Payments Acceptance Compliance 101

First Data Corporation reserves the right to make changes to this document at any time and without notice. The information furnished in this publication is believed to be accurate and reliable; however, no responsibility is assumed by First Data Corporation for its use.

This document provides an overview of the Interchange process for Visa®, MasterCard® and Discover®, as well as Program Pricing for American Express OptBlue™. The Interchange Qualification Matrix (IQM) and American Express Program Pricing Guide supplied by your Merchant Acquirer provide the qualification and criteria for the various interchange/pricing programs.

Contents

1. Interchange Process Overview

Visa, MasterCard and Discover (Card Brands) function as intermediary organizations creating networks between financial companies, including major banks and credit unions that issue cards bearing the Visa, MasterCard or Discover name, and merchants providing goods and services.

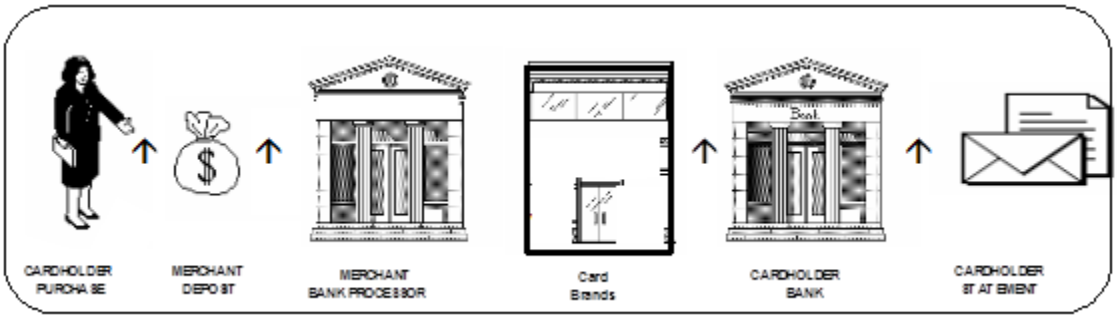
Visa, MasterCard and Discover perform several key functions including, but not limited to:

- Licensing of banks for card issuance
- Licensing of banks for merchant acquiring
- Operating regulations
- Global authorization and settlement
- Interchange
- Product development
- Advertising and promotion

A critical function managed by the Card Brands is interchange. This function enables banks around the world to exchange information, transactions, money and other items on a standard and consistent basis.

An important component of the interchange function is the fee, which is assessed on all transactions (i.e., Merchant Purchases, etc...) The purpose of the fee is to compensate the cardholder's bank for the period between settlement (payment) to the merchant's acquiring bank for the cardholder purchases and the collection of purchased amounts from the billing of the cardholder.

Additionally, other operating costs incurred by the cardholder's bank are also considered in the interchange fee. Visa, MasterCard and Discover determine and regularly adjust the fee. There are different sets of interchange fees for MasterCard, Visa and Discover transactions.



CARD BRANDS INTERCHANGE PROCESS

For example, if a purchase amount is $100 and the interchange fee is 1.50% + $0.07 per transaction, the amount of the interchange fee is calculated as follows:

$100 x 1.50% = $1.50 + $.07 = $1.57 (Interchange Fee)

The merchant's acquiring bank pays the interchange fee to the cardholder's bank through the respective Visa, MasterCard and Discover settlement systems.

The qualification for each interchange program varies based on specific criteria such as the merchant's industry (i.e., Restaurant), how the transaction is accepted (i.e., card is swiped or dipped), how long the transaction is accepted and then settled, etc.

1.1 Merchant Category Codes (MCC)

Visa, MasterCard and Discover have designated Merchant Category Codes (MCC) that will accommodate the acceptance of card products. An MCC is a four digit number that is assigned to a merchant based on the merchant's primary business. In addition, some MCCs identify a specific merchant or type of transaction. When an accurate MCC is assigned, Visa, MasterCard and Discover are able to analyze merchant sales, performance, assess levels of risk, and develop programs that are useful to members, merchants, and cardholders. The same MCC must be in authorization and settlement.

1.2 Point-of-Sale (POS) Entry Mode

The following are the entry mode values and descriptions:

Value	Description
00	Entry mode unknown
01	Manual key entry
02	Magnetic stripe read- Track Data was not complete
05	Chip read - data reliable
06	Magnetic stripe read- Track Data 1 read
07	PAN auto-entry via contactless chip. Contactless Chip transaction using Visa Smart Card, MasterCard chip, or Discover Electronic Commerce
09	PAN entry via electronic commerce, including remote chip. It would be used only when EMV Chip data (DE 55) is sent
79	PAN entry via electronic commerce, including remote chip. It would be used only when EMV Chip data (DE 55) is sent.
80	Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, the terminal defaulted to the magnetic stripe-read PAN
81	PAN entry via electronic commerce, including chip
85	Chip card at chip-capable terminal was unable to process transaction using data on the chip; terminal read the magnetic stripe-read PAN
90	PAN auto-entry via magnetic stripe - the full track, track 1 & 2 read (Visa and MasterCard); Voice Authorization (Discover)
91	PAN auto-entry via contactless magnetic stripe (Visa and MasterCard); Voice Response Unit(Discover)
95	Chip card read - data is unreliable (Visa only)

1.3 Timeliness

Timeliness is calculated as the number of days transpiring between the sale date and the processing date

1.3.1 Visa and MasterCard Timeliness

The following are excluded when calculating clearing timeliness:

- Transaction date
- Central Processing Date
- Sundays
- US Federal Holidays

1.3.2 Discover Timeliness

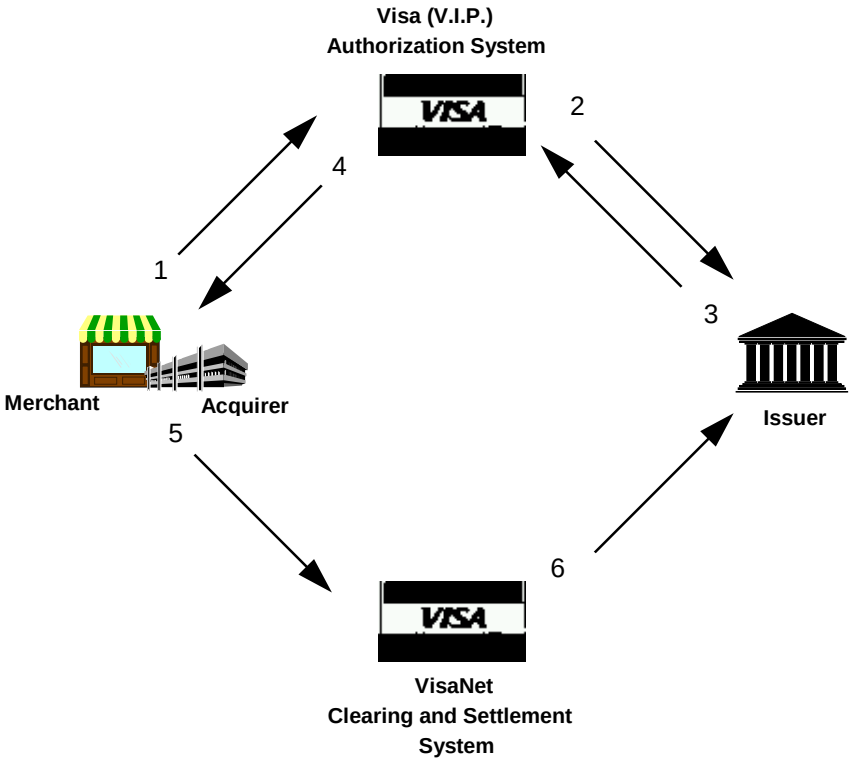
The following are excluded when calculating clearing timeliness

- Transaction date
- Sundays
- US Federal Holidays

1.3.3 American Express OptBlue Timeliness

American Express does not consider timeliness as part of pricing qualification for OptBlue.

2 Visa Interchange Overview



1. An authorization request is initiated at the point-of-sale. The Acquirer includes an Authorization Characteristics Indicator (ACI) within the authorization message before routing it to Visa. The presence of the ACI means that the transaction is being submitted as a Custom Payment Service (CPS) transaction, causing special edits and processing to be invoked at Visa.

2. The Visa V.I.P. Authorization System edits the content of the authorization message to ensure that the required information is present. If the requirements have been met, the V.I.P. system:
   - Assigns a unique Transaction Identifier to the message
   - Replaces the value in the ACI to reflect the characteristics of the transaction
   - Forwards the transaction to the Issuer.

3. The Issuer sends an authorization response to Visa and logs the authorization message, including the Transaction Identifier.

4. Visa matches the response with the authorization request. On an approved authorization response, the V.I.P. System computes a Validation Code and assigns it to the transaction. Visa forwards the response, including the Transaction Identifier, ACI, and Validation Code, to the Acquirer.

5. The Acquirer submits a clearing message to Visa Base II with a Requested Payment Service value, which specifies the CPS desired. The clearing transaction also contains the ACI, the Transaction Identifier, and Validation Code. Base II validates that the key authorization fields in the clearing transaction match those used in the authorization message. Edits are applied to ensure the transaction qualifies for the requested payment service and a Chargeback Rights Indicator is set to identify the set of chargeback rights applicable to the transaction.

6. The transaction is then forwarded to the Issuer with the ACI, Transaction Identifier, Validation Code, Requested Payment Service, and Chargeback Rights indicator. The Issuer uses the Transaction Identifier to match the clearing transaction to the authorization.

2.1 Card Verification Value (CVV)

Card Verification Value (CVV) is an enhanced security feature of the magnetic stripe. This is a unique check value, which is encoded for the purposes of validating the card information during the authorization process. At the time of authorization, transactions which include a POS entry mode of 90 (swiped) are verified by the issuer to contain full unaltered track information and to validate the CVV code encrypted in the stripe. If the data fails this check, a CVV failure notice will be generated by Visa.

2.2 Card Verification Value 2 (CVV2)

CVV2 is a card verification tool designed to reduce fraud losses when the card is not present or when the card cannot be swiped. Visa requires Issuers to print the CVV2 value on the back of all Visa credit, debit and prepaid cards.

- CVV2 is optional for merchants
- Participating merchants must manually enter the CVV2 values.
- All CVV2 participants (issuers, acquirers, and merchants) must be prepared to send and receive the information.

Visa has implemented requirements forbidding merchants and service providers to retain or store Card Verification Value 2 (CVV2) data subsequent to the authorization of a transaction. Fines may be assessed for failure to comply.

2.3 Visa Card Products

2.3.1 Consumer Card Products

Visa provides consumers with methods to pay for goods and services. Visa consumer card products offer convenience, security, reliability, and access. These products service both electronic commerce (e-commerce) and card usage at the point of sale (POS) or at automated teller machines (ATMs). Visa consumer credit products include:

- Visa Classic
- Visa Gold
- Visa Platinum
- Visa Signature
- Visa Signature Preferred
- Visa Infinite
- Smart Visa
- Co-Branded and Affinity Cards
- Visa Secured

2.3.2 Consumer Debit Products

The Visa consumer debit products enable consumers to purchase goods and services without having to carry cash, checks, or credit cards. Visa debit cards include:

- Visa Classic
- Visa Electron
- Visa Flag
- Visa Gold
- Visa Platinum
- V PAY

2.3.3 Debit and Prepaid Cards

The Visa consumer debit and prepaid products enable consumers to purchase goods and services without having to carry cash, checks, or credit cards. Visa debit and prepaid cards include:

- Visa Payroll Card
- Visa Healthcare Reimbursement Card
- Visa Gift Card
- Visa Buxx

2.3.4 Commercial Solutions

Visa commercial solutions enable businesses to purchase goods and services and track expenses. Visa business cards serve small businesses with up to $25 million in annual revenues and with fewer than 100 employees. Visa's suite of commercial payment cards include:

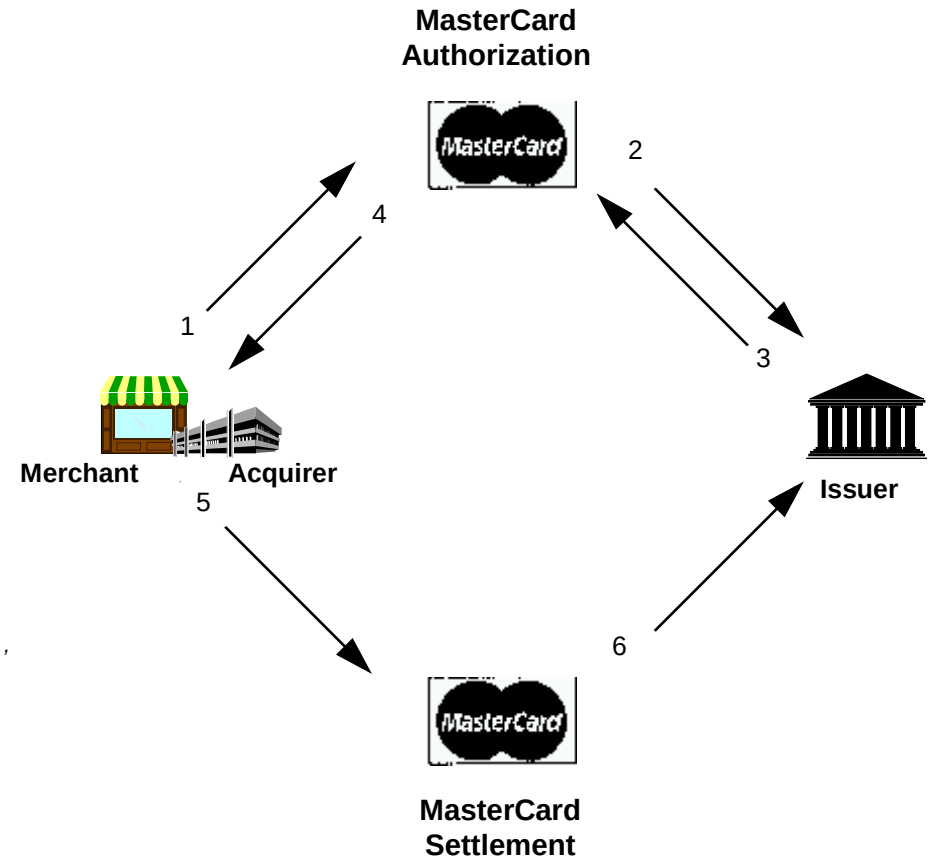
- Visa Commercial
- Visa Corporate
- Visa Purchasing
- Visa Fleet

2.3.5 Business Suite Products

Visa provides payment products that help entrepreneurs run a successful business. Visa business cards include:

- Visa Business Credit Card
- Visa Business Check Card
- Smart Visa Business Card
- Visa Business Line of Credit Card

3 MasterCard Interchange Program



1. An authorization request is initiated at the point-of-sale. The Acquirer routes the authorization request to MasterCard's Banknet Authorization System.

2. The Banknet Authorization System edits the message to ensure that the required information is present. If the requirements have been met, the Banknet Authorization System forwards the transaction to the Issuer.

3. The Issuer sends an authorization response to MasterCard and logs the authorization message.

4. MasterCard matches the response with the authorization request. On an approved authorization response, the Banknet Authorization System creates a Banknet Reference ID and assigns it to the transaction. MasterCard forwards the response, including the Banknet Reference ID and Date, to the Acquirer.

5. The Acquirer submits a clearing message to the MasterCard Settlement System with a requested interchange rate designator. The clearing transaction also contains the Banknet Reference ID, Banknet Date, and MCC code used in the authorization. MasterCard Interchange Compliance edits validate that the key authorization fields in the clearing transaction match those used in the authorization message by using the cardholder number, MCC, authorization code, and acquiring ICA to retrieve the original authorization data from the MasterCard history database. Edits are applied to ensure the transaction qualifies for the requested interchange rate.

6. The transaction is then forwarded to the Issuer.

3.1 Card Validation Code (CVC)

The intent of this program is to reduce fraudulent transactions by verifying the value of the Card Validation Code (CVC). This is done as part of the authorization process.

In many instances, if the issuer is unable to verify the information, they will generate either a referral or decline message. This may also prompt a CVC failure notice to be generated by MasterCard. MasterCard requires that either the issues be corrected or the merchant be disqualified. If the problem cannot be resolved, any resulting rate adjustments or counterfeit chargebacks become the client's responsibility.

3.2 Card Validation Code (CVC2)

CVC2 is a three-digit code algorithmically derived by the issuer and indent-printed on the signature panel to the right of the account number. CVC2 is one of several card authentication methods currently used by MasterCard to combat fraud. The use of CVC2 deters fraudulent use of an account number for non-face-to-face transactions or when the card cannot be swiped.

MasterCard has implemented requirements forbidding Merchants and Merchant Service Providers to store CVC2 data in any manner or for any purpose. Penalties may be imposed for failure to adhere to the CVC2 data use and safeguarding rules.

3.3 MasterCard Card Products

3.3.1 Consumer Card Products

MasterCard consumer cards include:

- MasterCard Standard Card
- Gold MasterCard Card
- Platinum MasterCard Card
- World, World Elite, and High Value MasterCard Cards
- MasterCard Unembossed Card
- MasterCard Flex Products

3.3.2 MasterCard Debit Card

A MasterCard debit card allows cardholders to make purchases using funds from their demand deposit or other asset account. A PIN is not required for such transactions.

3.3.3 MasterCard Rewards Card

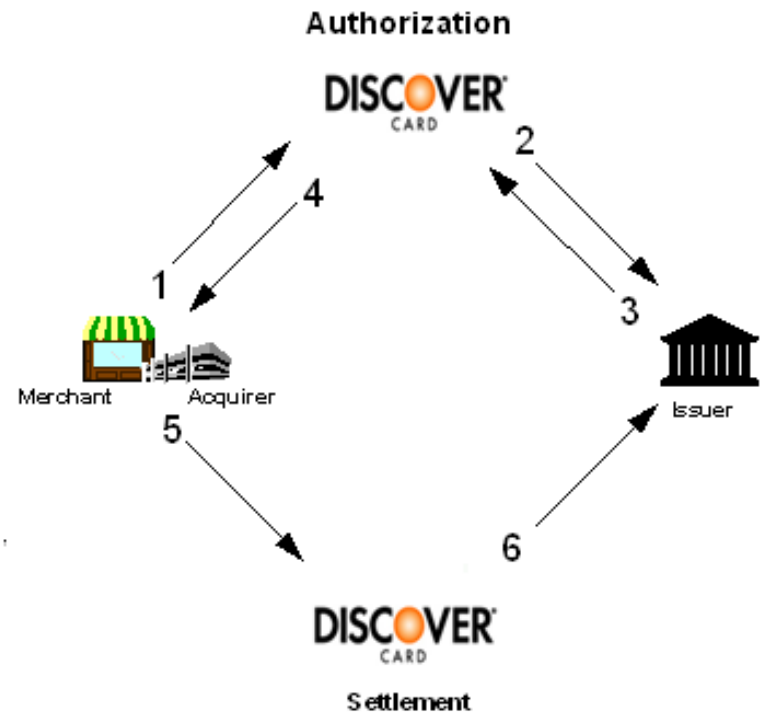
The MasterCard rewards program offers a suite of cardholder benefits provided directly from MasterCard such as travel protection, extended warranties, points, miles or cash back distributed by individual card issuers.

3.3.4 **Commercial Card Products**

The suite of MasterCard Corporate Payment Solutions offers a range of card programs for small businesses, corporations, universities, and the public sector. MasterCard commercial cards include:

- MasterCard Corporate Card
- MasterCard Corporate Executive Card
- MasterCard Business Card
- MasterCard Executive Business Card
- MasterCard Small Business Multi Card
- MasterCard Purchasing Card
- Fleet Card
- Corporate Fleet Card
- World, World Elite, and High Value Commercial Card Products
- Electronic Payment Account
- MasterCard Corporate Meeting Card

4 Discover Interchange Overview



1. An authorization request is initiated at the point-of-sale. The Merchant/Acquirer routes the authorization request to the Discover Network.

2. The Discover Network receives the message and routes to the Issuer.

3. The Issuer sends an authorization response to the Discover Network and logs the authorization message.

4. Discover Network matches the response with the authorization request.

5. Discover Network routes the 0110 Authorization Response to the Merchant/Acquirer.

6. The Acquirer submits a clearing message to the Discover Network Settlement with the requested Acquirer Interchange Program Code. The clearing transaction also contains the System Trace Audit Number, Local Time and Date of the Authorization Request, Authorization Response – Approved or Positive Authorization Code and Card number. Acquirer Interchange Program is assigned to the card transaction and is forwarded to the Issuer.

4.1 Card Identification Data (CID)

The CID is a three-digit number that follows the complete or truncated card number in the signature panel or in a separate box directly to the right of the signature panel on the back of a card.

4.2 Discover Card Products

4.2.1 Consumer Card Products

Discover Network supports the use of both standard and premium consumer credit cards that allow cardholders to access a specific line of credit on each cardholder's card account. Discover consumer cards include:

- Core Credit Cards
- Premium Credit Cards
- Premium Plus Credit Cards
- Rewards Credit Cards

4.2.2 Debit Cards

Discover Network supports the use of consumer debit cards that allow cardholders to make purchases by using a card to access funds from their demand deposit or other asset account. A personal identification number (PIN) is not required for such transactions.

4.2.3 Prepaid Cards

Discover Network supports the use of consumer prepaid cards (single use or reloadable) that allow Cardholders to spend up to the amount funded on the card or card account. Consumer prepaid cards are treated the same as consumer debit cards.

4.2.4 Commercial Card Products

Discover Network supports the use of business/corporate commercial credit cards targeted at cardholders expected to make purchases primarily for business purposes and that have spending patterns consistent with commercial use. Discover commercial cards include:

- Business/Corporate Credit Cards
- Business Debit Cards

5 American Express OptBlue Overview

The American Express OnePoint Program, referred to alternately as OnePoint or the Program, comprises an integrated service model designed to increase Card acceptance among the merchant population, located in the United States, but not Puerto Rico, the U.S. Virgin Islands, or any other U.S. territories or possessions.

Acquirer Interchange is assessed to each Card Transaction based on the Acquirer Interchange Program for which the particular Card Transaction qualifies. Below is the transactions cycle

5.1 American Express Card Products

5.1.1 Consumer Cards

American Express consumer cards include:

- Flexible Payment Cards
  - Earnings Card from Costco Blue Card
  - Blue Sky Card
  - Blue Cash Card
  - Clear Card
  - True

- Premium Rewards Cards
  - Preferred Rewards Green Card
  - Preferred Rewards Gold Card
  - Premier Rewards Gold Card
  - Platinum Card

5.1.2 Prepaid Cards

A preloaded and reloadable debit card allowing cardholders to spend up to the amount funded on the card. A PIN is not required.

5.1.3 Corporate Cards

American Express corporate cards include:

- American Express Corporate Card
- American Express / Business ExtrAA Corporate Card
- American Express Corporate Purchasing

6 Card Brand Programs

6.1 Payment Card - No Signature Programs

Visa, MasterCard, and Discover No Signature Required Programs include most Merchant Category Codes (MCCs). These programs enhance the card present Point of Sale (POS) experience for both merchants and cardholders in connection with low ticket sales.

6.1.1 Visa Easy Payment Service

Visa's No Signature Required program is referred to as the Visa Easy Payment Service (VEPS) program. It is a global program that allows qualifying low value transactions at specific merchants to take place without a cardholder signature or PIN and without a receipt, unless requested by the cardholder.

Program Requirements

The following criteria must be met to qualify for VEPS:

- Must be a Visa or Visa Electron card
- Authorization must be obtained
- Transaction takes place at a qualified merchant MCC (see excluded MCCs)
- Transaction must be equal to or less than the applicable amount limit
  - $50 or less: Supermarket (MCC 5411) or Discount Store (MCC 5310)
  - $25 or less: All other eligible MCCs in an attended environment
  - $15 or less: Face-to-Face unattended transactions (Cardholder Activated Terminals)
  - Full, unaltered content of the magnetic stripe, or unaltered chip data, is read and transmitted in the message

The following transactions are not eligible for VEPS:

- Account Funding
- Cashback
- Chip fallback
- Dynamic Currency Conversion
- Manual cash
- Prepaid load
- Quasi-cash

Chargeback Protection

VEPS qualified transactions are protected against the following chargeback reason codes:

- 60 – Illegible Fulfillment
- 75 – Transaction Not Recognized
- 81 – Fraud-Card Present Environment

6.1.2 MasterCard Quick Payment Service

The Quick Payment Service (QPS) program is MasterCard's No Signature Required program. The MasterCard QPS Program exempts eligible merchants from requiring a cardholder signature for qualifying QPS transactions.

Program Requirements

The following criteria must be met to qualify for QPS:

- MasterCard transaction
- Authorization must be obtained
- Face-to-Face transaction
- Full, unaltered content of the magnetic stripe, or unaltered chip data, is read and transmitted in the message
- Eligible merchant type (See excluded MCCs)
- Transaction amount must be equal to or less than $50 for all eligible MCCs

Chargeback Protection
QPS qualified transactions are protected against the following chargeback reason codes:
- 02 – Requested Item Illegible
- 37 – Fraudulent Transaction-No Authorization

6.1.3 Discover No Signature Program

Discover card present transactions of $50 or less (including applicable taxes, gratuity, and cash over amounts) are not subject to Dispute for failure to obtain the Cardholder's signature for qualifying transactions.

Program Requirements
The following criteria must be met to qualify for the No Signature Required program:
- Discover transaction
- Authorization must be obtained
- Face-to-Face transaction
- Full, unaltered content of the magnetic stripe, or unaltered chip data, is read and transmitted in the message
- Eligible merchant type (See excluded MCCs)
- Transaction amount must be equal to or less than $50

Chargeback Protection
Discover's No Signature Required Program offers protection from the following chargeback reason codes:
- 4584 – Missing Signatures
- 7010 – Swiped Card Transaction-No Cardholder Signature Obtained

6.1.4 American Express No Signature Required Program

The American Express No Signature Required program is designed to increase card acceptance and allow merchants to reduce the cardholder's time spent in line and at the POS, while increasing sales and customer satisfaction. Participating merchants may experience a reduction in back-office costs and chargebacks. As part of the program, eligible merchants are not required to obtain a signed sales draft at the point of sale for eligible transactions, but may provide a sales receipt to the consumer upon request.

Program Requirements
To qualify for the No Signature Program, both the merchant and each charge must meet the following criteria:
- Face-to-Face transactions with the appropriate transaction identifiers
- Transaction amounts $50 or less
- Magnetic stripe or key entered transaction
- Authorization must be obtained
- MCC Qualified - American Express must classify the merchant as an industry that accepts in-person charges, excluding the merchant establishments outlined below (U.S. Merchant locations only, does not include U.S. Territories) See excluded MCCs

The following merchant establishments are ineligible for the American Express No Signature Program:
- Merchants who do not conduct face-to-face transactions
- Prohibited merchants and/or transactions; refer to Chapter 10 "Risk Evaluation" and "Prohibited uses of the Card" within the Merchant Regulations for further details
- Merchants identified as "High Risk"
- Merchants placed in America Express "Fraud Full Recourse Program".

Note: Merchants are notified if considered High Risk or within American Express' Fraud Full Recourse Program

Chargeback Protection

American Express's No Signature Required Program offers the following chargeback protection:

- Chargebacks based solely on the establishment's failure to obtain the cardholder's signature at the point of sale
- American Express will block applicable chargebacks that meet the "No Signature Required" program criteria

NOTE: The No Signature Program does not provide protection against all chargebacks. Even if an establishment and charge qualify under the No Signature Program, the merchant may still be subject to chargebacks for reasons unrelated to its failure to obtain a signature from the cardholder at the point of sale.

6.1.5 MCCs Excluded from "No Signature Required Programs"

The following card present merchant types are excluded from the respective Visa, MasterCard, Discover, and American Express No Signature Required Programs.

MCC	Merchant Description	MasterCard	Visa	Discover	American Express
4829	Money Transfer Merchant	X	X	X	
5542	Fuel Dispenser Automated	X	X		X
6010	Member Financial Institution – Manual Cash Disbursement	X	X	X	
6011	Member Financial Institution – Automated Cash Disbursements	X	X	X	
6012	Financial Institution – Merchandise and Services		X		
6050	Quasi Cash – Member Financial Institution	X		X	
6051	Quasi Cash – Merchant	X		X	
6531	Payment Service Provider – Money transfer for a purchase			X	
6532	Payment Transaction – Member Financial Institution	X		X	
6533	Payment Transaction – Merchant	X		X	
6534	Money Transfer – Member Financial Institution	N/A		X	
6536	MasterCard MoneySend Intracountry	X	N/A	N/A	N/A
6537	MasterCard MoneySend Intracountry	X	N/A	N/A	N/A
7375	Information Retrieval Services				X
7393	Protective Agencies and Security Services				X
7995	Gambling Transactions	X	X	X	
9405	Intra-Government Purchases – Government Only	X	X		
9700	International Automated Referral Service	N/A	X	N/A	N/A
9701	Visa Credentaiai Server	N/A	X	N/A	N/A
9702	GCAS Emergency Services	N/A	X	N/A	N/A
9751	UK Petrol – Electronic Hot File	X	X		
9754	Gambling – Horse Racing, Dog Racing, State Lotteries	X	N/A	N/A	N/A
9950	Intra-company purchases	N/A	X	N/A	N/A

NOTE: The exclusion list does not include Card Not Present MCCs

6.2 Healthcare Auto-Substantiation

The IRS has revised the rules surrounding Flexible Spending Account (FSA), Healthcare Reimbursement Arrangement (HRA), and Health Savings Account (HSA) card acceptance.

All supermarkets, grocery stores, convenience stores, discount stores, and wholesale clubs that do not have a merchant category code (MCC) related to health care are deemed as "other medical care provider" as per the IRS Notice 2003-43 with respect to debit card transactions. In addition, mail order vendors and web-based vendors that sell prescription drugs will also be deemed to be an "other medical care provider". After December 31, 2007, health FSA, HRA, or HSA debit cards may not be used at any store, vendor or merchant that does not have a health care related MCC unless they are a SIGIS member and have implemented an Inventory Information Approval System (IIAS).

IIAS allows a merchant to identify Qualified Healthcare Products (QHP) at the point of sale. An IIAS must be in place for the continued acceptance of FSA/HRA/HSA cards at non-medical merchants as of January 1, 2008 and for pharmacies effective June 30, 2009.

The IIAS must identify each QHP within the POS system, flag the items on the customer receipt, and subtotal the QHP amount including tax and discounts on each order purchased with an FSA/HRA/HSA card.

The following data must be present in the authorization message to identify purchases on FSA/HRA//HSA cards that were appropriately processed within an IIAS:

Field	Status	Description
IIAS Indicator	**Required**	Signifies that the transaction has been validated by the Merchant's IIAS
Authorization Amount*	**Required**	Total transaction amount
Total QHP Amount*	**Required**	Total amount of the Qualified Healthcare Products ▪ Includes all QHP (Over-the-counter, Rx, Vision, Clinic and Dental amounts)
Total Rx Amount*	Optional	Total amount of Prescriptions, used to gain access to Rx only purses ▪ This amount is included in the Total QHP amount
Total Vision /Optical Amount*	Optional (Visa Only)	Total amount of Vision Care Items ▪ This amount is included in the Total QHP amount
Total Dental Amount*	Optional (Visa Only)	Total amount of Dental Services ▪ This amount is included in the Total QHP amount
Total Clinic /Other Medical Amount*	Optional (Visa Only)	Total amount of Clinic/Other Medical Services ▪ This amount is included in the Total QHP amount
Partial Authorization Indicator	**Required**	Flag used to indicate if partial approvals will be accepted ▪ If not supported, the authorization request will either be approved for the full amount or declined ▪ Balances will not be returned on FSA/HRA cards
Visa MVV	**Required**	Merchant Verification Value is required in the authorization request. Acquirer must register with Visa.
MasterCard ID	**Required**	MasterCard Assigned ID is required in the authorization request. Acquirer must register with MasterCard.

* Amounts include tax and shipping less any discounts

The settlement record must include the IIAS Indicator to identify that the transaction is from a POS system that verified qualified healthcare products against an IIAS during the authorization process.

Note: The Visa IIAS Indicator is a value of 'M' in the Market Specific Data Indicator (MSDI). The MSDI is included in the validation code calculation. Therefore, if the MSDI is not the same value in the authorization and settlement message, the transaction will downgrade from the CPS incentive interchange programs.

Under the IRS ruling, FSA/HRA/HSA cards may be used at stores with the MCC for Drug Stores and Pharmacies. However, many stores with this code also sell a significant number of items which do not qualify as medical expenses. In order to curtail the ability to purchase non-medical items with such cards, the IRS has determined that it is appropriate to require similar substantiation rules for all stores that sell a significant number of items which do not qualify as medical expenses as per the IRS guidelines.

Accordingly, after June 30, 2009, health FSA, HRA, and HSA debit cards may not be used at stores with a Drug Store or Pharmacy MCC unless:

- The store participates in the inventory information approval system (IIAS)

OR

- On a store location by store location basis, 90 percent of the store's gross receipts during the prior taxable year consisted of items which qualify as expenses for medical care under IRS guidelines (including non-prescription medications or over the counter medication (OTC)).

A card may have access to more than one type of account balance, known as 'multiple purses'. A multi-purse card may include several balances such as: FSA/HRA/HSA balance, a RX only balance, Vision only balance, and/or a non-substantiation required balance such as a credit line or HSA.

Multi Purse Examples:

1. Cardholder Balances on specified cards:
   FSA = $50
   RX = $50
   Credit Line = $50

Transaction Examples:

a) Total Purchase = $100

   QHP = $80
   Rx = $50
   Non-QHP = $20

   Full approval - $30 from FSA Balance, $50 from Rx only balance, $20 from Credit Line.

b) Total Purchase = $150

   QHP = $75
   Rx = $50
   Non-QHP = $75

   Partial Approval Supported – $25 from FSA Balance, $50 from Rx only balance, $50 from Credit Line. Split-tender for $25 must be completed. If an alternative payment option is not available the Non-QHP items can be removed from the total purchase, up

to the amount of $25. If more than $25 or QHP are removed from the total then the new total will impact the QHP and/or the Rx amount, the authorization must be reversed and a new transaction must be created providing the new amounts.
Partial Approval Not Supported – Declined, alternative payment or a new transaction must be created with modified amounts.

c) Total Purchase = $125

QHP = $125
Rx = Not provided
Non-QHP = $0

Partial Approval Supported – Approval for $100, split-tender for $25 must be completed. If an alternative payment option is not available, items can be removed from the total purchase, up to the amount of $25. If more than $25 is removed from the total then the new total will impact the QHP amount, the authorization must be reversed and a new transaction must be created providing the new amounts.

Partial Approval Not Supported – Declined, alternative payment or a new transaction must be created with modified amounts.

Multi Purse Example:

2. Cardholder Balances:
FSA = $50
Credit Line = $50

Transaction Examples:

a) Total Purchase = $100

QHP = $80
Rx = $50
Non-QHP = $20

Full approval - $50 from FSA Balance, $50 from Credit Line

b) Total Purchase = $100

QHP = $25
Rx = $10
Non-QHP = $75

Partial Approval Supported – Approval for $75, split-tender for $25 must be completed. If an alternative payment option is not available and the new total will impact the QHP and/or the Rx amount, the authorization must be reversed and a new transaction must be created providing the new amounts.

Partial Approval Not Supported – Declined, alternative payment or a new transaction must be created with modified amounts.

6.2.2 Visa Transaction Control

SIGIS certified merchants processing Visa Auto-Substantiation Transactions are required to include their assigned Merchant Verification Value (MVV) in IIAS authorization requests. The MVV can be inserted by the merchant, its acquirer or Visa via the Merchant Central File Service (MCFS).

Visa will implement processing rules to ensure that only IIAS-certified merchants are able to originate Visa Healthcare Auto-Substantiation Authorization Request Messages.

- Visa will remove the healthcare data from Field 54 and change the Market Specific Data Indicator in Field 62.4 from a value of M to N, if the MVV in the auto-substantiation request message does not match with the MVV Table of IIAS-certified merchants, and forward a standard authorization request to the issuer/issuer processor.
- If, as indicated above, Visa removes the healthcare data from Field 54, the issuer will receive a Field 62.4 - Market Specific Data Indicator value of N in the authorization request and the acquirer will also receive a value of N in Field 62.4 in the authorization response.

6.2.3 Business Identification Number (BIN) designation

Visa Auto-Substantiation Transactions using the SIGIS standard will be allowed only for those card types designated by the issuer and recorded in Visa systems as FSA or HRA cards with the product code of J3. This designation is allowed only for programs where the issuer has FSA, HRA or multi-purse card programs. Other program types are not eligible for IIAS transaction processing under terms of the SIGIS license. Issuers are responsible for verifying the correct product code identification for their programs. Visa will inform acquirers through eligible BIN ranges in the Account Range Definition (ARDEF) file.

6.2.4 MasterCard Transaction Control

SIGIS certified merchants processing MasterCard Auto-Substantiation Transactions are required to include their assigned MasterCard Assigned ID (MAID) in IIAS authorization requests.

MasterCard will implement processing rules to ensure that only IIAS-certified merchants are able to originate MasterCard Healthcare Auto-Substantiation Authorization Request Messages.

- Acquirers and processors must provide the MasterCard Assigned ID for IIAS transactions when the Transaction Category Indicator contains the real-time substantiation value of a 3.
- MasterCard will change the Real-time Substantiation Indicator from a value of 3 to a value of 4, if the MAID in the auto-substantiation request message does not match with the MAID Table of IIAS-certified merchants. The value of 4 will indicate to issuers that the transaction was submitted as IIAS, but from a Non-IIAS certified merchant.

  Note: Acquirers and processors are responsible for certifying their merchants, as well as any subsequent follow up recertification or decertification, as deemed necessary and appropriate by the acquirer.

6.3 MasterCard SecureCode

SecureCode is MasterCard's global e-commerce security program for protecting confidential cardholder data over the Internet.

MasterCard's SecureCode uses MasterCard's Universal Cardholder Authentication Field (UCAF) to provide an enhanced payment guarantee to online merchants by presenting, collecting, and passing cardholder authentication information. Using hidden fields and a merchant plug-in application that is integrated with a merchant's Web pages, along with authentication information generated by issuers, MasterCard SecureCode provides explicit evidence of the cardholder's involvement in a transaction.

Definitions:
MasterCard Secure Payment Application (SPA) is an application used to secure e-commerce transactions and is used in conjunction with the UCAF data transport used to authenticate the cardholder during the transaction.

SPA defines the protocols, messages, message formats, and data requirements for an over-all issuer-centric remote security solution. SPA is licensed separately to vendors and members (issuers, cardholders) to work in conjunction with existing infrastructure, like wallets. It is used to authenticate remote cardholders during the transaction and secures remote payments.

MasterCard Universal Cardholder Authentication Field (UCAF) is a field to support a universal, multipurpose data transport infrastructure that MasterCard uses to communicate authentication information among the cardholder, merchant, issuer and acquirer communities. It offers a universal method of collecting cardholder authentication data via the merchant's plug-in software.

MasterCard Accountholder Verification Value (AVV) is a unique value that is generated by the issuer's SPA server for each online transaction and is passed to the merchant via the Universal Cardholder Authentication Field (UCAF), when the issuer participates in SecureCode. It is used to prove that the cardholder conducted and authorized an electronic commerce transaction.

Participants:
Cardholder participates by entering their password for the issuer to validate via the merchant's plug-in software when making a purchase.

Issuer participates by validating the cardholder's password, assigns a MasterCard AAV (Accountholder Authentication Value), and provides the value to the merchant.

Merchant participates in SecureCode, their plug-in software forwards the cardholder account number to MasterCard's card directory to identify the issuer. The issuer determines cardholder participation and initiates the authentication prompt for the cardholder to enter their unique password. The issuer performs authentication, and the merchant receives the MasterCard AAV and provides it in the authorization request.

MasterCard SecureCode protects online participating merchants as follows:
- Merchants are not liable for fraud resulting from the unauthorized use of cards for transactions with valid SecureCode data
- Fraud on a merchant's site is reduced
- Higher rate of authorization approval

There are two types of cardholder authentication definitions:
- Approved "Full" Authentication
  - Cardholder, issuer, and merchant all participate
  - Cardholder properly enters their password
  - Issuer validated the password

- Attempted Authentication
  - Merchant participates and the cardholder was not authenticated:
    - Issuer may or may not participate or
    - Cardholder does not participate or
    - Password is not entered or unable to be validated by the issuer

How the process works for an E-commerce transaction:

- After an activated cardholder enters payment information, the issuer's SecureCode window will be displayed prompting the cardholder for a password. The cardholder is now on the issuer's website and the authentication process begins.
- The participating issuer validates the password and calculates the MasterCard AVV (populated in the UCAF field)
- The cardholder is asked to confirm the merchant name and sales amount, this is equivalent to the cardholder signing a sales draft
- The issuer sends the UCAF authentication information to the merchant
- MasterCard logs the results in the Authentication Central Repository
- The merchant receives the UCAF authentication information from the issuer via the plug-in and proceeds with the transaction
- The merchant initiates the authorization request with the following information:
  - The UCAF authentication information as received from the issuer **and**
  - E-commerce Security Level Indicator-Security Protocol/Cardholder Authentication:
    21 - Channel encryption; cardholder certificate not used (this is a preferred value for MasterCard SecureCode)
    91 - No security protocol/Cardholder certificate not used

- UCAF Collection Status Indicator:
  - 1 - Merchant is able to collect UCAF data, but UCAF was not populated **or**
  - 2 - Merchant is able to collect UCAF data, and UCAF data is present

- The issuer receives and validates the MasterCard UCAF value and provides the authorization response

6.4 MasterPass

MasterPass is a Digital Wallet which provides a secure and convenient method for consumers to conduct e-commerce transactions. MasterPass enables ecommerce merchants to convert browsing customers into buyers by providing a fast, convenient, and secure checkout experience.

The following is a high-level process flow for MasterPass transactions:

1. Consumer clicks on the MasterPass button on the merchant web site, and is taken to the MasterPass sign-in page.
2. Consumer chooses the integrated digital wallet they want to use and the authentication is completed.
3. Consumer selects the desired payment card and shipping address.
4. MasterPass securely transfers the payment and shipping information to the merchant's web site confirmation page, where the checkout process is completed.
5. Consumer's payment information is submitted to the merchant's acquirer for processing.

6.5 Verified by Visa (VbV)

Verified by Visa is a product that allows password information to be used to confirm the identity of the cardholder during the e-commerce transaction. The merchant's plug-in software facilitates the password validation between the cardholder and the issuer during the online transaction. In addition to fraud prevention and interchange benefits, VbV provides participating ecommerce merchants with chargeback protection and/or liability shift based on certain authorization and settlement information.

Definitions:

Visa 3-D Secure

A Visa-approved Authentication Method that is the global authentication standard for Electronic Commerce Transactions and requires no significant change to existing payment infrastructure.

Visa Cardholder Authentication Verification Value (CAVV)
The CAVV is a cryptographic value (20 bytes) calculated by the issuer's Access Control Server (ACS) using the issuer's encryption key and related elements according to protocol. The CAVV value is unique to the cardholder and to the transaction that was authentication. The acquirer transfers the ACS data to this field when preparing the authorization request. Visa or the issuer verified the CAVV to ensure that the issuer's ACS authenticated the cardholder for the transaction and that its contents have not been altered.

Chargeback liability for a transaction can shift depending on issuer or merchant participation and the outcome of the validation (Non-Secure, Attempt, or Authentication)

Participants:
Cardholder- participates by entering their password for the issuer to validate via the merchant's plug in software when making a purchase.
Issuer- participates by validating the cardholder's password, assigns a Visa CAVV (Cardholder Authentication Verification Value) and provides the value to the merchant.

Merchant- participates by forwarding the cardholder account number to Visa's card directory to identify the issuer through their plug-in software. The issuer determines cardholder participation and initiates the authentication prompt for the cardholder to enter their unique password. The issuer performs authentication, and the merchant receives the Visa CAVV and provides it in the authorization request.

Verified by Visa protects online participating merchants as follows:
- Merchants are not liable for fraud resulting from the unauthorized use of cards for transactions with valid VbV data
- Fraud on a merchant's site is reduced
- Higher rate of authorization approval

There are two types of cardholder authentication definitions:
- Approved "Full" Authentication
  - Cardholder, issuer, and merchant all participate
  - Cardholder properly enters their password
  - Issuer validated the password

- Attempted Authentication
  - Merchant participates and the cardholder was not authenticated:
    - Issuer may or may not participate or
    - Cardholder does not participate or
    - Password is not entered or unable to be validated by the issuer

How the process works for an E-commerce transaction:
- After an activated cardholder enters payment information, the issuer's VbV window will be displayed prompting the cardholder for a password. The cardholder is now on the issuer's website and the authentication process begins.
- The participating issuer validates the password and calculates the Visa CAVV
- The issuer sends the CAVV information to the merchant
- Visa logs the results in the Authentication Central Repository
- The merchant receives the CAVV information from the issuer via the plug-in and proceeds with the transaction
  - The merchant initiates the authorization request with the following information:
    - The CAVV information as received from the issuer **and**
    - E-commerce Indicator :
      05- "Authenticated" (Secure electronic commerce transaction) **or**

06- "Attempt" (non-authenticated secure transaction, merchant attempted to authenticate the cardholder using 3-D Secure "aka VbV")

- The issuer receives and validates the Visa CAVV and provides the authorization response
- Visa also provides the merchant with a CAVV Results Code to identify the outcome of the CAVV validation; indicates who performed the authentication (Visa or issuer) and if the transaction was:
  - Non-Secure- acquirer and issuer do not participate in VbV
  - Attempt- issuer or cardholder do not participate in VbV
  - Authenticated- cardholder, acquirer, and issuer all participate in VbV and cardholder was verified by the issuer

6.6 Visa Checkout

Visa Checkout is a digital payment service designed to simplify the checkout experience using a secure, single sign-on across channels and devices using a customer's preferred payment method.

Benefits:

- Secure - Visa Checkout uses multiple layers of security, including fraud-monitoring systems and encrypted tokens using SHA256 hash algorithms to help keep payment information safe.
- Open - Visa Checkout accepts any major credit or debit card so customers can check-out easily and securely using the payment method they use today on your site.
- Simple - Integrating Visa Checkout is easy and requires only a few simple HTML and JavaScript tags

Visa Checkout integrates with the merchant's website. A standard integration follows these steps:

1. On the merchants cart page, the cardholder would select "Visa Checkout" as the payment method, which loads the Visa Checkout Payment Widget over the merchant's webpage served securely by Visa Checkout.
2. The cardholder is then prompted to sign in or create an account with Visa Checkout.
3. The cardholder reviews the payment information within the Visa Checkout Payment Widget and clicks the continue button.
4. Control of the order is returned to the merchant's website and the cardholder submits the order.

6.7 Contactless

Contactless is the ability to conduct a card transaction simply by waving or tapping a contactless enabled card or device such as a smart phone using Near Field Communication (NFC) at participating merchants with contactless readers. Contactless payment offers an alternative to more traditional payment methods such as magnetic stripe cards or cash. This technology is being leveraged to improve speed, convenience and security in the marketplace.

Contactless targets quick payment environments such as quick-service restaurants, gas stations, drug stores, supermarkets and movie theaters.

Visa Card-Level Results (Field 62.23)

Visa enhanced both the authorization and clearing applications to support specialized processing at the cardholder account level. Account Level management allow issuers to efficiently manage their customer's needs and to easily move a cardholder from one card product to another, Visa will support card-level product identification. This will enable U.S. Consumer Credit Card Issuers to define the appropriate card product at the card account level.

Visa provides the Product ID in the Card-Level Results field in authorization and requires the Product ID and a valid validation code in settlement to identify U.S. consumer credit and debit, commercial, and prepaid products properly.

Visa will also include the product results in the validation code algorithm. The validation code is used for message consistency by checking values from the authorization process with the values supplied by the acquirer processor in the clearing message.

- All U.S. acquirer processors are required to receive the product results in Field 62.23 - Card-Level Results in authorization responses

- All U.S. acquirer processors are required to provide the Product ID field and valid validation code in clearing (settlement) messages.

Transactions will not be eligible for a CPS program if the Validation Code received in authorization doesn't match what's presented during settlement and/or if the Product ID is not populated or is invalid in settlement.

6.8 Partial Authorization

Partial Authorization permits issuers to return an approval for a partial amount based on the cardholder's funds available with prepaid cards as an alternative to declining the transaction. Partial authorizations will create the need for a split tender transaction.

6.8.1 Authorization Process

- Merchant sends an authorization request
- Issuer must review the request to identify if a Partial Authorization Indicator is present
- When the Partial Authorization Indicator of "Y" (merchant participates in partial authorization) is present, the issuer will partially approve the transaction based on the remaining balance on the card account

6.8.2 Partial Authorization Fields:

The Issuer will provide the following transaction data for Partial Authorization processing

- A specific response code indicates to the Acquirer and merchant that the transaction was partially authorized
- Partial Approved Amount
- Original Amount provided in the authorization request

6.8.3 Automated Fuel Dispenser- Partial Authorization

Traditionally, issuers will only authorize a $1.00 status check if the funds are available to cover the maximum fuel dispensed amount. Transactions eligible for Partial Authorization will be authorized based on the amount available on the card and not for the maximum fuel dispensed amount limit.

Gas dispensed can be less than the partial approved amount but requires an authorization reversal for the difference. The settlement amount cannot be submitted for an amount greater than the partial approved amount.

6.8.4 Partial Authorization Reversal Processing

Partial Authorization Reversal must be performed for transactions where the cardholder cannot provide additional funds to pay the remaining balance and the sale is canceled.

6.8.5 Partial Authorization Mandated

Visa

Visa requires MCC 5542 Automated Fuel Dispensers to support Partial Authorization.

MasterCard

MasterCard will require partial approval, real-time reversal of a partial approval and balance return with purchase based on the effective dates and MCCs below.

Effective Date	MCC	Description
May 1, 2010	5310	Discount Stores
	5311	Department Stores
	5411	Grocery Stores Supermarkets
	5499	Miscellaneous Food Stores-Convenience Stores, Markets, Specialty Stores and Vending Machines
	5541	Service Stations (with or without Ancillary Services)
	5542	Fuel Dispenser, Automated
	5812	Eating Places, Restaurants
	5814	Fast Food Restaurants
	5912	Drug Stores, Pharmacies
	5942	Book Stores
	5943	Office, School Supply and Stationery Stores
	7829	Motion Picture-Video Tape Production-Distribution
	7832	Motion Picture Theaters
	7841	Video Entertainment Rental Stores
	8011	Doctors—Not elsewhere classified
	8021	Dentists, Orthodontists
	8099	Health Practitioners, Medical Services-Not elsewhere classified
	5111	Stationery, Office Supplies
	5200	Home Supply Warehouse Stores
	5331	Variety Stores
	5399	Miscellaneous General Merchandise Stores
	5732	Electronic Sales
	5734	Computer Software Stores
	5735	Record Shops
	5921	Package Stores, Beer, Wine and Liquor
	5941	Sporting Goods Stores
	5999	Miscellaneous and Specialty retail Stores
	8041	Chiropractors
	8042	Optometrists, Ophthalmologists
	8043	Opticians, Optical Goods and Eyeglasses
	4812	Telecommunication Equipment Including Telephone Sales
	4814	Telecommunication Services
	5300	Wholesale Clubs
	5964	Direct Marketing-Catalog Merchants
	5965	Direct Marketing –Combination Catalog-Retail Merchants
	5966	Direct Marketing-Outbound Telemarketing Merchants
	5967	Direct Marketing-Inbound Telemarketing Merchants
	5969	Direct Marketing-Other Direct Marketers-Not elsewhere classified
	8062	Hospitals

Effective Date	MCC	Description
November1, 2010	4111	Transportation-Suburban and Local Passenger, including Ferries
	4816	Computer Network/Information Services
	4899	Cable, Satellite, and Other Pay Television and Radio Services
	7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers
	7997	Clubs-country Membership
	7999	Recreation Services-not elsewhere classified
May 1, 2011	8999	Professional Services-not elsewhere classified
	9399	Government Services-not elsewhere classified

All deployed stand-alone terminals on or after May 1, 2010 must support Partial Authorizations for MasterCard transactions. For the purposes of this section, stand-alone terminals are terminals that are not integrated into a merchant's POS system (e.g., cash register), such that the transaction amount must be manually entered in the terminal.

6.8.6 Discover

All merchants processing card present transactions are required to support partial authorization and reversal of a partial approval as of April 16, 2010. Partial authorizations for card not present transactions are optional, but recommended.

6.8.7 American Express

All merchant types are required to support partial authorization or partial authorization with balance return. Reversal of a partial approval is not mandated. Merchants should contact American Express for specific mandated dates.

Optional Support- Partial Approvals and Balance Return with Purchase

Support of partial approvals on all Debit MasterCard and Maestro cards and support of account balance responses on Prepaid Debit MasterCard and Maestro cards is optional for batch-authorized transactions:

- Electronic commerce
- Mail order and phone order
- Recurring payment

In addition, MasterCard & Maestro have provided an exception for MCC 5542 Automated Fuel Dispenser merchants. This merchant type does not need to support account balance responses.

6.9 EMV

EMV, which stands for Europay, MasterCard, and Visa, is a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

EMVCo was form to manage the EMV Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV Specifications based on contact chip, contactless chip, common payment application (CPA), card personalization, and tokenization.

6.9.1 **Visa EMV Mandate & Timeline**

Visa announced in August 2011 plans to accelerate the migration to contact chip and contactless EMV chip technology in the U.S. The adoption of chip technology will help prepare the U.S payment infrastructure for the arrival of Near Field Communication (NFC)-based mobile payments. Not only will chip technology accelerate mobile innovations, it will also enhance payment security through the use of dynamic authentication which will set the stage for Visa' counterfeit Liability Shift Policies. Visa will promote EMV chip technology in both contact and contactless for card present transactions across all markets.

Mandate	Effective Date	Description
Guide and Enforce Security Standards	August 2011	Visa developed a set of recommended practices for issuers, acquirers, merchants, processors and vendors while adopting and implementing chip technology programs in the U.S.
Tech Innovation Program (TIP)	October 2012	PCI validation relief for merchants that adopt dual interface terminals. This program will provide merchants with a waiver from the annual PCI validation exercise.
U.S. Acquirer Processors to support chip processing	April 1, 2013	Visa is requiring acquirer processors to support chip processing. Acquirers must certify to Visa for their ability to comply with this requirement
U.S. Third-Party ATM acquirer-processors and sub-processors to support chip	April 1, 2015	Visa is requiring U.S. third-party ATM acquirer-processors and sub-processors to support chip data by carrying and processing the additional data in chip transactions
Liability shift for credit and debit domestic cross border transactions.	October 1, 2015	Debit and Credit domestic and cross border counterfeit liability at all POS devices, excluding Automated Fuel Dispensers (AFD's). If a dual interface or a chip card is presented to a merchant that has not adopted a contact chip terminal liability for counterfeit fraud shifts to the merchant. EMV liability shift will be expanded to include all counterfeit magnetic-stripe fraud from EMV chip cards acquired at ATMs that have not been enabled for EMV contact chip acceptance in AP except for those in China, India, Japan and Thailand.
Liability shift for Automated Fuel Dispensers	October 1, 2017	The liability shift will include Automated Fuel Dispensers (AFD's). EMV liability shift will be expanded to include all counterfeit magnetic-stripe fraud from EMV chip cards acquired at ATMs that have not been enabled for EMV contact chip acceptance in China, India, Japan, Thailand and the U.S. Domestic transactions in China will remain excluded.

6.9.2 **MasterCard EMV Mandate & Timeline**

MasterCard announced in January 2012 its framework surrounding the payments industry liability shift from magnetic stripe to EMV technology.

Mandate	Effective Date	Description
MasterCard announcement	January 30, 2012	MasterCard announces their roadmap surrounding the payments industry liability shift regarding EMV technology.
Introduction of MasterCard PCI DSS Compliance Validation Exemption Program	October 1, 2012	Qualifying PCI Level 1 and 2 merchants located in the U S region become eligible for revised PCI DSS compliance validation procedures in which the merchants are exempt from the requirement to annually validate compliance with PCI DSS if set requirements are satisfied.
U.S Region acquirers must be capable of processing MasterCard contact and contactless chip transactions	April 19, 2013	Acquirers must support the transmission of contact chip transactions and contactless chip transactions. In addition, the PayPass reader of any POS terminal located in the U.S. region must support PayPass version 3.0 or later.
Potential Reduction of Calculated Account Data Compromise Operational Reimbursement and Fraud Recovery	October 1, 2013	For Account Data Compromise (ADC) Event cases opened by MasterCard on or after October 1, 2013 merchants may be eligible for a reduction in calculated Account Data Compromise (ADC) operational reimbursement (OR) and fraud recovery (FR) in the event of an Account Data Compromise (ADC) event.
Additional Potential Reduction of Calculated Account Data Compromise Operational Reimbursement and Fraud Recovery.	October 1, 2015	For Account Data Compromises (ADC) event cases opened by MasterCard on or after October 1, 2015 merchants that experience an Account Data Compromise (ADC) event may qualify for additional calculation enhancements for operational reimbursement (OR) and fraud recovery (FR). If the compromised entity is a merchant and MasterCard determines that the Merchant met all set requirements MasterCard will not assess for operational reimbursement (OR) and will apply a 100 percent deductible against the calculation of fraud recover (FR).
Chip and Chip/Pin liability shift Participation	October 1, 2015	U.S region acquirers may have second presentment rights when the issuer alleges counterfeit fraud and the acquirer can prove that the disputed transaction occurred at a hybrid POS terminal and involved a Chip Card.
Chip and Chip/Pin Liability shift for Automated Fuel Dispensers (AFD's)	October 1, 2017	Expansion of the second presentment rights to include Automated Fuel Dispensers (AFD's).

6.9.3 **Discover EMV Mandate & Timeline**

Discover announced March 15, 2012 it is implementing a 2013 EMV mandate for acquirers and direct-connect merchant in the U.S., Canada, and Mexico. Discover will include Diners Club, PULSE, and Discover card networks with this mandate.

Mandate	Effective Date	Description
Discover announces EMV mandate for U.S, Canada, and Mexico	March 15, 2012	Discover has aligned with the global industry mandates to support the transition towards EMV in the U.S.
Discover Authorization Interface	October 12, 2012	Discover will implement an indicator for partial chip card request messages from acquirers. In support of partial chip card acceptance. The partial chip indicator is used to notify issuers whether the chip card transaction was acquire with partial D-PAS capability.
Contactless Discovers EMV-compliant payment specification (D-PAS) Network Support Requirements	October 12, 2012	Discover will expand its chip card program to include a contactless EMV product. The requirements for this support will be released with the 12.2 program documents on April 13, 2012.
Support for Discovers EMV-compliant payment specification. (D-PAS)	April 19, 2013	Acquirers and Merchant operating in the U.S., Canada, and Mexico will be required to certify their ability to support EMV data however, Discovers EMV compliant payment specification (D-PAS) is not a requirement at this time.
Chip and Chip/Pin Liability shift Participation	October 1, 2015	Discover is introducing Fraud Liability Shift for Discover Network (in the U.S., Canada and Mexico) and PULSE (in the U.S.) at point-of-sale (POS) terminals. This Fraud Liability Shift policy will be a risk-based payments hierarchy that benefits the entity that leverages the highest level of available payments security.
Chip and Chip/Pin Liability shift for Automated Fuel Dispensers (AFD's)	October 1, 2017	Discover will institute Fraud Liability Shift for Discover Network (in the U.S., Canada and Mexico) and PULSE (in the U.S.) for Automated Fuel Dispensers (AFD's).

6.9.4 American Express EMV Mandate & Timeline

On June 29, 2012, American Express announced its network roadmap to advance EMV chip-based contact, contactless and mobile payments for all merchants, processors and issuers of American Express-branded cards in the U.S.

Mandate	Effective Date	Description
American Express announces EMV roadmap for U.S.	June 29, 2012	American Express announced its roadmap to advance EMV chip-based contact, contactless and mobile payments for all merchants, processors, and issuers.
Support for American Express EMV chip-based contact, contactless and mobile transactions.	April 2013	Processors must be able to support American Express EMV chip-based contact, contactless and mobile transactions.
Relief from PCI Data Security Standards (PCI) DSS Reporting requirements	October 2013	Merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if the merchant's point-of-sale acceptance locations, where 75% of their transaction occurs, are enabled to process American Express EMV chip-based contact and contactless transactions.
Fraud Liability Shift (FLS) policy	October 2015	American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology (excluding fuel merchants).
Fraud Liability Shift (FLS) for Fuel merchants	October 2017	American Express will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.

6.10 Tokenization

Tokenization is the process of replacing a traditional card account number with a pseudo credit card number. The tokenized account number will be used for transaction processing instead of the actual PAN. The Payment Token Standard is managed by EMVCo.

6.10.1 Tokenization Use Cases

EMVCo has introduced four (4) use cases in support of the Tokenization Standard as follows:

6.10.1.1 Mobile NFC at Point of Sale

In this use case, a Payment Token is stored within an NFC-enabled mobile device or alternatively in a remote server and delivered just-in-time to the device. Token Provisioning can be accomplished by the Token Requestor interfacing with the Token Service Provider. When a transaction is initiated, the mobile device and / or remote server will generate a contactless transaction including the Payment Token, Token Expiration Date, Token Cryptogram, and other chip data elements, and pass the transaction to the Merchant's point of sale terminal via the NFC interface.

6.10.1.2 Mobile / Digital Wallet E-Commerce (In App Purchases)

This use case refers to scenarios where a Cardholder initiates payment to an e-commerce site using a mobile / digital wallet to transfer payment and other order information. The wallets may be operated by Card Issuers, Payment Networks, or third parties; and the digital wallet operator will likely be the Token Requestor. When a Cardholder initiates payment at an ecommerce Merchant that supports the wallet, the wallet will pass a Payment Token in lieu of the PAN along with additional Payment Token-related fields through the wallet API to the Merchant. Merchants will initiate authorizations using the Payment Token and accompanying Token Expiration Date carried within the existing fields for PAN and PAN Expiration Date.

6.10.1.3 Card-On-File E-Commerce

This use case refers to scenarios where an e-commerce Merchant with payment card data on file in a database seeks to remove the underlying security exposure of storing card data by replacing the PANs with Payment Tokens. In such scenarios, these Merchants will likely be the a Token Requestor. Once Payment Tokens are returned to these Card-on-file Merchants, all subsequent ecommerce transactions that are processed will use the Payment Token and the Token Expiration Date in lieu of the PAN and PAN Expiration Date fields.

6.10.1.4 Scan at Point of Sale

The mobile quick response code (QR) at point of sale use case refers to the enablement of mobile devices to initiate QR codebased payments at Merchant locations that can accept this form of payment at the point of sale. In this use case, an application in the mobile device generates a dynamic QR code every time a payment is initiated in a secure manner. When a transaction is initiated, the mobile device will generate a transaction including the Payment Token, Token Expiration Date, and Token Cryptogram elements, and any other data from the QR code, and pass it to the Merchant's point of sale terminal.