Merchant Network Updates
Fall 2021

worldpay from FIS

We are committed to working closely with you to achieve your business goals. As a part of this commitment, we carefully monitor network changes and summarize them for your convenience. This communication serves as a summary of information from American Express, Discover® POINT OF SALE Network, Mastercard® Worldwide and Visa® U.S.A. outlining changes to operating rules and regulations, interchange rates, compliance of network mandates, and other industry updates that may impact your business.

Except where otherwise noted, the changes described in the articles will be effective October 15, 2021 central processing date of October 16, 2021**.** Please contact your Relationship Manager with any questions you may have regarding any of the information contained in this network updates newsletter.

ALL BRANDS

[UPDATE] Return Authorization Requirements, All Brands — CP/CNP/eComm

SEPTEMBER 2021 UPDATE

Core Platform

Worldpay from FIS has been sending credit/refund transactions to Visa and Discover for authorization for all core merchants since February 2021. Mastercard will be enabled for return authorization at a future date to be determined. Our Reauthorization product was also updated to support authorizations for returns.

eComm/VAP Platform

Visa credit/refund transactions from customers utilizing our global eComm/VAP platform continue to be sent for authorization. Mastercard and Discover will be enabled for return authorization at a future date to be determined.

Network Fees and Returns (Update)

Visa has announced a delay in the effective date for the Misuse of Authorization and Zero Floor fees for refund transactions from October 1, 2021 until July 1, 2022.

- **Visa:** Zero Floor Limit fee of $0.20 will apply to return transactions not authorized. Misuse Fee of $0.09 will apply to return transactions not reversed or settled within prescribed timeframes.
- **Discover:** Authorization fee of $0.0190 will apply to credit/refund authorization requests.
- **Mastercard:** The NABU fee will **not** apply to return transactions submitted for authorization.

Brand	Mandated Effective Dates	Chargebacks	Fees
Visa	**October 19, 2019 -** U.S., Canada, LAC **July 2020 –** AP, CEMEA **April 2022 –** Europe, UK, Republic of Ireland	July 18, 2020 (*excluding Europe*)	**July 1, 2022**
Mastercard	**TBD** - Optional for acquirers and merchants	TBD	N/A
Discover	**October 15, 2021**	July 17, 2020	Feb 1, 2021

[UPDATE] Return Authorization Requirements, All Brands (cont.) CP/CNP/eComm

Visa Stand In Processing for Invalid Authorization Decline Responses

Issuers are limited to responding with the list of valid decline response codes below. Merchants may continue to see decline response codes other than those listed below if the issuer does not permit Visa to stand in or the transaction is excluded from STIP.

Valid Decline Response Codes		
Status	**Response Code**	**Description**
Existing	03	Invalid Merchant
Existing	13	Invalid Amount
Existing	14	Invalid Account Number
New	46	Closed Account
Existing	57	Transaction Not Permitted to Cardholder
Existing	59	Suspected Fraud
Existing	93	Transaction Cannot be Completed – Violation of Law

Visa will decline refund authorizations for non-reloadable Visa prepaid cards with a decline response code of 57 "Transaction Not Permitted to Cardholder".

Exceptions

Visa will not apply the STIP process for the following:

- Transactions originating from the AP region
- Transactions from MCC 4829, 6012, 6051,6540 and 7995

Reminders

- Merchants should be prepared to handle receiving declines on return transactions and develop procedures for how to handle both in store and customer not present scenarios.
- Merchants are reminded Visa *response code '85' is a valid approval response* and to support this value accordingly.
- Processing code of 20 should be used on return authorizations for Visa, Mastercard and Discover.
- Merchants should include the expiration date in return authorization messages for all card types to prevent issuer decline.
- The expiration date should also be included when processing return transactions through Virtual Terminal within iQ.
- Refund transactions may be processed onto a different account (same brand) if the original account is no longer available or valid (expired, lost/stolen, discarded prepaid card) or the authorization request for the refund is declined by the issuer.
- Visa transactions that originated as Quasi Cash or Account Funding cannot submit credit refunds.
- Airlines (MCCs 3000–3350 and 4511) are excluded from the requirements.

[UPDATE] Return Authorization Requirements, All Brands (cont.) CP/CNP/eComm

Transaction ID in Credit Refund Authorizations

Visa will permit merchants to send the Transaction ID from the sale in the authorization request message for an associated credit refund. When Visa receives the Transaction ID in the authorization request, they will respond with the Transaction ID in the authorization response for the merchant to submit the same value in settlement.

This functionality is supported on both the VAP and Core platforms

- eComm/VAP auto fills tran ID in all credit refund authorizations on behalf of merchants.
- Core merchants can send in the tran id in credit/refund authorizations.

If an issuer initiates a chargeback for any reason code such as credit not processed, Visa's chargeback system will look at the credit/refund settlement message Transaction ID and will attempt to locate the corresponding sale with the same Transaction ID. If a match is found Visa will block the chargeback. Including the Transaction ID from the related sale transaction is optional for merchants.

EMV

[UPDATE] Expiring Certificate Authority Public (CAP) Keys CP

The Program: On an annual basis, EMVCo reviews the keys and makes recommendations on the expected life span (on a rolling 10-year projection window) of the different key lengths. Once EMVCo determines a key length is beginning to approach a point where it may become vulnerable, they will set the key's expiration date.

The Change: The following are the active CAP key lengths and their expiration or projected lifespan dates:

- UnionPay has announced the expiration date for their 1152-bit key is 12/31/2021
  - Per UnionPay rules, merchants must not remove the 1152-bit key for UnionPay until the expiration above
- 1408-bit keys have an expiry date of 12/31/2024
- 1984-bit keys have an anticipated expiry date of 12/31/2030
- Mastercard is extending the expiration date of their 1984-bit Payment System public keys from December 31, 2030, to December 31, 2031

The Impact: Once a key expires, it must be removed from the terminal within six months.

- Merchants and their solutions providers are advised to begin the process of removing of these keys
- Merchants are also reminded that because expiration dates can change, they should not be stored on terminals.

[REMINDER] Mastercard Updates EMV Data Integrity Edits CP

The Program: Data Element 55 provides valuable information to issuers including the application identifier/dedicated file name on the card, also referred to as Tag 84. The application identifier/dedicated file name, Tag 84, is used in the authorization message to verify the chip card and processing results, customer verifications, and offline/online authorization.

The Change: Mastercard has announced monitoring updates to three existing Data Integrity missing EMV tag edits which will now include Data Element (DE) 55 Tag 84 (Dedicated File Name) effective June 1, 2021.

The Impact and Timing:

- ✓ Mastercard monitoring for DE 55, tag value 84 begins — June 1, 2021
- ✓ Non-compliance notifications begin — July 1, 2021
- ✓ Comply by date — September 1, 2021
- • Assessments for non-compliance begin — October 31, 2021

[REMINDER] Discover Introduces D-PAS Connect and Outlines D-PAS Sunset Dates CP

The Program: Businesses of all sizes utilize D-Payment Application Specification (D-PAS) to process contact, contactless, and mobile transactions. D-PAS is used globally by Discover® Card, third-party debit cards issued through PULSE®, Diners Club International® franchises, and Network Alliance Partners.

The Change: Discover is introducing a more advanced solution, D-PAS Connect, that conforms to current EMV specifications and brings an enhanced level of security and utility to chip cards and payment devices. Discover Global Network encourages merchants and processors to begin their migration plans from D-PAS to D-PAS Connect using the established dates below:

Level 2 DFS Type Approvals for New and Existing Chip Products and Terminal Kernels	D-PAS v1 Sunset Date
All New Product Certifications	**December 31, 2021**
All Existing Product Renewals	December 31, 2023

All new product certifications and existing product renewals will be available to only D-PAS Connect products after the dates provided in the table above.

- New product certifications of D-PAS v1 chip products and terminal kernels completed after December 31, 2020 but on or before December 31, 2021 will be valid for three (3) years from the initial letter of approval with no option for renewal.
- Existing product certifications of D-PAS v1 chip products and terminal kernels expiring on or before December 31, 2023, can only be renewed for one (1) year.

[REMINDER] American Express Announces Sunset Dates for EMV POS Terminal Specifications

CP

The Change: American Express has announced the following requirements and sunset dates for EMV POS terminal specs:

Expresspay Version	No New Level 2 certification after	No New Level 3 Certification After	All terminals replaced with current Expresspay version by
3.0	Effective Immediately	December 31, 2020 or on devices with expired L2	**July 31, 2024**
3.1	February 10, 2020	August 10, 2023	**August 10, 2027**

Reminders:

- Level 2 is a component-based certification that focuses on the software interactions between the Card and terminal using the EMV Kernel.
- Level 3 certification interfaces with the payment application and specifications.

Certification and Important Dates

Merchants, Vendors and Third-Party Processors will need to manage existing, and certify new POS devices with Expresspay per the following requirements:

Requirement	Date
No new devices will be L3 certified utilizing Expresspay 3.0 kernel after the expiry of L2 kernel	✓ Immediate
No devices will be L3 certified utilizing Expresspay 3.0	✓ After December 31, 2020
All existing devices utilizing Expresspay 3.0 must be replaced with a valid and current Expresspay version	By July 31, 2024
No devices will be L2 certified utilizing Expresspay 3.1	✓ After February 10, 2020
No new devices will be L3 certified utilizing Expresspay 3.1	After August 10, 2023
All existing devices utilizing Expresspay 3.1 must be replaced with Expresspay 4.0.2 or newer	By August 10, 2027

Merchants and Third-Party Processors that are utilizing Expresspay 4.0.2 and are no longer supporting Expresspay magstripe mode are no longer required to certify for Expresspay magstripe mode.

American Express has published the Enhanced Expresspay Specification, Expresspay 4.0.3.

[REMINDER] Contactless Terminal Requirements: All Brands, All Regions CP

Merchants that support contactless transactions are reminded that contactless terminals must support EMV grade contactless technology as defined by region and effective date in the table below.

Failure to comply with the requirements to support EMV contactless technology may result in the decline of transactions by some networks. Merchants must work with hardware vendors to ensure that EMV contactless devices are properly configured as outlined by the brands.

United States / Canada

Brand	Effective Date	Terminal Type and Requirement
Amex	April 9, 2021	All existing contactless enabled POS systems must support contactless EMV mode.
Visa	October 19, 2019 (Canada)	All POS terminals in the ecosystem to remove MSD. Transactions submitted to Visa in this manner will be declined. Automated Fuel Dispenser (AFD) transactions with a contactless MSD card or mobile device transactions with MSD will continue to be permitted.
Visa	January 2021 (U.S.)	MSD Contactless will no longer be supported. Transactions may decline.
Discover	January 15, 2021	All new chip card terminals deployed with Contactless D-PAS support must disable support for contactless magstripe mode. Existing deployed chip card terminals that support Contactless D-PAS may continue to support contactless magstripe mode.
Mastercard	October 1, 2022 (Canada)	Any new contactless-enabled terminal must only support EMV mode contactless.
Mastercard	April 1, 2023 (U.S./ LAC / AP)	All newly issued or reissued contactless access devices must only be EMV mode contactless capable.

[NEW] Mastercard Announces Timeline to Retire Physical Magnetic Stripe from Cards

CP

The Change: As the markets become more EMV mature there is little to no benefit to continue support of the magstripe technology (which increases the opportunity for fraud). Mastercard has announced their timetable to retire the physical magnetic stripe from the back of cards.

The Impact: Newly issued EMV chip cards and POS devices will be required to adhere to the guidelines and effective dates outlined in the table below:

Effective Date	Regions	Details
April 1, 2024	APAC, Canada, Europe (minus Switzerland), LAC, Middle East	Newly issued EMV chip cards may optionally omit the mag stripe
April 1, 2027	United States	Newly issued EMV chip cards may omit the magstripe
April 1, 2029	Global (minus Switzerland) with exceptions	Newly issued EMV chip cards must omit the mag stripe except for: • All prepaid cards (reloadable and non-reloadable) in Canada and the US • Non reloadable prepaid card programs in all other regions
April 1, 2033	Global (minus Switzerland) with exceptions	Newly issued cards must support EMV chip technology and omit the mag stripe except for: • All prepaid cards (reloadable and non-reloadable) in Canada and the US • Non reloadable prepaid card programs in all other regions

[NEW] Mastercard Revises Cardholder Verification Method (CVM) limit for Automated Fuel Dispensers (AFD)

CP

The Program: Mastercard currently requires contactless AFD terminals in the U.S. region to have their CVM limit set to USD $0, which means that all contactless transactions are verified with a CVM.

The Change: Mastercard will align the CVM limit for AFD terminals with other point-of -service (POS) terminals by removing the requirement for the CVM limit at AFD terminals to be set to USD $0.

The Impact: AFD terminals should have CVM limits updated in the U.S. region to $100.

The Timing: February 17, 2022

[NEW] Mastercard Clarifies Standards for Gambling and Gaming Refund Transactions

CP/CNP

The Change: Mastercard is clarifying its standards as it pertains to the credit of winnings or value usable for gambling and gaming to a Mastercard or Maestro account.

The Impact: The standards clarify that the refund of cardholder funds resulting from the cardholder not using the funds for gambling or gaming, or the cardholder claiming that the transaction was fraudulent are not considered the crediting of winnings or value usable for gambling or gaming to a Mastercard account.

The Timing: Effective immediately

[NEW] Mastercard Increases the Availability of Payment Account Reference (PAR)

CP/CNP/eComm

The Program: The Payment Account Reference (PAR) is an industry-aligned approach to link Primary Account Number (PAN) based-transactions to associated tokenized transactions without using the actual PAN (which reduces the need for storage of the PAN). PAR also enables acquirers, merchants, and issuers to manage fraud, risk, customer service, and analytics such as loyalty programs.

The Change: Mastercard is expanding PAR to include support for Mastercard Digital Enablement Service (MDES) Lite and non-MDES issuers. The PAR will be included in the authorization message. Merchants may see an increase in the PAR being provided in transactions, as Mastercard will return the PAR for both tokenized and non-tokenized accounts.

The Timing: Mastercard will begin sending PAR for non-tokenized accounts in phases beginning November 2021.

[NEW] Mastercard Introduces Deferred Authorization Indicator

CP

The Program: When a card present merchant's system experiences a communication issue and an online authorization is not able to be obtained, a merchant will hold onto the authorization message and submit it when the system is back online.

The Change: In an effort to improve authorization approvals, Mastercard is introducing a new indicator to uniquely identify transactions that are stored and submitted once their system is back online.

The Impact: This new value will inform issuers the request was sent on a deferred basis and will help them to manage out-of-sequence chip Application Transaction Counter (ATC) data and reduce unnecessary declines.

Mastercard will require support of the new authorization indicator (existing field) to identify deferred (store and forward) authorizations (value of 045).

[REMINDER] Mastercard's New Data Element to Support Digital Secure Remote Payment (DSRP) Cryptogram

eComm

The Program: Mastercard has introduced a new data element to support the Digital Secure Remote Payment (DSRP) cryptogram.

The Change: Mastercard is requiring the mandatory use of a new field for Digital Remote Commerce (DSRP) transactions initiated with a token cryptogram in order to provide additional digital data-related information to issuers. The new field will allow for both the UCAF value and the cryptogram to be present in DSRP (In-app) transactions.

The Impact: Effective February 2022, merchants will need to support the following new field and sub-element so that the cryptogram and AAV may be sent for In-app transactions:

- **Digital Payment Data**
  - Digital Payment Cryptogram

Please refer to the charts below for details on the new fields within our specs.

Tran Type	Scenario	RAFT ISO Auth Request	RAFT ISO Response	EMD File
In-App with Cardholder Authentication or 3-D Secure transactions	**3-D Secure for MC Identity Check SPA AAV/Accountholder Authentication Value**	** Set Field 121 Tag 01 Position 1 to 'Y' ** Set Field 121 Tag 01 Position 3 to 'Y'	** Data may be returned in Field 121 Tag 05 (UCAF/AAV Data)	** Set MasterCard Record 41.2.2 (MC Customer Addendum Record Type 2) Accountholder Authentication Value to value from Field 121 Tag 05 response
In-App transactions	**Digital Payment Cryptogram**	**Set Field 62.85	N/A	N/A
In-App transactions	**Remote Commerce Acceptor ID**	** Set Field 62.86	N/A	N/A

Tran Type	Scenario	RAFT 610 Auth Request	RAFT 610 Response	EMD File
In-App with Cardholder Authentication or 3-D Secure transactions	**3-D Secure for MC Identity Check SPA AAV/Accountholder Authentication Value**	**Set Optional Processing Indicator G009, Field/Position 42, to 'Y'	** Data may be returned in Reply Group R030 Tag AA (UCAF/AAV data) Note: Spec reflects a length of 2 and should reflect 32. Will be updated in v2.33	** Set MasterCard Record 41.2.2 (MC Customer Addendum Record Type 2) Accountholder Authentication Value to value from Reply Group R030 Tag AA response.
In-App transactions	**Digital Payment Cryptogram**	**Set G065, Field 1	N/A	N/A
In-App transactions	**Remote Commerce Acceptor ID**	**Set G066, Field 1	N/A	N/A

[REMINDER] Mastercard Revises Chargeback Standards for Automated Fuel Dispensers in U.S. Region

CP

The Program: When a USD $1 authorization is obtained at an AFD in the United States region, the merchant/ acquirer is protected from authorization-related chargebacks, message reason code 4808 (Authorization-related Chargeback), up to the chargeback protection amount.

The Change: Mastercard is increasing the Authorization-related chargeback protection amount for automated fuel dispensers (AFDs) located in the U.S. region. This chargeback protection applies to all cards, regardless of the country in which the card is issued.

The Impact: The chargeback protection amount at AFDs in the United States region will increase to USD $350 for Mastercard commercial cards programs (such as Mastercard Corporate Card®, Mastercard Corporate Executive Card®, Mastercard Corporate Fleet Card®, or Mastercard Corporate Purchasing Cards®) and to USD $125 for any other Mastercard® card.

The Timing: October 15, 2021

[REMINDER] Mastercard Authentication Requirements for Identity Check and Retiring SPA 1

eComm

The Change: Mastercard is retiring Secure Payment Algorithm (SPA 1) Accountholder Authentication Values (AAV) usage in Identity Check and will map to SPA 2 values. Mastercard will end support of this algorithm for EMV 3DS 2.0 authentications and authorizations.

SPA 2 AAV will simplify **key management and will allow Mastercard to validate AAV integrity and the issuer to validate Issuer Authentication Value (IAV) correctness** without the need to exchange keys.

The Impact: Effective October 15, 2021 any SPA 1 AAVs generated by Access Control Servers will result in a 203-error code “SPA 2 algorithm was not used by ACS.” The SPA 1 AAV will then be converted to SPA 2 AAV values for processing by the Mastercard Directory Server.

SPA1 AAVs will still be permitted to process 3DS1 authentication and transactions. As a reminder, 3DS1 is set to retire in October 2022.

Merchants should contact their authentication provider for additional details.

The Timing: October 15, 2021

[REMINDER] Mastercard Outlines Roadmap to Transition from 3DS 1.0 to EMV 3DS 2.0

eComm

The Change: Mastercard is providing an update to their plan for transition of all customers to EMV 3DS (2.0) before the decommission date of EMV 3DS 1.0 services. Mastercard has taken the following steps to assist customers' transition from 3DS 1.0 to EMV 3DS (2.0).

- No longer approving new software for 3DS 1.0.
- Working actively with customers to enroll their accounts onto the EMV 3DS (2.0) network.
- Offering the Smart Authentication Stand-in solution to perform risk-based analysis for transactions where the issuer account range may not be enrolled.
- Decommission of the Attempts Server for 3DS 1.0 processing plan as outlined below. There are no Mastercard rules changes associated with this announcement. This is a technology change and Mastercard liability shift rules remain intact.

Updated Timeline	Actions	Impact
✓ May 25, 2021	Mastercard will reimplement 3DS1 card range caching so MP1 providers and merchants are aware which card ranges are supported by 3DS1 Directory Server.	Service Providers, Processors, Acquirers, Issuers
✓ July 1, 2021	Merchants and MPI providers are expected to submit their authentications to EMV 3DS (2.0) for non-supported EMV 3DS 1.0 account ranges which route to Mastercard Attempts Processing.	Acquirers, Service Providers, Processors, Merchants
October 1, 2021	**Mastercard will no longer generate Attempts transactions from the Mastercard 3DS 1.0 network.** **Issuers that still want to support Attempts must generate from their own ACS solution. 3DS 1.0 fully authenticated transactions will continue to be supported.**	Service Providers, Processors, Acquirers, Issuers
March 31, 2022	Merchants and MPI providers are expected to submit their authentications to EMV 3DS (2.0) rather than 3DS 1.0 Directory Server.	Merchants, Acquirers, Issuers
October 14, 2022	Mastercard will stop accepting EMV 3DS 1.0 transactions for cardholder authentication. Any transaction submitted with EMV 3DS 1.0 will result in an error response. All customers must be operating compliant EMV 3DS software.	Merchants, Acquirers, Issuers, Service Providers

The Impact: Mastercard is providing the final steps to complete the transition from 3DS 1.0 to EMV 3DS (2.0). These steps are designed to promote higher CNP approval rates, lower CNP fraud, and allow time for customers to complete their transition to EMV 3DS (2.0).

Merchants should contact their authentication provider for additional details.

[UPDATE] Mastercard Revises Standards for Decline Reason Code Service for Card-Not-Present Transactions

CNP/eComm

The Program: Currently, when an issuer declines authorization for a transaction, the issuer often defaults to the use of a generic decline reason code. The generic decline response code does not provide merchants or acquirers with any clarity as to why the CNP transaction was declined.

The Change: Mastercard is introducing a new Decline Reason Code Service to address challenges faced by issuers, processors, merchants, and acquirers when authorization requests are denied with a generic reason code.

The new Service will ensure proper use of transaction decline codes, indicate whether a merchant may retry a decline, and identify if updated payment information (new expiration date, card number, etc.) is available for a merchant to obtain to assist in authorization approval. This service will only apply to card-not-present Single Message and Dual Message authorizations. There will not be any new data elements introduced as part of this service.

Acquirers and card not present merchants will **no longer receive** the following decline response codes:

- 04 (Capture Card)
- 14 (Invalid Card Number)
- 41 (Lost Card)
- 43 (Stolen Card)
- 54 (Expired Card)
- 57 (Transaction Not Permitted)
- 62 (Restricted Card)
- 63 (Security Violation)

When Mastercard receives one of the above decline response codes from the issuer, they will map it to one of the following **new** response codes:

- **79** (Lifecycle)
- **82** (Policy)
- **83** (Security)

Note: All other Mastercard decline response codes will continue to be sent by Mastercard and will not be mapped to the new response codes.

Mastercard will also provide a corresponding **Merchant Advice Code (MAC)** in card not present authorization responses as applicable for the following three new response codes:

- **79** (Lifecycle)
- **82** (Policy)
- **83** (Security)

Note: Mastercard may assign a MAC to other types of response codes. Example: Recurring transaction, approved with MAC value of 01 (updated/additional information needed).

[UPDATE] Mastercard Revises Standards for Decline Reason Code Service for Card-Not-Present Transactions (cont.)

CNP/eComm

The MAC instructs the merchant how to handle subsequent authorizations using one of the following values:

- **01** - Updated/additional information needed
- **02** - Cannot approve at this time, try later
- **03** - Do not try again
- **04** – Token requirements not fulfilled for this token type
- **21** - Payment Cancellation
- **22** – (Installment only) - Merchant does not qualify for product code

The below table contains the new Mastercard mapped response codes 79, 82 and 83 and the possible combinations of MAC codes that will apply:

Samples of Response Code and Merchant Advice Code (MAC) Combinations			
MAC	**Description/Advice**	**Reason for Decline Examples**	**Merchant Action**
01	Updated/additional information needed	Expired card, account upgrade, portfolio sale, conversion	Updated information found to be available in Account Billing Updater (ABU) database – secure new information before reattempting Note: If the merchant is not enrolled in ABU, the merchant will need to contact the cardholder to acquire updated payment credentials
03	Do not try again	Account Closed, Fraudulent	Updated information NOT found in ABU database – do not retry
01	Additional information needed	Expired card, account upgrade, portfolio sale, conversion	Authentication may improve likelihood of an approval – retry using authentication (such as EMV EDS)
03	Do not try again	Account Closed, Fraudulent	Suspected fraud – do not retry
02	Cannot approve at this time, try later	Over credit limit, Insufficient Funds	Retry transaction 72 hours later

- When new expiry date is available, the MAC (Merchant Advice Code) is appended in the response message with a MAC value indicating to try again with the updated information, otherwise an indicator to not reattempt an authorization.
- For instances of recurring or credential on file transactions that include certain decline codes such as expired card, the service utilizes Account Billing Updater (ABU) to determine if new expiry date is available.
- In the case of security violation decline response codes, the Mastercard Decision Intelligence service is queried, and an appropriate fraud/security related MAC value is sent to the acquirer/merchant.
- Mastercard will require issuers to limit the use of decline response code 05 (do not honor) to five percent or less for all declines.

[UPDATE] Mastercard Revises Standards for Decline Reason Code Service for Card-Not-Present Transactions (cont.)

CNP/eComm

eComm/VAP platform development status

The Merchant Advice Code (MAC) is currently supported and is included as part of the enhanced authorization data. Merchants that wish to receive the MAC values will need to complete certification.

eComm/VAP development items below are on track and estimated to be in production in the first quarter of 2022:

- **Option to receive mapped service instead of the actual MAC** – all merchants will begin receiving existing VAP response codes that will indicate a hard (do not retry) or soft (retry) decline along with the decline description based on an internal decline code mapping service.
    - Compliance has evaluated the new response codes 83, 82, and 79 and all MAC code combinations and assigned existing VAP response codes that resembled the most common reason for the decline.
- **eComm/VAP reauthorization** – Logic will be added so that declined authorizations are not retried when in connection with a MAC value of 03 (do not try again) or 21 (payment cancellation).

Core platform development status

Merchants that wish to receive the MAC values will need to complete a recertification.

Development work for the core platform is in process and is estimated to be complete in November 2021. Updates to include:

- **Merchant Advice Codes (MAC's) in merchant specifications**
    - **ISO 8583** – Field 120.AC (Merchant Advice Code (request only) When the response indicator is Y, Worldpay responds with Merchant Advice Code data from the network in this ISO field)
    - **610 Interface** - Field 43 (A value of Y will attempt to send reply group R030 tag AC 'Merchant Advice Code Indicator" in the reply)
    - **Raft API** – Fields 18.36 (Y/N flag to request data) and 20.1 (field for the return data from Mastercard)
    - **PCD Petro** – Does not apply for CNP/ecommerce transactions
    - **Merchant Batch Authorization** – Support is planned for the first quarter of 2022. This will address ecommerce, recurring, and installment transactions.
- **Reauth product** – Logic will be added so that declined authorizations with MAC values of 03 (do not try again) or 21 (payment cancellation) are not retried. Timing is TBD.
- **New response codes 79, 82, 83** – These response codes are currently supported in ISO 8583, 610, Raft API, and Batch Auth.

Mastercard Acquirer Merchant Advice Code Transaction Processing Excellence (TPE) Program

A fee will be assessed in the event an authorization is retried within 30 days of a decline received with a MAC value of 03 (do not try again) or a 21 (payment cancellation).

[NEW] Visa Introduces Additional Data Requirements for Visa Fleet Card Transactions

CP

The Program: Visa has received feedback from the fleet industry that additional data and more controls are needed in order to determine what is eligible for purchase with a Visa fleet card.

The Change: Visa is introducing new rules and data requirements for Visa fleet card transactions accepted at Automated Fuel Dispensers (AFD) with MCC 5542 and inside the service station MCC 5541.

Some highlights of the changes include:

- Expanded Fuel Type (moving from a 2-digit to a 4-digit product code)
- Fleet Employee Number
- Fleet Trailer Number
- Fleet Additional Prompted Data 1 and 2 (Additional data that the issuer asks the cardholder to enter at the POS)
- Purchase Restriction Flag (merchant can indicate what card or host-based restrictions they can support at the POS)
- Host-Based Purchase Restrictions (If the merchant supports this, the issuer can send new restrictions within the Preauth response to override those within the card chip data)
- Various fields have been moved to new fields with the authorization and clearing records while others have been deleted

The Impact: AFD and Service Station merchants will be required to comply with the new data requirements for Visa fleet cards.

Merchants that currently use the 2-digit Visa product codes must change to the new 4-digit Visa product codes by April 2022. Merchants that use the Conexxus codes will not need be required to make product code updates as Worldpay will continue to map the codes to the new 4-digit code.

The Timing: April 2022

[NEW] Visa Introduces Changes to Stand-In Processing Attempts CAVV (Cardholder Authentication Verification Values)

CP/CNP/eComm

The Program: Visa is implementing changes to allow issuers to determine how their Visa Secure transactions with attempts CAVV should be processed when in STIP.

The Impact:

U.S. and Canada Regions

If the issuer's VisaNet STIP parameter is set to not decline all attempts CAVV, Visa will process authorization, full financial, and account verification transactions using the issuer's existing CAVV STIP and other STIP parameter settings.

LAC and AP Regions

If the issuer's STIP parameter is set to decline all attempts CAVV, Visa will decline the authorization, full financial, and account verification transactions.

New VIP STIP Rules for Attempts CAVV – Applies to attempts CAVVs created by the issuer attempts server or Visa Attempts Service.

Issuer parameter is set for Visa to **not decline all attempts** CAVV in STIP ((U.S. and Canada Regions (default)):

Condition	Processing
Field 126.9.1-CAVV Data, Usage Code 3, position 1 (Authentication Results Code) Contains one of the following existing ECI values: • 07 – Acquirer attempt-(status A); proof of authentication attempt generated for non-participating issuer or cardholder • 08 – Acquirer attempt, issuer ACS not available (status A); proof of authentication attempt generated for participating issuer with server unavailable (Visa Proof of Attempts STIP)	V.I.P. will process the transaction based on existing processing using the issue's CAVV STIP and other STIP parameters regardless of ECI value.

Issuer parameter is set for Visa to **decline all attempts** CAVV in STIP ((LAC and AP Regions (default)):

Condition	Processing
Field 126.9.1-CAVV Data, Usage Code 3, position 1 (Authentication Results Code) Contains one of the following existing ECI values • 07 – Acquirer attempt-(status A); proof of authentication attempt generated for non- participating issuer or cardholder • 08 – Acquirer attempt, issuer ACS not available (status A); proof of authentication attempt generated for participating issuer with server unavailable (Visa Proof of Attempts STIP)	• Decline the transaction with existing response code 82 (Negative online CAM, dCVV, iCVV, or CAVV results) in existing Field 39- Response Code • Return the CAVV results code value in existing Field 44.13-CAVV Results Code in the response message to the acquirer based on existing CAVV processing

[NEW] Visa Outlines Support for Visa Secure Credential Framework

eComm

The Program: As payments increase in the ecommerce space, Visa strives to make digital payments as simple and secure as face-to-face transactions. The Visa Secure Credential Framework aims to:

- Increase security in the e-commerce payment ecosystem with wider use of tokens
- Reduce fraud within the card not present payment ecosystem
- Ensure availability of tokens when requested to drive improved performance based on set performance requirements

The Change: Visa is adding support of a new subfield of an existing field to indicate if a merchant participates in Visa's Token program. The Additional Token Response Information field will be used to identify transactions that are eligible for token services and will be sent back in the authorization response.

The Impact: If a transaction is eligible for token services, a value of 1 will be returned in the authorization response. Visa will return a space if the transaction is not eligible. The indicator must also be sent in the clearing/settlement message.

The following must be present to receive the value of 1:

- Card not present transaction
- PAN is a payment token
- One of the following transaction types is present (purchase, account funding, quasi cash, credit/refunds, original credit, bill payment)

- Visa's goal is to identify if a PAN is registered with their token service, which may be part of the criteria reviewed in future interchange qualification.
- Please note that the value will be sent back in the authorization response from Visa and must also match in settlement, as this information will be used for interchange qualification.
- Merchants will need to capture this value in both authorization and settlement to qualify for the upcoming card-not-present token rates. More information on interchange impact will be shared once available.

[REMINDER] Visa Reminder to Follow Token Cryptogram Requirements to Avoid Authorization Declines

CP/CNP/eComm

The Program: Token cryptograms must be new and unique for each authorization request and must not be stored beyond the authorization request. Ensuring the integrity of cryptograms is essential as part of a key token domain control and to prevent fraud.

The Change: Effective January 30, 2022, a resubmitted or stale token authentication verification value (TAVV) or dynamic token verification value (DTVV) will result in a declined authorization request.

To avoid declined authorization requests, acquirers and merchants must ensure compliance with the following existing rules and requirements regarding TAVV and DTVV cryptograms for cardholder-initiated, token-based COF and e-commerce transactions, including in-app e-commerce:

- Must be new and unique for each authorization request
- Must be one-time use
- Must not be stored beyond the authorization request. The TAVV, DTVV and electronic commerce indicator values provided by the token requestor must be unchanged when submitted in the authorization request message
- A resubmitted or stale TAVV or DTVV will result in a declined authorization request
- Merchant-initiated transactions must follow the merchant-initiated transaction framework, and do not include token cryptograms

The Timing: January 30, 2022

[REMINDER] Visa will No Longer Permit Merchant/Card Acceptor and Terminal ID Numbers to be Printed on Receipts

CP/CNP/eComm

The Change: Through investigations conducted by Visa, it has been determined that fraudsters may use the identification numbers on printed receipts, like the card acceptor ID (CAID), merchant ID (MID) and the terminal ID (TID), to clone terminals and process fraudulent transactions.

The Impact: To aid in the ongoing efforts around security in the payments system, the printing of merchant/card acceptor (MIDs/CAIDs) and terminal (TIDs) identification numbers on all transaction receipts will no longer be permitted. This includes POS, ATM, Quasi-Cash and Manual Cash Disbursement transactions.

Masking or truncation is permitted if the full values cannot be easily derived. Merchants who need to identify or recover transactions when a terminal is down/offline and require the TID for identification, are permitted to place a label on the bottom of the terminal with the TID if it is not in plain sight.

Exceptions

- POS devices and payment gateways connected to a processor host using payment card industry validated point-to-point encryption (P2PE) or cryptographic keys for all host connectivity. While these scenarios offer appropriate protection against merchant cloning, it is still advised not to print MIDs, TIDs, or CAIDs.
- Merchants located in a jurisdiction where the printing of these identification numbers is required by law.

The Timing: October 15, 2022

[REMINDER] Visa 3DS 1.0.2 to EMV 3DS Migration and Fraud Liability Protection Updates

eComm

The Program: Visa is committed to supporting the industry's transition from 3DS 1.0.2 to EMV 3DS; therefore, Visa will discontinue support for 3DS 1.0.2 and all related technology as of October 15, 2022.

The Change: To provide merchants more time to prepare for the full sunset of 3DS 1.0.2, Visa has made the decision to revise the rule change that was previously communicated to remove merchant fraud liability protection on 3DS 1.0.2 transactions.

The Impact: Effective October 16, 2021 Visa will continue to support 3DS 1.0.2 transaction processing, including the 3DS 1.0.2 Directory Server, but will stop support of 3DS 1.0.2 Attempts Server for non-participating issuers.

If an issuer continues to support 3DS 1.0.2 after October 15, 2021 it will be able to respond to merchants with a fully authenticated response and Cardholder Authentication Verification Value (CAVV), **and merchants will obtain fraud liability protection and these transactions will be blocked from fraud-related disputes in Visa's system.**

Visa Secure Using 3DS 1.0.2	Prior to October 16, 2021	Effective October 16, 2021
Fully Authenticated - Electronic Commerce Indicator (Issuer participates)	Merchant ***receives*** fraud-related dispute protection (ECI 05)	NO CHANGE
Attempted Authentication - Electronic Commerce Indicator (Issuer participates)	Merchant ***receives*** fraud-related dispute protection (ECI 06)	NO CHANGE
Attempted authentication (Issuer does not participate)	Fraud liability with Issuer (ECI 06)	Fraud liability with merchant (ECI 07)

Note: There are no changes to the Visa Secure rules using EMV 3DS

[REMINDER] Visa Introduces New Decline Response Code Rules and Integrity Fees

CP/CNP/eComm

The Program: Acquirers and merchants have been communicating to Visa that it is difficult to understand why an authorization declined as most issuers respond with 05 (Do Not Honor) response code. Merchants could make more informed decisions on how to proceed with the transaction if they understood the actual reason for decline.

The Change: To address numerous issues around decline response code usage, Visa is introducing a set of new rules and fees to ensure that issuers, acquirers, and merchants use and act upon decline response codes, appropriately. The new rules and fees announced as part of this effort are designed to:

- Enhance decline code management
- Ensure authorization consistency
- Improve authorization approval rates
- Reduce operational costs
- Reduce fraud

Visa Grouping of Decline Codes and Rules for Retries

U.S., Europe, Canada, and LAC Regions

Visa is revising the rules regarding the resubmission of declined transactions as outlined below:

- Grouping all decline response codes into four categories and changing rules around usage and treatment of the response code in each group by issuers and merchants
- Expansion to allow merchants to resubmit authorization requests that were previously declined in the Canada, LAC, and U.S. Regions
- Changing the resubmission timeframe and frequency of declined auth response
- Managing first party fraud
- New Fees will be introduced for non-compliance

Core platform

- Development and support are complete, and all Visa response codes are supported.
- Merchant specifications have been updated with a new data formats called “Raw Network Data” that contains a “Y/N” flag/indicator. When a merchant sends a “Y”, this indicates that the actual Visa response code value will be sent in the authorization response to the merchant.
- If the merchant sends a “N” then the actual Visa response code values are not returned in the authorization response.
- An “N” is the default value for this field in all specifications.

Core Merchant specification field updates are outlined below:

- **ISO 8583 Spec**: added to Field 120 - Additional request data – Table 5-122
- **610 Interface Reference Guide**: added Field 40 to G009, Optional Processing Indicators, Table 4-12
- **PCD/Petroleum Transaction Message Specification**: added Field 07 to G001 – Table 6-1
- **RAFT API**: screen shot below

```
RawNetworkDataRequest_Type:
  type: string
  maxLength: 1
  description: "Y/N flag indicating the acquirer would like the Raw Network Data returned in the response if available."
  example: "Y"
```

[REMINDER] Visa Introduces New Decline Response Code Rules and Integrity Fees (cont.)

CP/CNP/eComm

eComm/VAP platform

- We have identified four response codes that are not currently mapped to an eComm 3-digit response code.
- The new response codes have been mapped to the **existing eComm 3-digit response codes below** as of August.
  - The four response codes are as follows:
    - 01 (refer to issuer) – 120
    - 02 (refer to card issuer, special condition) - 120
    - R1 (revocation of authorization order) - 361
    - R3 (revocation of authorizations) - 361

Merchants should review their resubmission processes and timing, as there may be financial implications if authorizations are resubmitted for a decline response that is not permitted.

Enhancing Decline Code Management

Many issuers respond to an authorization request with a generic decline response code or with a response code that does not provide enough information to merchants to understand why the issuer declined the authorization. Visa will be redefining decline codes to provide acquirers and merchants with additional information that will increase merchant approval rates.

Merchants in the U.S., Canada, Europe, and the LAC regions may resubmit an authorization request following a decline for response codes listed in categories 2, 3, and 4 only.

- Retries are limited to 15 in 30 days and applies to all transaction types, except transit.
- For transit transactions, (all regions except Europe) resubmission retries are limited to 4 attempts in 14 days.
  - For Europe/transit transactions, resubmissions cannot exceed 6 reattempts in 14 days.

Decline Response Code Use – Effective April 17, 2021

Category	Category Description	Response Codes	Are Retries Permitted?
1	This category represents decline response codes indicating the card is blocked for use or never existed. As such, there are no circumstance in which the issuer will ever grant an approval.	04 - Pickup card, no fraud 07 - Pickup card, special condition 12 - Invalid transaction 14[1] - Invalid account number (no such number) 15 - No such issuer, first 8 digits of account number do not relate to an issuing identifier 41 - Pickup card, lost card 43 - Pickup card, stolen card 46 - Closed Account (NEW effective 4/17/21) 57 - Transaction not permitted to cardholder R0 - Stop payment order R1 - Revocation of authorization order R3 - Revocation of all authorization orders	No.

Category	Category Description	Response Codes	Are Retries Permitted?
2	This category represents decline response codes indicating that the issuer may approve but cannot do so at this time. This could be due to a system issue or a lack of funds. This category includes temporary decline decisions made by issuers which may change over time. They occur when the issuer is prepared to approve a transaction at some point, is unable to do so at the time, but would welcome an additional authorization attempt in the future.	03 - Invalid merchant 19 - Re-enter transaction 51 - Not sufficient funds 59 - Suspected fraud 61 - Exceeds approval amount limit 62 - Restricted card (card invalid in region or country) 65 - Exceeds withdrawal frequency limit 75 - Allowable number of PIN-entry tries exceeded 78 - Blocked, first used - transaction from new cardholder, and card not properly unblocked (NEW effective 4/17/21 – Brazil only) 86 - Cannot verify PIN 91 - Issuer or switch is inoperative 93 - Transaction cannot be completed– violation of law 96 - System malfunction N3 - Cash service not available N4 - Cash request exceeds issuer or approved limit	Yes. Limit retries to 15 in 30 days (excludes transit). Exception: transit transactions, all regions (except Europe) limit retries to 4 in 14 days. For Europe transit, limit to 6 retries in 14 days.
3	Data quality: revalidate payment information and enter correct/updated information before resubmitting entry. This category represents decline codes indicating the issuer cannot approve based on the details provided. Examples include incorrect Card Verification Value 2 (CVV2) or expiration date.	14[1] - Invalid account number, no such number 54 - Expired card or expiration date missing 55 - PIN incorrect or missing 6P- Verification data failed (NEW effective 4/17/21) 70 - PIN data required (Europe region only) 82 - Negative online CAM, CAVV, dcVV, iCVV, or CVV results or offline PIN authentication interrupted 1A - Additional customer authentication Required (Europe region only) N7 - Decline for CVV2 Failure	Yes. Limit retries to 15 in 30 days. Exception: transit transactions, all regions (except Europe) limit retries to 4 in 14 days. For Europe transit, limit to 6 retries in 14 days.
4	Most decline reason codes fall into the above categories, but some special codes may be used on an ad-hoc basis. Their usage should remain minimal. This category includes all other decline response codes, many of which are technical in nature or provide little to no value to acquirers or merchants.	All other decline response codes NOT listed in categories 1-3.	Yes. Limit retries to 15 in 30 days. Exception: transit transactions, all regions (except Europe) limit retries to 4 in 14 days. For Europe transit, limit to 6 retries in 14 days.

[1] Response Code 14 will be included in both Category 1 and Category 3 (data quality). Merchants must not reattempt any transaction using the same account number following a decline for Response Code 14, but it will be included in transaction counts for data quality monitoring.

[REMINDER] Visa Introduces New Decline Response Code Rules and Integrity Fees (cont.)

CP/CNP/eComm

Ensuring Authorization Consistency

To obtain an approval, some merchants and acquirers are in the practice of modifying data fields upon an issuer decline; attempting to identify a gap in issuer authorization controls and detection systems. This data manipulation is damaging to the Visa system and can impact the issuer's ability to effectively authorize transactions.

Visa will assess the following fees on a per transaction basis when a merchant exceeds the reattempts threshold and/or reattempts a transaction after receiving a declined response code under Category 1.

U.S. | Canada | Europe **APRIL 1, 2021**		
Transaction Criteria	**Domestic Fee**	**Cross-border Fee**
Decline transaction resubmission in excess of the allowable re-try limit	USD $0.10	USD $0.15
U.S. | Canada **APRIL 1, 2022**		
Transaction Criteria	**Domestic Fee**	**Cross-border Fee**
Issuer will never approve - reattempt	USD $0.10	USD $0.15
LAC **APRIL 1, 2021**		
Transaction Criteria	**Domestic Fee**	**Cross-border Fee**
Issuer will never approve (Category 1)	USD $0.10	USD $0.25
Issuer cannot approve at this time (Category 2)	USD $0.10	USD $0.25
Issuer cannot approve with these details (Category 3)	USD $0.10	USD $0.25
Generic response codes (Category 4)	USD $0.10	USD $0.25

[NEW] Discover Expands Non-Compliance Fee Program

CP/CNP/eComm

The Change: Discover is expanding the types of transaction failures that will be considered as part of their Program Performance Standards.

The Impact: Failure to accurately populate authorization requests and/or settlement messages may result in non-compliance assessments (up to $1,000 per month) to merchants.

Discover may assess non-compliance fees for the following transaction failures:

- Not passing appropriate authorization and sales data (settlement information)
- Non-support of all IIN ranges
- Non-support of all Discover brand products (JCB, UnionPay)

Merchants will be notified of transaction failures and be provided a minimum of ninety (90) days to remediate.

The Timing: November 2021

[NEW] Discover Reminds of ProtectBuy Support and Announces the Sunset of ProtectBuy 1.0.2

CNP/eComm

The Change: As of October 15, 2021, merchants that support a 3DS program offered by another payment network, must also support Discover ProtectBuy to remain in compliance with the Discover Operating Regulations.

Effective October 14, 2022, Discover will no longer support authentication using ProtectBuy 1.0.2.

The Impact: Merchants and acquirers will need to support ProtectBuy 2.0 as 1.0.2 will be sunset and no longer available after October 2022.

American Express

[NEW] American Express Introduces New Decline Action Codes

CP/CNP/eComm

The Change: American Express is introducing two new action codes to provide clarity as to why a transaction was declined by the issuer.

The Impact: Merchants and partners may begin to see the following new action codes on applicable declined transactions.

- 116 – Not sufficient funds
- 121 – Limit exceeded

The Timing: October 2021

[NEW] American Express Updates OptBlue MCC Eligibility and Exclusion Lists

CP/CNP/eComm

The Change: American Express has updated their OptBlue participation list to allow three new MCCs. American Express has also updated their exclusion list to identify brands that are no longer eligible to participate in the OptBlue program.

The Impact: The following three MCCs are **now eligible to participate** in the American Express OptBlue program:

- MCC 5552 Electrical Vehicle Charging
- MCC 6540 Non-Financial Institutions – Stored Value Card Purchase/Load
- MCC 6211 Securities Brokers/Dealers

American Express announced that the following brands are **no longer eligible to participate** in the OptBlue Program.

- Choice Hotels

[UPDATE] American Express Outlines new SoftPOS Terminal Classification Codes

CP/CNP/eComm

The Program: SoftPOS is a product that allows merchants to turn their mobile phone or tablet into a point of sale (POS) device. These transactions will be treated as contactless Expresspay and a new indicator will identify these contactless transactions as SoftPOS (transactions that originated from a mobile device).

The Impact: American Express requires a new indicator to uniquely identify these contactless transactions from mobile devices. The terminal classification code values should be used as outlined below.

Terminal Classification Code	Description
AC	mPOS Accessory/dongle with contact and contactless interfaces, with or without PIN pad.
AS	mPOS Accessory/dongle with contact and contactless interfaces and PIN on Glass support (SCRP,Software-based PIN on COTS [commercial off the shelf]).
CC	Contactless Payment on COTS (CPoC) - Mobile device based contactless only mPOS without PIN support.
CS	Contactless Payment on COTS (CPoC) - Mobile device based contactless only mPOS with PIN on Glass support.