terminals must have the Interlink AID; and support for US Common Debit AID is optional.

[6] In some cases for ATMs, the chip reader might be inaccessible to the card due to damaged clamps, caused by wear and tear (clamps are used to hold the card). This could lead to fallback at these locations.

Fallback if a Card Won't Read When Swiped

A key-entered transaction is manually keyed into a point-of-sale (POS) device when a magnetic-stripe cannot be read; key-entry procedures may be used at the POS as a last resort and only if fallback to magnetic-stripe is not possible.

Key-entered transactions have different rules than chip fallback to magnetic stripe and should not be considered "fallback to magnetic stripe."

During the migration to chip, clients should ensure that staff are trained to follow the prompts on the terminal to avoid higher levels of key-entered transactions.

KEY POINT TO REMEMBER

As of 1 October 2015, counterfeit fraud chip liability shift also affects key-entered transactions. The liability remains with the party that has not invested in chip technology.

Key-Entered or Voice-Authorized Transactions

Key-entry is optional for POS terminals that are chip enabled.

Key-entered[7] transactions must be processed by making an imprint of the front of the card. The imprint proves the card was present at the POS and can protect a merchant's business from potential disputes if the transaction is fraudulent. The imprint can be made either on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.

Voice-authorized transactions must be processed by making an imprint of the front of the card.

To minimize key-entered transactions, acquirers and merchants should implement staff training and monitoring to effectively pinpoint areas with high key-entry rates. The following monitoring steps help identify problem areas:

- Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which stores, terminals or sales associates have high key-entry rates.
- Merchants are encouraged to monitor these key-entry fallback rates on a monthly basis, as these transactions are less secure and have higher processing fees.

Key-entered and voice-authorized transactions are not supported for Visa Electron cards or Unattended Cardholder Activated Terminals (UCATs).

For key-entered transactions, an issuer dispute for Dispute Condition 10.3 is valid unless:

- The merchant can provide an imprint for domestic and international transactions.
- The merchant captured the CVV2 for U.S. domestic transactions only.

Unembossed Cards

If an unembossed card will not swipe and the chip cannot be read, you should ask for another form of payment.

Do not manually key-enter unembossed cards, take photographs of, or write the account number on a paper draft. A marked paper draft will not protect a merchant against disputes.

[7] If the use of the terminal's manual override feature is allowed.

Properly Place Contactless Readers

Properly place contactless readers to ensure seamless usage by cardholders and maintain the principle of a fast transaction.

Best practices include to:

- Ensure the reader is free from obstructions and easily accessible for cardholders to use the contactless payment feature.
- Place contactless card readers at least 12 inches away from each other.

  In retail locations where the counter space is limited, the magnetic field of multiple readers in close proximity may overlap. This can disrupt the contactless transaction when a single contactless card is presented.
- Display the contactless symbol on all readers to let cardholders know "how and where" they can use Visa payWave cards.

Visa Branding of Payment Terminals

Visa has developed a set of guidelines and artwork to be used by acquirers, merchants, and other partners to accurately reproduce the Visa brand mark and the contactless symbol on payment terminals.

The guidelines and artwork are available from Visa. Acquirers and vendors should contact their Visa representative to obtain a copy.

Support of No Cardholder Verification Method and PIN

PIN pads remain a requirement for POS terminals that process debit transactions via Interlink.

It is recommended that when accepting online PIN for magnetic-stripe debit, to also accept chip debit with online PIN.

Support for offline PIN is not required when supporting online PIN, as those offline PIN preferring cards from foreign markets are also required to support signature allowing for traditional acceptance in the U.S. market.

Finally, if a merchant does not support PIN today then there is no Visa requirement to support PIN on chip in any format.

If participating in VEPS, there will be programing of the terminal capabilities based on transaction parameters.

Effective 1 July 2015, all online-capable chip enabled (contact and contactless) terminals including AFDs (ATMs excluded) must support the processing of transactions without a CVM.

V. Accepting Fleet Card Payments and Visa Fleet and Automatic Fuel Dispenser Recommendations

Accepting Fleet Card Payments

Introduction

The Accepting Fleet Card Payments section outlines merchant considerations and best practices for ensuring proper Visa Fleet card payment acceptance in the retail petroleum environment.

Visa Fleet Card Functionality

The Visa Fleet card is used by mid -to large-sized companies and government entities as a payment tool for fuel and maintenance expenses for company fleets or vehicles.

Visa Fleet functionality includes enhanced authorization and clearing capabilities for participating fuel locations in the United States. To support the Visa Fleet product, enhanced data is provided by fuel merchants.

Requirements

Since 1 October 2013, fuel merchants for Visa Fleet cards are required to:

- Recognize a Visa Fleet card when it is presented at the point-of-sale and provide complete and accurate enhanced data from the fuel transaction to their processor.
- Correctly identify the service prompt indicator encoded on a Visa Fleet card magnetic-stripe and prompt the cardholder to provide the required data; afterward, fuel merchants forward this information with the enhanced data from the fuel transaction to their processor.

Levels of Enhanced Data

Visa Fleet transactions may qualify for three data capture levels as defined in the chart below.

Level	Example
1	Provides standard Visa draft transaction data provided by Visa merchants. No enhanced data is captured at this level.
2	Supports enhanced data capture at the point-of-sale without significantly affecting merchant operations or acquirer clearing processes. Level 2 data capture includes a six-digit numeric vehicle, driver, or generic ID; type of purchase; fuel type; unit of measure; quantity; gross fuel price; odometer reading, and tax information. Clients can use these elements to track expenditures and for tax obligations.
3	Provides the most comprehensive reporting available, allowing a merchant to pass a detailed accounting of fuel and non-fuel goods and services purchased to buyers. Level 3 enhanced data provides summary information about Visa Fleet card transactions and detailed information about each line item.

Fleet Transaction Data Processing

The VisaNet clearing and settlement system is the transport mechanism for enhanced data. The transactions use financial and non-financial records that must be matched to form a complete, enriched transaction. The enhanced data can be generated by the acquirer.

A unique characteristic of the Visa Fleet card data approach is the use of two separate record types for enhanced data capture.

- Level I and Level II data capture is designed to work within the existing TC 05 financial clearing record. No additional records are required for these transactions to be cleared.
- Level III data requires the use of one or more TC 50 specifically-formatted records in most cases.

Visa Fleet enhanced data provides unprecedented spend visibility for fraud prevention and vehicle management.

Highlighted are Level II and Level III data:

Level II Data	Level III Data
• Vehicle's odometer reading • Driver or Vehicle ID • Transaction Date/Time/Location • Total Purchase Amount • Fuel Type • Fuel Purchase Amount • Fuel Unit of Measure • Fuel Unit Cost • Fuel Unit Quantity Purchased • Service Type • Gross/Net Fuel Amounts • Gross/Net Non-Fuel Amounts • Fuel Tax/Non-Fuel Tax	**Level II fuel data plus for each line item:** • Item Commodity Code • Item Descriptor • Product Code • Quantity • Unit of Measure • Unit Cost • Tax Amount • Tax Rate • Discount Amount • Line Item Total

Expanded Authorization Controls

Custom authorization controls, preselected by fleet managers, can be used to help direct and control the type(s) of purchases that cardholders are allowed to make.

Issuers can use a vehicle, driver, or generic (customer-specified) ID entered at the point-of-sale as part of their process to approve or decline a transaction.

Examples of authorization control criteria follow:

	Example	Custom authorization control criteria
Vehicle card	A fleet manager may restrict use of a vehicle to drivers from one department.	Issuer matches the account number to an authorization file of driver IDs (or generic IDs) to verify authorized drivers for a specified vehicle.
Driver card	A fleet manager may allow any driver in sales to use any sales department vehicle, while restricting drivers in operations from using vehicles assigned to the sales department.	Issuer matches the Visa account number to an authorization file of vehicle IDs (or generic IDs) to verify which vehicles the driver is authorized to operate.

POS System Modifications

POS systems vary depending on the configuration at each store location. Merchants are encouraged to work with their merchant bank in preparing for Visa Fleet card payment acceptance and processing.

To implement the enhanced data capability, modify your systems to support the following levels 2 and 3 data capture requirements:

- Capture enhanced data with the proper POS device. It must be able to:
  - Read the data on Track 1 or Track 2 of the magnetic-stripe or track 2 equivalent data on the chip card.
  - Display the appropriate prompts, and capture the appropriate response.
  - Depending on the merchant's card acceptance system, this enhancement may require changes to the register or in-store processor software. The register must recognize Visa Fleet card transactions.
- Ensure Visa Fleet authorization request messages; enter BASE I for processing.

Best Practices

- Develop enhanced settlement file formats for batch to your merchant bank. Changes may be required to the message formats used between the merchants and their merchant banks to accommodate the enhanced data.
- Develop procedures to create the new data formats for enhanced transaction data and BASE II line item detail information.
  - For example, merchants that accept fleet cards may provide detailed fuel information or an item descriptor and quantity for maintenance products.
- Provide additional clearing and settlement reports for your merchant bank, when required, to assist with settlement.
- Restrict the purchase of non-fleet items.
  - For cards with a service enhancement Indicator of 1 in the magnetic-stripe, indicating Visa Fleet service, make the necessary changes to restrict the purchase of non-fleet items point-of-sale. Non-fleet items are defined as those items with a Visa-defined product code of 70 or greater, including grocery items and cigarettes.
  - For cards with a service enhancement Indicator of 2 in the magnetic-stripe, indicating fuel-only cards, make the necessary changes to restrict the purchase of non-fuel items at the point- of-sale, including grocery and maintenance items.

KEY POINT TO REMEMBER

Some merchant POS systems may not be able to restrict the purchase of some items.

- Modify your visual display units to display Visa Fleet card transaction prompts and messages to the cardholder during the course of the transaction
  - Examples of prompts that can be displayed are the odometer reading and the six-digit numeric vehicle, driver, or generic ID.
  - Examples of messages include decline messages based on product restrictions. The merchant's POS configuration determines where the messages are displayed.
  - Determine the appropriate messages to display at the POS for Visa Fleet card transactions. Although Visa Fleet has not introduced any new authorization responses, the POS fleet cardholder prompts must be considered.

- Modify printer receipts to reflect added information available through Visa Fleet card transactions.
  - Examples include: odometer reading, product code, POS device location (merchant name, city, state, and ZIP code), local transaction date and time, Visa card number, total transaction amount, unit price, fuel type, and fuel quantity (number of gallons).
- Evaluate and modify your POS systems to include Visa Fleet card transaction data elements in the logs. Transaction logs assist in daily internal reconciliation and facilitate research and exception transaction processing. The evaluation should include a review of how the logs will be used (e.g., transaction research to assist in dispute resolution). This evaluation assists the merchants in identifying data requirements.

Migration to EMV

The same indicators and service prompts as current magnetic-stripe should be supported. This approach will minimize changes and enable acquirers and merchants to support both chip and magnetic-stripe cards during the chip migration.

The service enhancement Indicators and service prompts reside in the same position in the Track 2 equivalent data (Tag '57') of the EMV chip (Visa Global Credit AID).

Merchants should continue to maintain BIN tables to identify fleet cards to indicate the use of the service Indicator and service prompts. In the product ID field a value of:

- S1 indicates Visa Purchasing with Fleet
- S2 indicates Visa Government Purchasing with Fleet

Fleet Training and Communication

Merchants are encouraged to work with their merchant bank to ensure that their staff is properly trained to support Visa Fleet card payment acceptance.

- Develop materials and procedures necessary that meet the needs of your back-office staff based on the estimated impact that Visa Fleet card acceptance will have on your back-office operation.
- Create procedures for performing Visa Fleet card acceptance at the POS.
- Create marketing and quick-reference materials that describe POS card acceptance and device operation procedures.
- Create a store implementation plan to establish priorities and timeframes for availability of required Visa Fleet card POS marks, and a schedule for store activation by region and city.

POS Processing Requirements

Modify your POS devices to support the following processing requirements:

- If a POS device erroneously prompts for fleet information from a non-fleet participant, the POS device must allow the cardholder to press "enter" and bypass the fleet prompt.
- If the chip or the magnetic-stripe cannot be read and the card account number must be manually entered, the POS device must prompt for a six-digit numeric vehicle, driver, or generic ID and the odometer reading.
  - If the cardholder is prompted for the vehicle, driver, or generic ID or the odometer reading, or both, and the information is not supplied, the data fields in the clearing record must be filled with zeros.

Education and Training

Participate in your merchant bank training programs to familiarize your staff on how to:

- Process the Visa Fleet card point-of-sale, including identification of the cards and their electronic and manual processing
  - Perform POS device procedures and reference materials (including enhanced data entry procedures)
- Answer customer questions about the use of Visa Fleet cards
- Refer customer questions to the appropriate authority

Visa Fleet and Automatic Fuel Dispenser Recommendations

Introduction

As the U.S. market prepares for the 2020 Automatic Fuel Dispenser (AFD) EMV® counterfeit liability shift, many stakeholders ask: "What are Visa's recommendations for migrating from magnetic stripe to EMV in the petroleum retail market in the U.S.?"

Visa's U.S. migration strategy for the point of sale has been to focus on a very simple, online only acceptance, leveraging existing online magnetic-stripe infrastructure which is robust, real-time, and always online for authorization and authentication. The petroleum retail industry is no different. The primary goal of this strategy is to limit disruption by simplifying implementation.

Chip terminal implementations are more complex when compared against their magnetic-stripe counterparts. However, Online Only chip terminals are significantly less complex when compared to offline capable solutions. Finally, the scope and effort associated with testing an Online Only chip terminal is significantly reduced when compared against all other terminal configurations.

Fleet card issuance follows a similar approach. Visa recommends leveraging the existing infrastructure to ensure a smooth transition to chip, by using an online only chip card profile with the fleet service indicators in the Track 2 Equivalent Data on the chip. This approach reduces complexity in personalization and host development.

The balance of this section is divided into two parts.

- Part One focuses on U.S. chip card issuance in the context of fleet
- Part Two focuses on Visa's Online Only AFD configuration in the context of the U.S. market.

Because the U.S. is a zero-floor limit country, all transactions must go online for authorization. Additionally, due to the presence of both magnetic stripe and chip terminals in the market place over the next few years, as well of the lack of a fully agreed industry standard, the fleet service indicators should be kept in Track 2 Equivalent Data on the chip.

Online Only AFD terminals always send a transaction online for authorization. If PIN support is needed, a PIN pad is added to the hardware configuration.

Merchants are encouraged to work directly with their acquirer and/or terminal deployer to determine the approved EMVCo terminal configurations offered that satisfy Visa's U.S. Online Only terminal requirements. Approved EMVCo terminal configurations (chip reader and chip software) are a global industry requirement, and the U.S. is no exception.

To ease implementation and testing, Visa has developed the Quick Chip specifications, which are recommended for any online-only implementation, and strongly recommended for AFDs.

Considerations for Fleet Card Issuance

Chip Card Personalization – Online Only

Personalizing a chip card as online only is significantly simpler than adding any offline functionality. There are no requirements for certificates, nor are there any requirements to update the issuer's host system to add offline risk parameters. Furthermore, because there is no need for issuer authentication and scripting, this functionality also doesn't need to be developed for issuer host systems.

Fleet Service Indicators

Due to the co-existence of magnetic stripe and chip terminals, the simplest way to incorporate fleet prompts is to mirror the process as it is done for the magnetic stripe today, by adding the Fleet Service Indicators in Track 2 Equivalent Data (tag '57') on the chip. The Fleet Service Indicators are in the last 3 positions of field 57, as defined below:

Field Position	Field Name	Possible Values
1	Reserved	Reserved for future use; the default value is 0 (zero)
2	Service Enhancement Indicator	0 = Fleet, No Restriction (fuel, maintenance, and non-fuel purchases) 1 = Fleet (fuel- and maintenance-only purchases) 2 = Fleet/Fuel Only (fuel-only purchases) 3-9 = Reserved
3	Service Prompt	0 = Reserved (no prompt required) 1 = Identification (ID) and odometer reading 2 = Vehicle ID and odometer reading 3 = Driver ID and odometer reading 4 = Odometer reading 5 = No prompt 6 = ID[8]

Application Interchange Profile – Online Only

The Application Interchange Profile (tag '82') is a list of capabilities the card sends to the terminal stating what the card is able to do. The simple Online Only value is '18 00', which corresponds to no Offline Data Authentication and no Issuer Authentication.

Cardholder Verification Method List (CVM)

The Cardholder Verification Method List (tag '8E') is a list of Cardholder Verification Methods supported by the card. Visa's standard CVM List for fleet is '0000 0000 0000 0000 0201 1E04 0005 5E00 1F00'. This corresponds to a simple signature-preferring card, with No CVM at unattended devices (which include AFDs), as well as Online PIN for ATM access.

Issuer Action Codes

An EMV terminal will determine how to direct a transaction (online, offline, or decline) by comparing the Terminal Verification Results (tag '95') with Terminal Action Codes (TACs) and Issuer Action Codes (IACs). The TVR is a 5-byte bit map that tracks specific transaction events and the Action Codes share that same 5-byte bitmap. The terminal compares the Action Codes in pairs against the TVR as follows:

1. **TAC/IAC – Denial**, any match vs. TVR results in decline request. Card must respond with decline cryptogram.
2. **TAC/IAC – Online**, any match vs. TVR results in online request. Card must respond with online cryptogram or decline cryptogram.
3. **TAC/IAC – Default**, only if terminal cannot go online, any match vs. TVR results in decline request. Card must respond with decline cryptogram.

Visa's recommended Issuer Action Codes for U.S. fleet cards are the following values:

Issuer Action Code – Denial	= '00 00 00 00 00'
Issuer Action Code – Online	= 'FC 70 BC 98 00'
Issuer Action Code – Default	= 'FC 50 AC 88 00'

[8] After prompt for ID, the cardholder enters the six-digit numeric vehicle, driver, or generic ID.

Quick Chip

Quick Chip is an enhanced implementation of the standard EMV flow, which allows for early removal of the card, without waiting for the issuer response, similar to how the magnetic stripe works today. Quick Chip additionally allows for a much simpler testing suite. Since it removes the possibility for Issuer Authentication and scripting at the terminal, testing for those possibilities has also been removed. For more information please refer to Quick Chip for EMV Specification (**www.visachip.com**, under "Quick Chip for EMV") regarding how to implement Quick Chip.

Considerations for EMV Acceptance at Petroleum Retail Merchants

Authorization and Clearing Considerations

In-store transactions follow the standard EMV processing flow used for general retail transactions. There are three acceptable ways to process AFD authorizations:

- **The cardholder may determine an exact amount to be authorized and dispensed.**
  The AFD generates an authorization for the exact amount, and a clearing record (TC05) for the exact amount is generated later.
- **The cardholder does not know the final amount of purchase.**
  The AFD sends a pre-authorization request for $1. This type of pre-authorization request is known as a "status check."[9] An AFD Confirmation Advice (0120 non-financial message) containing the actual amount is generated within two hours of the status check authorization. A clearing record (TC05) is generated for the actual purchase amount.
- **The cardholder does not know the final amount of purchase.**
  If the merchant and acquirer participate in the Real Time Clearing program, the AFD sends an estimated pre-authorization request. The pre-authorization amount is a good faith estimate based on spending patterns at the merchant and can be up to US $500. A real-time clearing record (0220 Acquirer Financial Advice) is generated for the actual purchase amount.

In each case, the chip data, including the cryptogram, will be included in the authorization/pre-authorization message (0100). For contact or contactless chip transactions, the chip cryptogram amount should be whatever amount is contained in the authorization message.

No chip data is required in the clearing/advice (TC05/0220) or the final amount notification (0120) from the dispenser as long as the transaction is online authorized.

Terminal Type – Online Only

A terminal configuration is essentially a collection of parameters that drive specific behavior associated with a chip transaction. It also determines the EMV testing that is performed by the accredited laboratory. Visa does not require that specific terminal configurations (i.e., Terminal Types) be used in production, but does require that the EMV kernel always requests an online configuration. (Always asks for an ARQC at 1st Gen AC, unless a product restriction is in place.)

Online Only chip implementations are significantly less complex when compared against offline capable solutions.

The first parameter considered when setting up an Online Only terminal is Terminal Type (tag '9F35'). The Fleet Terminal Type value for Visa's U.S. Online Only configuration is '24' – Online Only, Unattended Merchant (POS). However, other Terminal Types may be used for AFDs as long as the Level 2 configuration effectively acts as an Online Only Unattended terminal.

While the Terminal Type data object is important in expressing the device capabilities, alone it is not sufficient to ensure that the terminal will always attempt

[9] A status check provides authorization protection up to a certain value depending on card type. Please see "Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants" for more information.

to go online. The Terminal Floor Limit (tag '9F1B') must be set to zero ('00 00 00 00') and the Terminal Action Code – Online byte 4, bit 8 is set to 1.

Note: If the Level 2 configuration supports a Terminal Type of Offline w/ Online Capability, these can easily be deployed as Online Only configurations by ensuring the Terminal Floor Limit and TAC values are configured as defined in this document.

During an EMV transaction the Floor Limit is compared against the transaction amount. When the transaction amount is greater than or equal to the Floor Limit, the terminal sets an indicator in Terminal Verification Results (tag '95'). The comparison of IAC/TACs vs. TVR is described under Issuer Action Codes above, and is called Terminal Action Analysis. An Online Only terminal may forgo the normal Terminal Action Analysis and always request to go online.[10]

Minimally, Visa's (POS) Terminal Action Codes must carry the following values:

Terminal Action Code – Denial	= '00 10 00 00 00'
Terminal Action Code – Online	= '58 40 04 F8 00
Terminal Action Code – Default	= '58 40 00 A8 00'

An Online Only device must configure Terminal Action Code – Online byte 4, bit 8 = 1. As the Terminal Floor Limit is set to zero, this forces the setting of TVR byte 4, bit 8 = 1. Therefore, if a terminal has not already determined a condition to decline the transaction, the transaction will be forced online based on the process described above.

Application AIDs

Visa Application Identifiers (AIDs) allow the terminal to recognize and interact with Visa's payment applications on the chip. The Visa AIDs that must be programed in an Online Only AFD are:

Visa Credit/Debit (Required)	– 'A0 00 00 00 03 10 10'
Visa Electron (Required)	– 'A0 00 00 00 03 20 10' (processed in the U.S. as Visa credit transactions)
Interlink (Optional)	– 'A0 00 00 00 03 30 10'

The Visa U.S. Common Debit AID may be added to support debit routing arrangements:

Visa U.S. Common Debit AID (Optional)	– 'A0 00 00 00 98 08 40'

Terminal Capabilities & Additional Terminal Capabilities

Terminal Capabilities (tag '9F33') and Additional Terminal Capabilities (tag '9F40') will also carry specific settings for an Online Only AFD. These data objects are both formatted as binary bitmaps and their settings are expressed as such. For a Visa U.S. Online Only AFD, the minimum settings are as follows:

Terminal Capabilities (tag '9F 33')	
Byte 1, bit 7	– Magnetic stripe (when the chip terminal integrates such hardware)
Byte 1, bit 6	– IC with contacts
Byte 2, bit 7	– Online Enciphered PIN
Byte 2, bit 4	– No CVM Required

[10] See EMV v4.3 Book 3, Section 10.7 for a summary of special Online Only kernel options associated with Terminal Action Analysis.

Additional Terminal Capabilities (tag '9F 40')	
Byte 1, bit 7	– Goods
Byte 1, bit 6	– Services
Byte 4, bit 7	– Printer, cardholder
Byte 4, bit 5	– Cardholder display

Final Contact Chip Terminal Considerations

Readers familiar with EMV terminal configurations will note that features common in other regions of the world are not expected in Visa's U.S. Online Only AFD configuration. In particular, no Offline Data Authentication (ODA) is specified in the Terminal Capabilities. Online Only devices are not required to support ODA features, reducing the need for EMV terminal key management. Support for offline PIN is not required when supporting online PIN, as those offline PIN preferring cards from foreign markets are also required to support No CVM, allowing for traditional acceptance in the U.S. market.

U.S. EMV Fleet cards (as described in this paper) and Online Only terminals do not support offline approvals, meaning merchants/acquirers with temporary network connectivity issues should consider adopting a Deferred Authorization approach. This Deferred Authorization approach, sometimes called Store & Forward, is common in many magnetic-stripe environments and is equally suited to Online Only EMV environments. Such an approach addresses network latency issues for EMV without the cost, development, and complexity of a fully offline capable EMV solution.

Visa U.S. EMV transactions will initially attempt to go online (i.e. GenAC 1 = ARQC). When a host connection is unavailable, the card/terminal will typically perform an EMV offline decline (i.e. GenAC 2 = AAC) due to the Zero Floor Limit and the mandatory Terminal Action Codes. However, when implementing Deferred Authorization the terminal may approve the transaction and delay or defer the GenAC 1 ARQC authorization request until the network connection is restored.

No special terminal logic is needed to determine if a Deferred Authorization is allowed, such as checks on TVR or TSI4, which could override the card decision to initially send the transaction online. In the U.S., chip data in clearing is optional for Visa. However, if the merchant chooses to include chip data in the clearing record, the GenAC 1 ARQC, and not the GenAC 2 AAC, should be included assuming an approval was received. In the event the deferred authorization request was declined, that transaction must not be cleared or settled.

In a Deferred Authorization environment, the merchant must consider the risk of completing a local approval, and implement appropriate risk management such as velocity checking and total cumulative amount checking. Deferred Authorization risk management for EMV is identical to magnetic-stripe situations, carrying the same open to buy risk, meaning an issuer could decline for insufficient funds and merchants would absorb the loss should this occur. However, such exposure is typically small and can be sized by evaluating the current overall decline rate, applying the likely number and value of transactions that would occur during a host outage. Visa's Acceptance Solutions team can help evaluate the financial impact of a Deferred Authorization approach.

Merchant/acquirers who also wish to participate in the TIP program to reduce their PCI audit must deploy a dual-interface terminal which supports both EMV contact chip and contactless chip transactions.

Finally, while chip data is required to be included in the authorization request and authorization response messages: **there are no requirements to carry chip data in the clearing and settlement messages.** This means that in the U.S. these merchant and acquirer interfaces remain largely unchanged.

EMV Configuration

EMV terminal providers will be intimately familiar with the configuration options associated with their particular device and will provide guidance on satisfying Visa's Online Only requirements. However, to facilitate discussions with terminal providers, this table is an extraction from the EMV application kernel Implementation Conformance Statement (ICS). This extraction summarizes the necessary options for a Visa Online Only AFD; these features are also expressed on the EMV Letter of Approval.

Other brands may have other requirements which are outside the scope of this paper.

FEATURE	SETTING
Terminal Type	Online Only
. . .	
Magnetic Stripe	Required
IC with Contacts	Yes
. . .	
Onlined Enciphered PIN	Optional
. . .	
No CVM	Required
. . .	
Transaction Type – Goods	Yes
Transaction Type – Services	Yes
. . .	
Print, Cardholder	Yes
Display, Cardholder	Yes
. . .	
Partial AID Selection	Yes
. . .	
Common Character Set	Yes
. . .	
Fail CVM	Yes
. . .	
Floor limit checking	Yes
. . .	
Terminal Risk Management irrespective of AID Setting	Online Only

Contactless Considerations

Older versions of Visa payWave supported two different transaction flows: legacy Magstripe Data (MSD) that passes over the RF interface track 1 & track 2 data along with a dynamic CVV, and a Quick Visa Smart Debit Credit (qVSDC) flow that passes over the RF interface with full cryptographic data. Globally, merchant terminals should now be designed to support only qVSDC transaction flows. Issuer cards may still be designed to support both the MSD and qVSDC transaction flows, which ensures that any contactless form factor can be accepted at any merchant terminal.

With the global migration to full chip processing now underway, the need for terminal support of the legacy MSD transaction flow is redundant and should be avoided as:

- Visa Approval Services no longer accepts contactless terminals / readers supporting MSD only
- All issuer products minimally support qVSDC
- Development, certification, and integration efforts are essentially doubled when supporting both MSD & qVSDC
- Terminals supporting both MSD & qVSDC will never process the MSD flow as qVSDC has priority

Supporting the qVSDC path alone, and removing MSD support, from contactless reader development or integration requirements is the streamlined approach to contactless acceptance.

Streamlined qVSDC Configuration

Support of contactless acceptance is not required, however if supported, the qVSDC reader/terminal configuration can be significantly simplified by following this streamlined qVSDC Configuration.

- Terminal Transaction Qualifiers (tag '9F66')
  - AFDs must minimally support qVSDC, CDCVM, and require an online cryptogram ('20 80 40 00')
  - Optionally, add support for Online PIN ('24 80 40 00')
- Reader Contactless Floor Limit (terminal proprietary data object) = $0 - as the U.S. is a zero floor limit country, does not preclude Store & Forward/Deferred Authorization integrations
- Reader Contactless Transaction Limit (terminal proprietary data object) = maximum or null value - allows for a contactless transaction of any amount (per Visa Rules, this limit must not be set)
- Reader CVM Required Limit (terminal proprietary data object) = $0

Additional Reading for Acquirers and Issuers

Additional Reading for Acquirers

The following resources are available via acquirer licensing:

- Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants
- Visa Smart Debit/Credit (VSDC) and Visa payWave U.S. Acquirer Implementation Guide (www.visachip.com) – Acquirer guidance for chip acceptance.
- EMV in the U.S.: Simplifying Deployment in a Zero Floor Limit Environment – Detailed review of the Visa online only strategy.
- Visa's Transaction Acceptance Device Guide (www.visachip.com) – Overview of terminal chip acceptance.
- Visa Transaction Acceptance Device Requirements – Summary of Visa acceptance business rules.
- Quick Chip for EMV Specification www.visachip.com, under "Quick Chip for EMV") – Specification regarding how to implement Quick Chip.

Additional Reading for Issuers

The following resources are available via issuer licensing:

- Visa Smart Debit/Credit (VSDC) U.S. Issuer Implementation Guide – Issuer guidance for contact chip issuance.
- Visa Smart Debit/Credit Personalization Requirements for U.S. Implementations – Issuer guidance for chip personalization.
- VCPS U.S. Issuer Implementation Guide – Issuer guidance for contactless issuance.

VI. Interchange Costs Management

Introduction

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

Interchange and Pricing

Payment acceptance has associated costs that need to be closely monitored and managed. An important component of this cost is the Interchange Reimbursement Fee (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, it is imperative that retail petroleum merchants control interchange downgrades.

Interchange Best Practices

Interchange best practices include:

- Ensuring that the transaction qualifies for the appropriate Custom Payment Service (CPS) program
- Avoiding downgrades that result from miscoded transaction files. Consider the following:
  - Carefully testing initial deployment and any subsequent changes to the POS system.
  - Ensuring that each POS is coded to the proper Merchant Category Code (MCC):
    - 5542 must be used for all automated fuel dispenser transactions.
    - 5541 is used for in-store and attended forecourt fuel purchases.
- Ensuring that transaction clearing batches are transmitted to the merchant bank at least once a day.
- Working with the merchant bank to ensure correct interchange is 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.
- Using peer benchmarks and historical patterns to identify anomalies in qualification patterns in conjunction with the merchant bank.
- Conducting 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.).

CPS/Retail Service Station (Credit or Debit) Program Qualification

Service station transactions can qualify for the CPS Retail Service Station Program. In a CPS/Retail Service Station transaction, the card, the cardholder, the merchant, and the terminal are all present.

The magnetic-stripe or chip is read, the authorization request is approved, the receipt is typically signed, and the cardholder's signature is typically verified.

To qualify for the CPS/Retail Service Station program, a transaction must have the following characteristics:

- MCC must be 5541 (Service Stations)
- One authorization per clearing transaction is allowed.
- Unaltered contents of Track 1 or Track 2 of the card's magnetic-stripe must be read and transmitted, or unaltered chip data must be sent.
- The card must be present at the point-of-sale.
- Transaction must clear in two days.
- Purchase date must be within one day of the authorization date.
- Cardholder's signature must be obtained, unless the transaction qualifies as a VEPS transaction.

Debit card transactions must also have the merchant name and location included in the authorization request.

CPS/Retail Key Entry Program Qualification

In a CPS/Retail key-entered transaction, the card, cardholder, merchant, and terminal are all present.

The magnetic-stripe cannot be read, the authorization request is approved, the receipt is signed, and the cardholder's signature is verified.

To qualify for the CPS/Retail Key-Entry (credit or debit) program, a transaction must have the following characteristics:

- One authorization per clearing record allowed.
- Cardholder must be present and signature must be obtained.
- Card must be present, with key-entry due to failure in reading the magnetic-stripe.
- Transaction must not be a mail order/telephone order (MOTO) or eCommerce transaction.
- Transaction must clear in two days.

Fuel transactions processed as Real-Time Clearing (RTC) will clear same day. For more information regarding the RTC processing option, refer to the *Visa Real Time Clearing for Fuel Program Implementation Guide for Acquirers and Merchants.*

- AVS is requested in the authorization, resulting in a ZIP code match, retry, or unsupported AVS result.
- Purchase date must be within one day of the authorization date.

CPS/Automated Fuel Dispenser (Credit or Debit) Program Qualification

To qualify for the CPS/Automated Fuel Dispenser (credit or debit) program, a transaction must have the following characteristics:

- MCC must be 5542.
- The transaction must take place at a cardholder-activated terminal connected to a fuel dispensing device for the purchase of fuel such as gasoline, diesel fuel or propane.
- The cardholder-activated terminal must be equipped to accept cards.

- The final transaction amount must be $125.00 or less.
  - If the transaction was only partially approved, then the final transaction amount must be equal to or less than the approved amount.
- One authorization per transaction allowed, which includes:
  - $1 status check, **and**
  - Merchant name and location.
- Full magnetic-stripe must be read and transmitted or the unaltered chip data must be sent.
- No verifiable cardholder identification is present.
- Transaction must clear in two days and include the following:
  - Clearing amount must be less than or equal to $125.00.
  - Purchase date must be within one day of the authorization date.
- Business certification must be completed for operation of the Cardholder-Activated Terminal (CAT) transaction.

VII. Cardholder Data Security

Introduction

The Cardholder Data Security section focuses on the tools and controls to safeguard cardholder data. It addresses how to deal with attacks by fraudsters through skimming devices. It also covers Payment Card Industry, Data Security Standard (PCI DSS) compliance and the validation of compliance.

Payment Card Fraud Major Concern for Retail Petroleum Merchants

Payment card fraud continues to be a major concern for retail petroleum merchants. Unattended fuel dispensers are easy to access for the fraudster who wishes to remain anonymous to commit 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 test whether counterfeit cards could be accepted. Attended forecourts also have exposure, particularly when the attendants participate in fraudulent activities.

As fuel is a desirable commodity, the fuel purchases, whether in-store or at an AFD, 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.

Payment Card Skimming Devices

Fraudsters are targeting AFDs by installing skimmers to capture payment card data from magnetic stripe cards. It is important to understand the current threats and risks to properly safeguard against skimming devices.

Different types of skimmers can be installed on AFDs. One type of skimmer can be installed between the card reader and ribbon to capture payment card data as it is entered. Another type of skimmer is an overlay device that fits over a POS terminal that can be undetected by the store cashier or customer. Both types can capture payment card data to memory and are copied or sent to the fraudster to commit counterfeit fraud.

Safeguards against skimmers for retail petroleum merchants should include:

- Use of anti-tampering tape over the gas pump access door
- Ensure CCTV monitoring of all gas pumps
- Check POS terminals regularly inside the store
- Provide employee training and awareness to look for skimming devices and overlays on POS terminals

What to do if Skimming Devices are Discovered

If skimming devices are discovered, take the following steps:

- Do not approach or confront anyone who looks suspicious, or who is installing or removing a skimming device.
- Document and take pictures of the skimming device.
- Use protective gloves to remove the device.
- Contact the local authorities and U.S. Secret Service.

PCI DSS Compliance

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 PCI 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.
  - The PCI DSS consists of twelve basic requirements. These requirements are the foundation of Visa's data security compliance program.
  - 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.

Twelve Basic Requirements

The PCI DSS reflects a layered approach in which no single security measure should ever be relied on to provide complete protection from trespassers.

Risk of intrusion is minimized by applying multiple layers of security measures that work together. All Visa members, merchants and service providers must adhere to the PCI DSS twelve basic requirements, which are supported by more detailed sub-requirements.

PCI DSS Basic Requirements	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Validation of Compliance

Separate from the mandate to comply with PCI DSS is the validation of compliance. Validation ensures the merchant has achieved PCI DSS compliance and helps ensure that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined validation levels based on volume of transactions and the potential risk and exposure introduced into the Visa system. All merchants are required to re-validate PCI DSS compliance annually.

Use of an approved PCI PIN Transaction Security PIN Entry Device also referred to as PCI PTS PED and adhering to PCI PIN Security Requirements are intended to further protect Visa cardholder PINs both in the POS and in the transporting networks.

Visa requires both PCI PTS PED and PCI PIN compliance for all PIN entry. This compliance includes mandates to use Triple DES to protect PIN data. This compliance includes use of approved PCI PTS PEDs as well as use of Triple DES and/or AES to protect PIN data..

PIN Security

Visa is committed to protecting Visa cardholder PIN data. To that end, Visa created a PIN Security Program outlining compliance requirements. Acquirers, their merchants and/or their third party agents must comply with this program.

The baseline requirements for the Visa PIN Security Program include:

- PCI PIN Security Requirements
  www.pcisecuritystandards.org/document_library Filter by PTS
- Visa PIN Entry Device (PED) Requirements
  www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

When purchasing PIN entry devices ensure you check they are on the Approved PIN Transaction Security (PTS) Devices list.

In addition to the PED requirements Visa's maintains a list of compromised PEDs which are an extension of the PED requirements.

- Visa Triple Data Encryption Standard (TDES) Requirements are:
  - All ATMs must use TDES to protect pins

Visit the Visa PIN Security website (www.visa.com/pinsecurity) to understand PIN Security Program requirements.

Adherence to the requirements of the Visa PIN Security Program results in more than simply securing PIN data. Sound security practices help to protect organizations from adverse financial and reputational consequences often associated with PIN data compromises.

Petroleum merchants that acquire PIN transactions and/or perform key management services for only their own acquiring business must perform appropriate due diligence to ensure compliance with the PIN Security Program requirements. This may include performing self-assessments using an internal or external resource. Individuals performing the self-assessment must have adequate knowledge of the PCI PIN Security requirements but do not need to be Visa approved PIN Security Assessors.

Self-assessment results do not need to be submitted to Visa; however, Visa may request evidence of PIN security compliance or request an on-site PIN Security review of any organization, at any time, to ensure the security of the payment system. A PIN Self-Assessment Questionnaire (PIN SAQ) template is available on Visa's PIN Security website, www.visa.com/pinsecurity.

Secure technologies such as point-to-point encryption and tokenization, when implemented in accordance with the PCI DSS may help simplify PCI DSS compliance.

Go to https://www.pcisecuritystandards.org for guidelines on these technologies.

More information on Visa requirements for PCI DSS are available on www.Visa.com/CISP.

VIII. Chip Implementation

Introduction

The Chip Implementation section covers terminal configuration, testing and AID requirements. All other specific chip best practices and procedures are detailed as they relate to the other sections in this guide.

Terminal Configuration

Given the U.S. is a zero floor limit market and online infrastructure, Visa recommends to support the U.S. Minimum Terminal Configuration Guidelines. The majority of U.S. chip cards will not support offline approvals.

Refer to Visa's Minimum terminal configuration guidelines at www.Visachip.com.

These guidelines provide 100% protection against liability shift while significantly reducing implementation cost and complexity, and there are no requirements for offline functionality.

DID YOU KNOW?

There is no difference in terminal configuration between attended and unattended AFDs.

Contact and Contactless Chip Terminal Testing Requirements

Visa developed the Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET) to provide separate sets of test cards and test cases to be used on contact and contactless chip POS terminals prior to deployment.

These test cards help to ensure correct terminal configuration, assist with integration testing and meeting Visa's terminal requirements for both EMV contact chip and contactless chip devices.

The test results for ADVT and CDET are submitted to Visa via the Chip Compliance Reporting Tool (CCRT). Acquirers must use the appropriate toolkits before initial terminal deployment to help ensure that the terminal is fully operational and configured correctly.

Use of the ADVT and the CDET is intended to:

- Ensure basic contact and contactless chip functionality is not compromised during application integration
- Ensure all Visa requirements are satisfied
- Identify common interoperability issues

Use of the toolkits does not imply or guarantee that a terminal is fully compliant with EMV specifications or Visa requirements.

The ADVT and the CDET can be obtained through Visa's third party fulfillment service, Merrill Corporation. Similar tools are also available from Visa-confirmed third party vendors.

For a list of Visa-confirmed tool vendors, see Products and Toolkits at https://technologypartner.visa.com/default.aspx.

These tools can help reduce required testing, standardize point-of-sale solutions and modularize and/or isolate EMV chip functionality with the payment application.

Merchants should consult with their acquirer for their testing requirements.

For further information, see Visa Chip Bytes and the Visa U.S. Chip Terminal Testing Requirements at www.Visachip.com.

Visa Electron and Interlink AID Support

All chip-reading devices (contact and contactless) must contain the appropriate Application Identifier (AID). Terminals must support the Visa Electron and Interlink (if applicable) AIDs to avoid interoperability issues.

If the required AIDs are missing from chip-enabled terminals, transactions from chip cards may be processed as fallback transactions.

Visa Electron is issued exclusively outside the U.S.; Visa Electron transactions are processed as Visa transactions in the U.S., so Visa Electron can be accepted anywhere Visa is accepted.

Merchants should continue to accept Visa Electron the same way they accept magnetic-stripe transactions today; for chip transactions, terminals need the Visa Electron AID. Therefore, to support Visa Electron acceptance in the U.S. when implementing contact and/or contactless chip, POS terminals and ATM devices must have the Visa Electron AID—A0000000032010 present.

KEY POINT TO REMEMBER
Visa Electron cards will not contain the Visa AID.

To support Interlink acceptance, contact and contactless chip-reading POS terminals must have the Interlink AID—A0000000033010 present when they are deployed. All POS terminals accepting Interlink must support the Visa AID and Visa Electron AID, in addition to the Visa Interlink AID; support for the Visa U.S. Common Debit AID is optional.

Note: Interlink can be accepted only at terminals capable of processing online PIN verification.

All chip-reading devices (contact and contactless) must contain the appropriate AIDs.

A table outlining the complete AID list for each product is included in the Visa Minimum U.S. Online Only Terminal Configuration guide on www.Visachip.com

With Chip, What is the Same?

Review the Myth versus Reality chart to better understand what remains the same with chip implementation:

As fuel merchants prepare to upgrade their automated fuel dispensers (AFD) to support chip there are special considerations to be taken into account for CVM processing. Those fuel merchants who do not support PIN at the ADF are not impacted and can accept chip cards in much the same was as is done in magstripe, completing the transaction with No CVM.

Cardholder Choice for Debit Transactions

For those fuel merchants who do support PIN at the AFD, processing both credit and debit transactions, chip offers a variety of implementation options. Visa recommends one of the following be adopted during the AFD chip integration:

- Selectable Kernel were the Terminal Capabilities (tag '9F 33') are dynamically configured based on a Debit / Credit button push, or its equivalent (e.g. "Debit Y/N", "Is this a Debit card", etc.)
  - Credit push loads No CVM only configuration (tag '9F 33' = '00 08 00') and transaction processed as credit
  - Debit button push load Online PIN & No CVM (tag '9F 33' ='00 48 00') and transaction processed as debit

This approach closely replicates the existing magstripe infrastructure use of Debit / Credit buttons today.

- Configure the AFD kernel Terminal Capabilities to support Signature, Online PIN, and NO CVM (tag '9F 33' = '00 68 00'). This allows a single terminal configuration and relies on the CVM List personalized to the card for the chosen AID. Should the CVM List resolved Signature discard the signature capture line.

This approach aligns with how contactless CVM processing has been implemented at the ATM.

Note: When automatically selecting the US Common Debit AID the cardholder must still be allowed an option to cancel or exit from PIN entry.

- Implement EMV PIN Entry Bypass for both the Visa Global AID & US Common Debit AID. This is consistent with how cardholder choice is managed in some US POS implementations.
- For an Online PIN prompt offer a proprietary method to cancel or exit from PIN entry, where the transaction is restarted with a dynamic configuration of Terminal Capabilities set to No CVM only (tag '9F 33' = '00 08 00').

Any of the above options provide a consistent cardholder experience, when compared to magstripe, for those cardholders who prefer not to enter their PIN at the AFD while preserving merchant debit routing options.

Quick Chip at the AFD

All benefits available for Quick Chip at the point-of-sale are inherently available for Quick Chip at the AFD. Quick Chip allows for a simplified integration effort of EMV technology taking advantage of an online only terminal configuration, which additionally reduces the scope of test and certification. Quick Chip solutions can be deployed in a manner of days or weeks, when compared to the months or years necessary to deploy a classic chip terminal solution.

Quick Chip at the AFD allows for removal of the card before transmission authorization request and receipt of the issuer authorization response, without impact to merchant routing options while supporting all CVM methods.

Quick Chip at the AFD processing follows this basic procedure:

- Cardholder chip insert and transaction initiated with single unit of currency (e.g. $1.00).
- EMV selection process, read application data, and CVM processing.
- EMV terminal action analysis where the card returns an online cryptogram (ARQC).
- All chip data necessary for the authorization forwarded to the AFD payment application.
- EMV completion processing, allowing for card removal. Some UI management may be required to correctly alert the cardholder of the various transaction state.
- AFD payment application forwards the chip authorization request, authorization approval then allows fuel to be dispensed.

More information on Visa Quick Chip is available from https://www.visa.com/chip or by contacting your Visa representative directly.

Additional Resources for EMV Chip

To learn more about EMV Chip, go to Visachip.com Merchant Resources page at:
https://www.visa.com/chip/personal/security/chip-technology/index.jsp

Refer to:

- *Visa Inc. U.S. EMV Chip Terminal Testing Requirements*
- *Visa Kernel Management Guidelines for Contact and Contactless Chip Terminal Implementations*
- *Visa Minimum U.S. Online Only Terminal Configuration*
- *Visa Transaction Acceptance Device Guide*
- *Visa U.S. Merchant EMV Chip Readiness Guide: 10 Steps to Planning Chip Implementation for Contact and Contactless Transactions*
- *Visa Chip Bytes—EMV Chip Acceptance: When to Test*

Go to VisaOnline.com and refer to:

- *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide*

Glossary of Terms

Account Number	The 16-digit account number that appears embossed or printed 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.
Address Verification Service (AVS) (Canada)	An optional VisaNet service through which a merchant can verify a cardholder's billing address before completing a transaction in a card-absent environment.
Application Identifier (AID)	A data element that identifies the application in a card or terminal such as Visa Debit/Credit or Visa Electron. It is composed of the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX)
Address Verification System (AVS) (U.S.)	A VisaNet service through which a merchant can verify a cardholder's billing address before completing any one of the following: • A mail/phone order or eCommerce transaction where merchandise or airline tickets will be delivered to the cardholder or the cardholder's designee, or where services were purchased. • A CPS/retail key-entry transaction • A CPS/account funding transaction or CPS/eCommerce basic transaction • A CPS/eCommerce preferred retail transaction • A CPS/eCommerce preferred hotel and car rental transaction • An AFD transaction (ZIP code only inquiry) • A face-to-face environment transaction if the merchant has been qualified by Visa to use AVS (ZIP code only inquiry)
ATM	An unattended magnetic-stripe, contactless or chip-reading terminal that has electronic capability, accepts pins, and disburses currency.
Authorization	A process where an issuer, a VisaNet processor, or Visa Stand-In Processing (STIP) approves a transaction. This includes offline authorization.
Authorization Center	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.
Authorization Monitoring	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.
Authorization Reversal	A VisaNet message that cancels an approval response previously sent through the V.I.P. System as specified in the *Visa Core Rules and Visa Product and Service Rules* and applicable VisaNet manuals. An authorization reversal may be for the full amount.
Automated Fuel Dispenser (AFD)	A Self-Service Terminal or Automated Dispensing Machine that dispenses fuel such as gasoline, diesel fuel, or propane.
Card Security Features	The alphanumeric, pictorial, and other design elements that appear on the front and back of all valid Visa cards, as specified in the *Visa Product Brand Standards*. Card-present merchants must check these features when processing a transaction at the point-of-sale to ensure that a card is valid.
Card Verification Value (CVV)	Unique check value encoded on the magnetic-stripe of a card to validate card information during the authorization process. The card verification value is calculated from the data encoded on the magnetic-stripe using a secure cryptographic process.
Card Verification Value 2 (CVV2)*	A unique check value printed on the back of a card, which is generated using a secure cryptographic process, as specified in the ***Payment Technology Standards Manual.***

Cardholder	The person or entity whose name is embossed on the face of a card or encoded on the magnetic-stripe.
Cash-Back	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.
Chargeback	A transaction found to be improper and sent back to the Acquirer Center with other outgoing interchange.
Chip	An electronic component designed to perform processing or memory functions.
Chip card	A card embedded with a chip that communicates information to a point-of transaction terminal.
Chip-initiated transaction	An EMV and VIS-compliant chip card transaction that is processed at a chip-reading device using full-chip data, and limited to Visa and Visa Electron Smart Payment Applications, or EMV and VIS-compliant Plus applications.
Chip-reading device	A point-of-transaction terminal capable of reading, communicating, and processing transaction data from a chip card.
Contactless Payment Terminal (U.S.)	A point-of-transaction terminal that reads the magnetic-stripe data on a contactless payment chip through a Visa-approved wireless interface, and that includes magnetic-stripe-reading capability.
Counterfeit Card	A counterfeit card includes one of the following: • A device or instrument that is printed, embossed, or encoded so as to purport to be a card, but that is not a card because an issuer did not authorize its printing, embossing, or encoding • An instrument that is printed with the authority of the issuer and that is subsequently embossed or encoded without the authority of the issuer • A card that an issuer has issued and that is altered or re-fabricated, except one on which the only alteration or re-fabrication comprises modification of the signature panel or cardholder signature
Dispute	A dispute provides an issuer with a way to return a disputed transaction through VisaNet. It's a value that an issuer returns to an acquirer—and most often, to the merchant—as a financial liability. In essence, the issuer reverses a sales transaction.
Dual-Interface	A dual-interface chip card supports both contact and contactless transactions (as well as magnetic-stripe).
Embossed Account Number	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.
Expired Card	A card on which the embossed, encoded or printed expiration date has passed.
Face-to-Face Transactions	An environment where a transaction is completed under all of the following conditions: • Card or proximity payment device is present • Cardholder is present • Individual representing the merchant or acquirer completes the transaction Transactions in this environment include the following: • Retail transactions • Manual cash disbursements • Visa Easy Payment Service (VEPS) transactions Transactions in this environment exclude the following: • eCommerce transactions • Mail/phone order transactions • Recurring transactions • Unattended transactions • Installment billing transactions
Fallback Transaction	An EMV chip card transaction initially attempted at a chip-reading device, where the device's inability to read the chip prevents the transaction from being completed using the chip card data. The transaction is instead completed using an alternate means of data capture and transmission.

Interchange	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.
Issuer	A client that enters into a contractual relationship with a cardholder for the issuance of one or more card products.
Key-entered transaction	A transaction that is manually keyed into a point-of-sale device. Card present key-entered transactions also require an imprint of the card and a signature, to verify that a card was present at the time of the transaction.
Magnetic-Stripe (Mag-Stripe)	A magnetic-stripe on a card that contains the necessary information to complete a transaction.
Magnetic-stripe reader	The component of a point-of-sale device that electronically reads the information on a payment card's magnetic-stripe.
Merchant	A principal or entity entering into a card acceptance agreement with a Visa member financial institution.
Merchant Agreement	A contract between a merchant and an acquirer containing their respective rights, duties, and obligations for participation in the acquirer's Visa or Visa Electron Program.
Merchant Bank	Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services.
Merchant Discount Reimbursement (MDR)	The fee charged to the merchant by the merchant bank for processing services that enable the merchant to accept payment cards. MDR is the Interchange Reimbursement Fee (IRF), plus agreed upon merchant bank costs.
Mini-Dove Hologram *(May appear on the back of Visa Brand Mark cards)*	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."
Payment Card Industry Data Security Standard (PCI DSS)	A set of comprehensive requirements that define the standard of due care for protecting sensitive cardholder information. The PCI DSS was developed by Visa and other major card brands to help facilitate the broad adoption of consistent data security measures on a global basis.
Personal Identification Number (PIN)	A personal identification numeric code that identifies a cardholder in an authorization request.
Point of Sale (POS)	The location at which the sale/transaction takes place.
Point-of-sale (POS) terminal	The electronic device used for authorizing and processing Visa card transactions at the point-of-sale.
Printed Account Number	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.
Printed Number	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.
Processor	A client, or Visa-approved non-member acting as the agent of a member, that provides authorization, clearing, and/or settlement services for merchants and/or members. The *Visa Core Rules and Visa Product and Service Rules* refers to three types of processors: authorizing processors, clearing processors, and V.I.P. system users.
Referral Response	An authorization response where the merchant or acquirer is instructed to contact the issuer for further instructions before completing the transaction.

Sales Transaction Receipt	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).
Skimming	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. The account information 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.
Split tender	The use of two forms of payment, or legal tender, for a single purchase. For example, when buying a big-ticket item, a cardholder might pay half by cash or check and then put the other half on his or her Visa credit card. Individual merchants may set their own policies about whether or not to accept split-tender transactions.
Third Party Agents	An entity, not defined as a VisaNet processor, that provides payment-related services, directly or indirectly, to a member and/or stores, transmits, or processes cardholder data. No financial institution eligible to become a principal member of Visa may serve as a third party agent. A third party agent does not include: • Financial institutions that perform agent activities • Co-branding or Affinity partners • Affinity co-brand partners or global co-branding partners • Card manufacturers • Card personalizers
Transaction	The act between a cardholder and a merchant that results in the sale of goods or services.
Visa Easy Payment Service (VEPS)	Visa point-of-transaction service that permits qualified Visa Easy Payment Service merchants to process small value transactions, as specified in the *Country Level Visa Easy Payment Service Transaction Limits* without requiring a cardholder verification method or the issuance of a transaction receipt unless requested by the cardholder in accordance with the procedures specified in the *Visa Core Rules and Visa Product and Service Rules*.
Visa payWave Application	A Visa application contained on a contactless chip that enables a contactless payment transaction to be performed, as specified in the Visa contactless payment specification.
Visa Transaction Advisor (VTA)	Helps fuel retailers prevent credit and debit card fraud at the pump. It uses intelligent analytics that identify higher-risk transactions that may be fraudulent.
Voice Authorization Center	VTA assigns a risk score for each fuel pump transaction. If the score exceeds the fraud score threshold set by the merchant, Visa sends the merchant a response code of '19' which the fuel pump translates to "See attendant." An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic point-of-sale terminals or whose electronic terminals are temporarily not working, or who have transactions that require special assistance.

® EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.