Merchant Network Updates
Spring 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 April 16, 2021 central processing date of April 17, 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

April 2021 UPDATE

Core Platform

Worldpay from FIS enabled the code to send credit/refund transactions to Visa, Mastercard, and Discover for authorization for all core merchants effective **February 2, 2021.** Due to unfavorable approval rates on Mastercard return transactions, code was turned off for Mastercard only on February 5. Mastercard will be re-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.

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

Network Fees and Returns

With the change to authorize return transactions, additional network fees will start to be assessed to returns:

- **Discover:** Authorization fee of $0.0025* will apply to credit/refund authorization requests.
  *Effective April 2021, the Authorization fee will be $0.0190
- **MasterCard:** The NABU fee will **not** apply to return transactions submitted for authorization.
- **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.

Important Dates by Brand

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, 2021**
Mastercard	**TBD** - Optional for acquirers and merchants	TBD	N/A
Discover	**July 17, 2020**	July 17, 2020	**Feb 2, 2021**

Visa Stand In Processing for Invalid Authorization Decline Responses

Effective April 16, 2021 – Visa will stand in based on issuers' STIP rules, and override with approval (in most cases or continue with a decline) when an issuer responds with a decline response code not permitted for returns. Issuers will be limited to responding with the list of valid decline response codes. 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; however, the volume should decrease as a result of this change.

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

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

Visa will begin to decline credit 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

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 auths on behalf of merchants
- Core merchants can send in the tran id in credit/refund auths

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

[NEW] 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 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 on or before December 31, 2020 are valid for three (3) years from the initial letter of approval and a maximum of one, 1-year renewal subject to completion of renewal certification requirements.
- 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.

[REMINDER] EMV Automated Fuel Dispenser (AFD) Liability Shift Update CP

The Change: The Brands' EMV liability shift for U.S. acquired AFD transactions[1] under Merchant Category Code 5542 – Automated Fuel Dispensers have been revised as outlined below:

- SHAZAM has announced a delay in the EMV AFD liability shift date until April 2021.

April 1, 2021

- ACCEL and STAR have announced a delay in the EMV AFD liability shift until April 1, 2021.

April 16, 2021

- CULIANCE, JEANIE, and NYCE have announced a delay in the EMV AFD liability shift until April 16, 2021.
- Mastercard / Maestro has announced a delay in the EMV AFD liability shift date until April 16, 2021**.**
- Discover & American Express have announced a delay in the EMV AFD liability shift date until April 16, 2021**.**

April 17, 2021

- Visa / Interlink has announced a delay in the EMV AFD liability shift date until April 17, 2021**.**
- Voyager and AFFN have announced a delay in the EMV AFD liability shift date until April 17, 2021.

April 19, 2021

- PULSE has announced a delay in the EMV AFD liability shift date until April 19, 2021.

July 1, 2021

- **WEX** has announced a delay in the EMV AFD liability shift until **July 1, 2021.**

[1]In late 2016 and early 2017, the brands delayed the liability shift for U.S. domestic AFD transactions under MCC 5542 from October 2017 to October 2020.

In May 2020 the brands delayed the liability shift for U.S. domestic AFD transactions under MCC 5542 from October 2020 to April 2021 as outlined above.

REMINDERS

- For properly formatted and identified fallback transactions, fraud liability will remain with the issuer except for Visa lost/stolen transactions.
- For Visa, merchants may be liable for fallback transactions in lost-or-stolen cases.
- Visa advises that, where possible, magnetic stripe transactions on AFD terminals be directed to pay inside.
- Issuers may decline fallback transactions at a higher rate than chip read transactions.

AFD Merchants should be finalizing their EMV certifications in order to meet the outlined liability dates.

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

The Program: The EMV standard uses Public Key technology to perform certain functions related to offline authentication, some aspects of online transactions and offline PIN encryption. Each of the card brands publish sets of these keys for use with their EMV applications.

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**
- 1408-bit keys have an expiry date of **12/31/2024**
- 1984-bit keys have an updated anticipated expiry date of **12/31/2030**

  Note: while the card brands set their own expiration dates, generally they will align with EMVCo guidance.

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.
- Per UnionPay rules, merchants must not remove the 1152-bit key for UnionPay until the expiration as outlined above

[UPDATE] 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
Mastercard	October 2016	Newly deployed terminals must support EMV contactless functionality
Discover	August 23, 2018	Terminals that are being upgraded must also support EMV mode contactless.
Amex	April 10, 2020	All new and replaced contactless enabled POS systems must support EMV contactless only.
Amex	April 9, 2021	All existing contactless enabled POS systems must support contactless EMV mode.
Visa	April 13, 2019 (U.S.)	Newly deployed POS terminals or terminals being upgraded must disable MSD contactless.
Discover	October 18, 2019	All newly deployed point-of-sale (POS) terminals that support contactless acceptance must only support EMV mode contactless transactions. *Magstripe mode contactless must not be supported.*
Mastercard	October 18, 2019	All newly deployed POS terminals that support contactless acceptance must only support EMV mode. ***Magstripe mode contactless must not be supported.***
Visa	October 18, 2019 (U.S.)	All POS terminals in the ecosystem must only support EMV mode contactless (remove MSD)
Visa	October 19, 2019 (Canada)	All POS terminals in the ecosystem, 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.
Mastercard	January 1, 2020 (Canada)	Support of contactless mag-stripe mode at terminals will be optional
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	All contactless-enabled terminals must only support EMV mode contactless transactions

[NEW] Mastercard Revises Standards for Point of Interaction (POI) Currency Conversion

CP

The Change: Mastercard is revising its standards to update and introduce new requirements for point of interaction (POI) currency conversion (DCC).

The Impact: An overview of the revised standards include, but are not limited to the following:

- Introducing new requirements for cardholder disclosure when POI currency conversion (DCC) is offered for ecommerce transactions
- Introducing new requirements for Priority Check-Out
- Creating overarching cardholder disclosure for all acceptance environments and eliminating the breakout of cardholder disclosure across acceptance environments
- Clarifying that Mastercard may approve or reject the presentment or display of cardholder disclosure at the POI
- Eliminating the suggested model screens offering POI currency conversion (DCC) and consolidating the other suggested model screen

The Timing: Immediately

[NEW] 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).

[NEW] 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
- **21** - Payment Cancellation

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.

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

Mastercard is also introducing a new program, the Acquirer Merchant Advice Code Transaction Processing Excellence (TPE) Program, and fees for non-compliance to ensure that merchants are using the Merchant Advice Codes (MACs) and retrying declined authorizations properly.

Acquirers/merchants must ensure that a decline is not retried for authorization when MAC 03 (Do not try again) or 21 (Payment Cancellation) is received in the authorization response. 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 or 21.

Worldpay from FIS is working with Mastercard to delay the implementation of TPE Fees as the Merchant Advice Code (MAC) is not currently supported across all merchant formats on our core and eComm platforms.

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

eComm

The Change: Mastercard has announced their plan to transition all customers to EMV 3DS (2.0) prior to the decommission date of 3DS 1.0. There are no changes to the Mastercard 3DS liability shift rules with this announcement. Current liability shift rules will continue to apply to both EMV 3DS and 3DS 1.0 transactions.

The Impact: Customers must begin their transition to the new specification version immediately to ensure no transaction impact. Failure to move to EMV 3DS 2.0 by the deadline may result in declined transactions.

Mastercard will continue to support 3DS 1.0 transactions on the Mastercard Authentication Network up until the final decommission date.

Revised Payment Network Rules

Mastercard's global decommissioning plan of 3DS 1.0 is outlined below.

Effective Date	Actions	Impact
✓ October 1, 2020	Mastercard will start monthly notifications to customers of their need to transition to EMV 3DS.	Merchants, Acquirers, Issuers
✓ February 1, 2021	Mastercard will no longer accept SHA1 server certificates for 3DS 1.0 transactions. All transactions using SHA1 server certificates by this date will result in an error from the Mastercard Directory Server.	Service Providers
April 30, 2021	**Mastercard will no longer allow 3DS 1.0 account range or merchant ID enrollments unless the customer is already enrolled onto EMV 3DS.**	Merchants, Acquirers, Issuers
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.**	Merchants, Acquirers, Issuers
April 30, 2022	Mastercard will no longer allow 3DS 1.0 account range or Merchant ID enrollment.	Merchants, Acquirers, Issuers
October 14, 2022	Mastercard will no longer process any 3DS 1.0 transactions for cardholder authentication. Any transaction submitted to the Mastercard 3DS 1.0 Directory Server will result in an error response.	Merchants, Acquirers, Issuers, Service Providers

[UPDATE] Mastercard Transaction Integrity Classifications (TIC) CP/CNP/eComm

The Program: Mastercard has introduced the Transaction Integrity Classification to provide a mechanism to evaluate the safety and security of a transaction. The intent of the Transaction Integrity Classification (TIC) indicator is to assess both the validity of the card and the cardholder.

UPDATE

Worldpay from FIS advocated on behalf of our customers to delay the compliance monitoring mandate. As such, Mastercard transactions will not be downgraded to standard interchange rates if the TIC value does not match between the authorization response and settlement message. A new compliance monitoring date has not yet been announced by Mastercard. Once announced merchants will need to ensure compliance to avoid downgrades and/or rejects.

Background

- Mastercard transactions will be downgraded to standard interchange rates if the TIC value does not match between the authorization response and settlement message.
- Mastercard will be introducing a new clearing edit to verify that a valid TIC value is present in settlement. Transactions that do not include a TIC value in settlement may reject.

Reminders

- The TIC will be provided by Mastercard for point-of-sale purchase and purchase with cash back transactions as part of the authorization response message for Mastercard credit and Debit cards.
- The TIC value must be provided in the clearing/settlement record in order to avoid interchange downgrades and transaction rejects.
- All customers that send an EMD file or Batch Authorization file will be required to support receipt of the TIC indicator value in the authorization response message and to return this same value in the clearing/settlement record.

Valid values for the TIC are outlined in the chart below.

Valid Values for the Transaction Integrity Class		
Card and Cardholder Present	EMV/Token in a Secure, Trusted Environment	A1
Card and Cardholder Present	EMV/Chip Equivalent	B1
Card and Cardholder Present	Mag Stripe	C1
Card and Cardholder Present	Key Entered	E1
Card and Cardholder Present	Unclassified	U0
Card and/or Cardholder Not Present	Digital Transactions	A2
Card and/or Cardholder Not Present	Authenticated Checkout	B2
Card and/or Cardholder Not Present	Transaction Validation	C2
Card and/or Cardholder Not Present	Enhanced Data	D2
Card and/or Cardholder Not Present	Generic Messaging	E2
Card and/or Cardholder Not Present	Unclassified	U0

- Customers should work with their RMs or Account Managers to open a project to test and certify all updates made to support the Mastercard TIC.
- HDC customers will not be required to send the TIC value as Worldpay will handle submitting the TIC in the settlement message.

[NEW] Visa Eliminates Status Check Messages for All Merchants (Excluding AFDs)

CP/CNP/eComm

The Program: Since 2008 Visa has required merchants in all regions to use zero-account verification messages to verify a customer's account status. Unfortunately, merchants continue to incorrectly use authorizations with low dollar amounts instead of zero-amount account verifications.

The Change: Visa has announced that they are eliminating status check messages for all merchants, except for Automated Fuel Dispenser (AFD) merchants. While Visa has not confirmed transaction rejects to enforce the elimination of status checks, these messages may become subject to compliance action in the future.

The Impact:

- **Account Verification – Non-AFD merchants** - Use account number verification in the amount of $0.00 to validate the cardholder account.
  - Account Verification usage includes the addition of an account number to the customer profile for credential on file as well as any time there is a re-validation of stored credentials.
  - In the LAC region, Hospital merchants (MCC 8062) - Must ensure they use account verification and discontinue using the $1 status check message for validation, as currency conversion will begin to take place on $1 status checks and the dollar amount authorized will be converted to the currency used to bill the cardholder account.
- **Status Check - AFD merchants not participating in Real Time Clearing (RTC)** - Use this method to authorize $1 at the pump to validate the cardholder account. The authorization must then be reversed unless settling the transaction for $1. **Reminder:** Non AFD merchants using Status Check messages will only receive dispute protection for an authorization request approved for $1.

The Timing: April 16, 2021

[REMINDER] Visa Checkout is Changing to Click to Pay

eComm

The Program: A new set of industry-wide standards have been created for ecommerce transactions. Click to Pay will serve as a framework for easy and smart online buying solutions. EMVCo has developed reproduction requirements to enable all users compliant with EMV digital commerce solutions to use the Click to Pay icon, which was created to promote globally interoperable EMV digital commerce payments.

The Change: Visa's digital commerce solution, Visa Checkout, is changing to EMVCo's Secure Remote Commerce Solution called **Click to Pay**. Visa rules were updated to replace Visa Checkout with Click to Pay in October 2020 with the applications of the Visa Checkout mark being removed and replaced with the updated solution.

The Impact:

EMVCo Click to Pay
The Click to Pay icon (owned by EMVCo and licensed to Visa) may be used along with network branding to let consumers know that a merchant is enabled to provide a faster, more secure and seamless digital checkout experience.

Once enabled for the Click to Pay digital solution, merchants and other SRC participants should advertise the ability to simplify digital commerce using the Click to Pay icon. Merchants should discontinue using Visa Checkout in all digital applications for payment transactions.

Branding
Effective January 2021, merchants will be required to fully comply with Visa Product Brand Standards requirements for Click to Pay when using the icon or referencing Click to Pay in marketing or other materials. Visa will no longer support the Visa Checkout brand.

Examples of the Click to Pay icon and network branding:

The Timing: Effective Immediately

[REMINDER] Visa Reminds of Proper Credential-on-File Visa Brand Marks

CNP/eComm

The Change: In 2017, Visa introduced the updated Visa Brand Marks (solid Visa Blue against a white card shape or solid white against a Visa Blue card shape) to be used for credential-on-file (COF), stored credential or online transactions. Merchants were given until April 2018, to implement the COF Visa marks.

In a recent Visa audit of e-commerce merchants globally, it was determined that nearly 50% of merchants are still displaying outdated versions of Visa Brand Marks (Visa Blue and Visa Gold wing).

The Impact: Online merchants must immediately implement either version of the new Visa COF mark in their stored credential/COF/online checkout locations as illustrated below.

New COF Visa Marks for Immediate Implementation

Outdated Mark for Immediate Removal

The Timing: March 31, 2021

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

CP/CNP/eComm

The Change: Through a series of 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 assistance 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 Updates Dynamic Currency Conversion (DCC) Rules for Card-Present POS Transactions

CP

The Change: Visa is updating cardholder verification method (CVM) rules requirements for Dynamic Currency Conversion (DCC) transactions and is announcing plan to phase out paper-based DCC disclosures.

The Impact:

New DCC CVM Requirements – VEPS – October 17, 2020

Due to increased usage of contactless payment methods, signature optional changes and increases in Visa Easy Payment Service (VEPS) limits due to COVID-19, Visa is clarifying rules to allow DCC for a VEPS transactions (i.e., without CVM).

All other DCC requirements must be met; presenting the required DCC disclosures to the cardholder, ensuring the cardholder understands DCC availability, and providing them the option whether to use or not.

The POS is to be set to 'decline' as the default choice if the cardholder does not choose to accept DCC. Merchants should not process transactions as DCC to cardholders who tap and go without making the choice to accept DCC.

Paper-Based DCC Disclosure and Active Cardholder Choice

Visa Rules have been updated for DCC in a card present environment to prohibit the deployment of paper-based DCC solutions where disclosures are provided on a transaction receipt, and/or where the cardholder makes a choice for DCC by checking a box on a transaction receipt.

These updates will help to reduce the level of non-compliant DCC and make for a more frictionless cardholder experience at the POS.

Miscellaneous DCC Rule Updates – April 17, 2021

To ensure accurate DCC monitoring and reporting, Visa is clarifying rules to state that the DCC indicator must not be populated in the clearing record if DCC was declined by the cardholder.

The sales tax rebate rule has been corrected to clarify how a sales tax rebate must be processed, determined by who the original seller of the goods or services is.

DCC Reminders - Avoiding Non-Compliance

- DCC must always be offered in the correct cardholder billing currency.
- Consumer debit or prepaid cards with the Visa Multi-Currency Solution and consumer travel prepaid cards are ineligible.
- The DCC guide, an account billing currency file, is available from Visa and provides billing currency for each account range and identifies the DCC-ineligible account ranges.

Effective Date:

October 17, 2020	DCC permitted without CVM on Visa Easy Payment Service (VEPS) transactions
April 17, 2021	New DCC solutions or terminals may no longer be paper-based
October 15, 2022	Paper-based solution eliminated and must be replaced by DCC disclosure and choice on a customer-facing screen or handheld terminal

[REMINDER] Visa Updates, Expands, and Clarifies Digital Wallet Policy **CP/CNP**

The Change: Visa is updating rules to provide greater clarity globally for clients deploying or partnering with digital wallets.

The Impact:

Stored Value Digital Wallet

There are several digital wallets that operate as neither Pass-Through nor Staged Digital Wallets. Therefore, Visa has created a third digital wallet category to establish baseline standards for clients working with these wallets.

Stored Value Digital Wallets are wallets that assign a separate 'account' to the customer, which the customer then pre-loads with funds using the Visa payment credential to then complete transactions using the wallet. Usage of the wallet is limited to the available funds in the digital wallet account.

May either or both:

- Support a proprietary multi-retailer acceptance network and/or person-to-person (P2P) functionality, where payments are accepted via the digital wallet's own brand
- Partner with an issuer to assign a Visa or non-Visa open-loop payment network product (e.g., a general-purpose payment network prepaid credential) to the 'front' of the wallet's account to allow the customer to use the wallet's stored funds anywhere Visa or the non-Visa open-loop payment network is accepted.

May enable manual and/or automated reloads of the wallet's balance, where automated reloads may be:

- Established at a regular frequency (e.g., reload $50 on the 1st of every month) or
- Triggered by a balance threshold, based on customer usage (e.g., reload $50 whenever the balance reaches$10).

  Note: Stored Value Digital Wallet accounts must always hold a balance of pre-loaded funds to be able to transact.

- Must not support 'back-to-back' funding transactions

Back-to-Back Funding Definition

Rules-Driven Load: If the load is a single, predetermined amount, it is not defined as back-to-back funding.

Live/Real-Time/Purchase-Driven Loads: If the automated reload is triggered by the attempted transaction amount (in full or part), including multiple reloads of a predetermined/default amount to increase the wallet's balance to cover the transaction amount, these are considered back-to-back funding transactions.

[REMINDER] Visa Updates, Expands, and Clarifies Digital Wallet Policy (cont.) CP

Back-to-Back Funding Prohibitions

Effective April 17, 2021, Visa is clarifying its policy to state back-to-back funding is prohibited for all use cases and payment flows, except those facilitated by registered and approved Staged Digital Wallets when completing transactions within the proprietary Staged Digital Wallet network.

Due to the potential risks that back-to-back funding introduces when combined with 'open-loop' payments (potential fraud, high-risk merchant, anti-terrorism and anti-money laundering concerns), the prohibition includes but is not limited to Stored Value Digital Wallets and issuers/operators of Visa or non-Visa general purpose prepaid portfolios that may be funded by a Visa payment credential.

Effective date: April 17, 2021

DIGITAL WALLET COMPARISON (Not an all-inclusive list)

	Requirement	Pass-Through Digital Wallet (The 'Pays'- Samsung, Google, Applepay)	Stored Value Digital Wallet (April 17, 2021)	Staged Digital Wallet (Paypal)
Acquirer and Contract Requirements	Additional acquirer capitalization standard	No	No	Yes
	DWO registration and approval with Visa[2]	No	No[3]	Yes[3]
	DWO contract with acquirer	No	Yes	Yes
	DWO contract with sellers	No	No	Yes
	Direct seller contract with acquirer	Yes	No	No
	Eligible to be acquired by payment facilitators or other DWOs?	Yes, for transactions processed through payment facilitators No, for other DWOs	No	No
	Seller located in acquirer country?	All applicable seller/acquirer combinations	DWO must located in acquirer's country;4 seller may be in another country	DWO and seller must be located in acquirer's country5
	Merchant location determined by	Seller	DWO	DWO
Acceptance Brand	Acceptance mark at seller's POS, website or mobile application	Visa	DWO's brand Visa or other general-purpose payment network if the wallet is 'fronted' by a Visa payment network credential (e.g., prepaid card)	DWO's brand only
Transaction Responsibility	Who is the merchant of record?	Seller	DWO	DWO
	Name in transaction record and customer statement	Seller	DWO	Pre-load: DWO Name Back-to-back funding: DWO*Seller Name
	Dispute resolution provided by	Seller	DWO	DWO

Transaction Processing	Unique identifier included in transactions	No	No	Merchant Verification Value (MVV)
	Transaction Type	Purchase	Account Funding Transaction (AFT)	Pre-load: Account Funding Transaction (AFT) Back-to-back funding transaction: Purchase
	Business Application Identifier (BAI)	None	Funds Transfer (FT)6	Wallet Transfer (WT)
	Merchant Category Code (MCC)	Seller's line of business	One of the following: MCC 6540-Non-Financial Institutions – Stored Value Card Purchase/Load, or digital wallets with most transactions through a proprietary multi-retailer network MCC 4829-Money Transfer, for digital wallets with most transactions as person-to person (P2P) MCC 6012-Financial Institutions-Merchandise, Services, and Debt Repayment, if eligible If the DWO enables transactions with certain high-risk sellers, (e.g., gambling), seller MCC[3]	Pre-load: MCC 6051 Back-to-back funding transaction: Seller's line of business If the DWO enables transactions with certain high-risk sellers, (e.g., gambling), seller MCC[3]
Additional Functionality	Back-to-back funding allowed	N/A; does not store funds	No	Yes
	Visa/non-Visa general purpose payment network product at the 'front' of the DWO account (e.g., a prepaid credential)	N/A; transactions facilitated using digital tokens representing underlying Visa credential	Yes	No
	Eligible to become a Visa token requestor[2]	Yes	Yes	Yes
Pricing	Entity-base Visa transaction pricing	No	No	Yes, USD 0.10 per transaction 7

2 If the DWO intends to be a token requestor, the DWO must be registered with Visa Token Service.
3 If the DWO enables transactions with certain high-risk sellers, the DWO and each high-risk seller must be registered with Visa under Visa's High-Brand Risk program.
4 In the Europe region, the acquirer and Stored Value Digital Wallet operator may be in different countries within Europe. Consult the Visa Rules for more information.
5 In the Europe region, the acquirer, Staged Digital Wallet operator and seller may be in different countries within Europe. Consult the Visa Rules for more information.
6 The BAI value of WT may be used in Visa's AP region until 14 April 2023.
7 Excluding India and the Europe region.
Visa is also creating a Digital Wallet Companion Guide to help clients and partners apply Visa's policies for supporting different types of digital wallets.

[REMINDER] Visa Fraud Monitoring Program Extended to Help Mitigate Counterfeit Fraud at U.S. Automated Fuel Dispensers (AFD)

CP

The Change: As previously communicated, Visa has extended the U.S. Automated Fuel Dispenser (AFD) EMV liability shift until April 2021. In addition, Visa has announced that they are also extending the Visa Fraud Monitoring Program for automated fuel dispensers (VFMP-AFD) through **April 30, 2021**.

The Visa Fraud Monitoring Program for AFD (VFMP-AFD) identifies U.S. AFD merchant locations that experience excessive counterfeit fraud.

VFMP-AFD Monitoring:

- Visa will monitor AFD counterfeit transaction activity posted through April 16, 2021.
- The program will end in May 2021, following the processing of April 1–April 16, 2021 transaction activity.
- After the conclusion of the monitoring program, AFDs will revert to monitoring under the terms of the Standard/Excessive VFMP per the current Visa Rules.
- Merchant outlets that have excessive fraud should use tools such as address verification, velocity monitoring, etc. to assist in mitigating fraud.

[UPDATE] 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 (ECI) 05 (Issuer participates)	Merchant ***receives*** fraud-related dispute protection	NO CHANGE
Attempted Authentication - Electronic Commerce Indicator (ECI) 06 (Issuer participates)	Merchant ***receives*** fraud-related dispute protection	NO CHANGE
Attempted authentication (ECI) 06 (Issuer does not participate)	Fraud liability with Issuer	Fraud liability with merchant (ECI) 07

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

[REMINDER] Visa Updates Sunset Dates for Expired PIN Entry Devices CP

The Program: Visa requires that all organizations that accept cardholder PINs use an approved PIN Entry Device (PED) that has been evaluated and approved by the Payment Card Industry Security Standards Council (PCI SSC) and is listed on the Approved PIN Transaction Security (PTS) Devices section of the PCI SSC website.

The Change: Expired devices can become vulnerable to attacks, as they may not be able to support security code updates or patches to address malware. In an effort to reduce these potential attacks, Visa has updated its PIN Entry Device sunset and replacement mandates for expired POS PIN entry and ATM devices and introduced new sunset dates for expired Host Security Modules (HSMs).

These modifications will help to establish the framework for advances in cryptographic changes as well as keeping the payments ecosystem safe.

The Impact: Updating sunset and replacement dates Visa strives to:

- Clarify Visa requirements for replacement of PCI PEDs and HSMs
- Position the payment ecosystem to better defend against modern-day attacks
- Set the foundation for advances in cryptographic changes for PEDs
- Ensure payment participants remain vigilant about PIN security

Device	PCI Device Expiration Date	Revised Sunset Date	Action Required After Sunset Date
Devices never lab-evaluated by Visa or PCI	N/A	December 31, 2022	• Sunset / retire devices • Replacement required
Pre-PCI Approved Encrypting PIN Pad (EPP) Devices	N/A	December 31, 2022	• Sunset / retire devices • Replacement required
PCI PED or EPP PED V1.x	April 30, 2014	December 31, 2022	• Sunset / retire devices • Replacement required
PCI PED or EPP PED V2.x	April 30, 2017	December 31, 2022	Clear-key injection is prohibited
		December 31, 2027	• Sunset / retire devices • Replacement required
PCI PTS Point of Interaction (POI) V3.X1	April 30, 2020	December 31, 2030	• Sunset / retire devices • Replacement required
All versions of PCI HSMs	V1.0— April 30, 2019 V2.0— April 30, 2022 V3.0— April 30, 2026	10 years after the version's PCI HSM security approval expires	Replacement required

[1] PCI security approval for Version 3.x devices expires 30 April 2020.

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

CP/CP/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"
```

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

CP/CP/eComm

eComm/VAP platform

- Development is underway
- We have identified four response codes that are not currently mapped to an eComm 3-digit response code.
- Because the new response codes will be mapped to existing eComm 3-digit response codes there are no coding changes required by merchants.
  - The four response codes are as follows:
    - 01 (refer to issuer)
    - 02 (refer to card issuer, special condition)
    - R1 (revocation of authorization order)
    - R3 (revocation of authorizations).

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.

Effective April 17, 2021

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.

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

CP/CP/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.

Data Consistency

Visa is introducing a fee that will apply when a merchant / acquirer resubmits an authorization with changed data elements following an issuer decline. Merchants/Acquirers will not be permitted to change any data elements in an authorization reattempt; those elements will include but are not limited to:

- Merchant country
- POS condition code
- POS environment field
- Merchant Category Code
- Electronic Commerce Indicator (ECI)
- POS entry mode

U.S. | Canada | LAC | Europe OCTOBER 1, 2021		
Transaction Criteria	**Domestic Fee**	**Cross Border Fee**
Data Consistency	USD 0.10	USD 0.15 USD 0.25 (**LAC**)

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

[REMINDER] Visa 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, Visa is introducing a new indicator to uniquely identify transactions that are stored and submitted once their system is back online.

The Impact: Visa will require support of a new authorization indicator (existing field 63.3) to identify deferred (store and forward) authorizations (value of 5206).

- Deferred authorizations must be obtained within one (1) day of the transaction date*

  * Transaction date is the date when the goods/services were provided. Visa understands there will be exceptions (e.g., natural disasters, etc.) where the submission of the deferred authorization may extend beyond one day.

- MCCs 4111 (Local and Suburban Commuter Passenger Transportation including Ferries), 4122 (Passenger Railways) or 4131 (Bus Lines) must obtain an authorization within four (4) days of the transaction date

The Timing: Visa has revised the effective dates for support of the Deferred Authorization Indicator:

- **April 16, 2021** – **mandatory for merchants**

[NEW] Discover Increases Transaction Limit for Transit in Canada, Mexico, and the Caribbean

CP

The Program: Currently, the aggregated transaction limit for Mexico, Canada, and the Caribbean is $15 for contactless chip.

The Change: Discover will increase the aggregated transactions limit from $15 to $35. Discover will also update the dispute rules to reflect this change.

The Impact: Eligible transit merchants may obtain an authorization for $1.00, or one unit of local currency for aggregated transit transactions outside of the U.S. and aggregate multiple fare transactions into a single transaction up to the aggregated transaction amount limit established by Discover.

The following transit MCCs are permitted to perform transaction aggregation:

- 4111 (Local and Suburban commuter Passenger Transportation, Including Ferries)
- 4112 (Passenger Railways)
- 4131 (Bus Lines)

Note: The aggregated transit transaction limit remains $15 for aggregated transit transactions in the US.

[REMINDER] Discover Reminder for Customer Related Data in Payment Account Reference (PAR) Transactions

CP/CNP/eComm

The Program: PAR is the primary mechanism to achieve a consolidated view of transactions associated with a PAN (e.g., phone, PC, tablet). Loyalty programs, customer support, and merchant systems that are responsible for monitoring fraud analytics such as limits and thresholds and those needed to meet regulatory and anti-money laundering requirements, will benefit from the visibility enabled by using the PAR.

The Impact: Discover is reminding both merchants and acquirers that the Customer Related Data field the PAR tag 01 are used for both PAN and token transactions.

The Timing: Effective immediately.

[REMINDER] Discover Increases Threshold for Card Present Contactless Transactions without CDCVM

CP

The Change: Due to COVID-19, Discover has increasing the threshold amount for card present contactless card sales or credits that may be conducted without a PIN or Consumer Device Card Verification Method (CDCVM).

The Impact: This increase should allow for a more expedited checkout process and minimize contact with POS devices.

Device	Action Required After Sunset Date
United States	100 USD
Mexico	50 USD or equivalent Originating Currency
Other Authorized Jurisdictions	50 USD or equivalent Originating Currency

*Subject to applicable requirements of law

Exclusions: Merchants operating in the MCCs below are not eligible for card present card sales and credits with no PIN entry or CDCVM.

MCC	MCC Name
4829	Money Transfer – Non-Financial Institution
6010	Member Financial Institution – Manual Cash Disbursements
6011	Member Financial Institution – Automated Cash Disbursements
6050	Quasi Cash – Member Financial Institution
6051	Quasi Cash – Non-Financial Institution
6531	Payment Service Provider – Money Transfer for a Purchase
6532	Payment Service Provider – Member Financial Institution – Payment Transaction
6533	Payment Service Provider – Merchant – Payment Transaction
6534	Money Transfer – Member Financial Institution
7802 (New)	Government Licensed Horse/Dog Racing
7995	Betting (e.g., sportsbook/fantasy/social gaming; when regulated and not covered by other

[REMINDER] Discover Updates to Credential on File (COF) Framework for Merchant Initiated Transactions (MIT)

CP/CNP/eComm

The Change: Discover is expanding their Credential on File (COF) framework to include additional types of Merchant Initiated Transactions (MIT) and is defining transaction level requirements.

The Impact: These changes are mandated for PANs and Discover network tokens. The following Merchant Initiated Transactions (MIT) must be identified with the status indicator value as outlined below:

Discover Merchant-Initiated Transaction		
MIT Type	**New Status Indicator Value**	**MIT Definition**
Delayed Card Sale	D	A card sale for an additional amount payable by the cardholder that is determined or applicable after the original card sale and service date (e.g., car rental or hotel damage)
Resubmission Card Sale	E	A resubmission of the authorization request and sales data where a merchant received a declined authorization response (such as insufficient funds or daily limits exceeded); and delivered goods or services to the cardholder
No-Show Charge	N	A card sale for a fee assessed by a merchant operating in lodging and car rental, such that if the cardholder does not cancel a reservation within the disclosed terms (e.g., hotel charge when the cardholder does not use the accommodation)
Installment Payment	S	A card sale in a series of one or more future card sales over a period agreed upon by the merchant and cardholder for a single purchase of goods or services
Unscheduled Payment	U	A card sale for a fixed or variable amount, agreed upon by the merchant and cardholder, that does not occur on a scheduled or regularly occurring transaction date, (e.g., snow removal service on an as-needed basis, automatic refill of a balance on a pre-paid mobile phone subscription, or extra toll charges)

Existing Status Indicator Value Reminder	
MIT Type	**Value**
Recurring	R
Incremental	I
Partial Ship	P
Reauthorization	A

[REMINDER] Discover Updates to Credential on File (COF) Framework for Merchant Initiated Transactions (MIT) (cont.)

CP/CNP/eComm

Transaction ID Requirements
Merchants must pass the transaction identifier in PAN and payment token merchant-Initiated authorization requests, which include:

- Incremental authorizations
- Recurring payments
- Partial shipment transactions
- No-Show Charge
- Re-authorizations transactions (e.g., use re-auth when authorization from issuer is no longer valid)
- Installment
- Unscheduled
- Delayed Card Sales
- Resubmission

POS Entry Mode Requirements
When applicable, Discover requires POS entry mode of 10 in authorization and settlement messages to identify credential on file (COF) transactions. Discover requires the POS entry mode 10 to be sent in subsequent COF transactions.

- Merchants are **required** to send POS entry mode of 10 in authorization and settlement messages for the following types of COF transactions: cardholder-initiated and the following MITs: delayed card sale, resubmission card sale, no-show charge, partial ship, incremental, and reauthorization.

- It is **optional** for other types of COF transactions (e.g., recurring, installment, **NEW:** unscheduled payments)

[REMINDER] JCB Expands Existing BIN Ranges

CP/CNP/eComm

The Change: JCB has announced they are expanding their BIN ranges.

The Impact: Merchants and partners should ensure all point of sale devices are able to identify, accept, and process the expanded BIN ranges.

New JCB 8-Digit BIN ranges

Start	End	Issuing Network
30880000	30949999	JCB
30960000	31029999	JCB
31120000	31209999	JCB
31580000	31599999	JCB
33370000	33499999	JCB

The Timing: The new BINs are expected to be in market **October 2022**.

American Express

[NEW] American Express Releases New Version of ExpressPay and Announces New Indicator for SoftPOS Transactions

CP/CNP/eComm

The Change: Expresspay is an EMV- based payment application that uses a contactless interface to communicate with a terminal. American Express has announced the release of version 4.0.3 of the Expresspay MPOS terminal format and a new field to properly identify SoftPOS transactions. (transactions that originated from a mobile device).

SoftPOS is a new 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 this new indicator will identify a contactless transaction as SoftPOS.

The Impact: In addition to the new 4.0.3 version of Expresspay, American Express is also requiring a new field to identify SoftPOS transactions. This field must be populated in the Terminal Classification Data Field and will be used to identify transactions that originated from a mobile device.

All merchants that use the Expresspay format should consider migrating to the new version and begin planning to support the new terminal classification data field. There will be four values used for identifying SoftPOS transactions that will be communicated soon.

There are no changes to the current POS DC requirements as SoftPOS transactions are considered contactless transactions.

[NEW] Shazam PINless Bill Pay MCC Eligibility Changes

CP/CNP/eComm

The Change: Shazam has announced changes to their Bill Payment Tiers. Bill Payment Interchange Fees are determined based on the category of their business (MCC) and the tier assigned to that category.

The Impact: Shazam is modifying the business categories assigned to these tiers as indicated in the table below:

TIER 1		
4784	Toll and Bridge Fees	New
TIER 2		
4111	Mass Transit	Moved from Tier 3 to Tier 2
4225	Public Warehousing & Storage	
4789	Transportation Services	
4816	Computer Network/Information Services	
5912	Mail-Order Pharmacy Co-Pays	
5963	Home Services Water Delivery	
7012	Timeshares	
7997	Clubs – Membership (Athletic, Recreation, Sports)	
8011	Healthcare – Medical Doctors	
8062	Healthcare – Hospital Payments	
8071	Healthcare – Laboratories & Testing	
8099	Healthcare – Medical Services	
8660	Religious Organizations	
8661	Religious Organizations	
4928	Money Orders – Wire Transfer	New
5045	Computers/Peripheral Equipment and Software	
5047	Medical, Dental Ophthalmic, Hospital Equipment and Supplies	
5541	Service Stations (With or Without Ancillary Services)	
5542	Automated Fuel Dispensers	
5719	Miscellaneous Home Furniture Specialty Stores	
5815	Digital Goods: Books, Movies, Music	
5816	Digital Goods: Games	
5817	Digital Goods: Applications (Excludes Games)	
5818	Digital Goods: Large Digital Goods Merchant & Multi-Category	
TIER 3		
4899	Cable and Other Pay Television	Moved from Tier 2 to Tier 3
5960	Direct Marketing – Insurance Services	
6300	Insurance Underwriting, Premiums	
6513	Apartment Building Operators	
8220	Colleges, Universities	
8299	Educational Services	
9211	Court Costs, including Alimony & Child Support	
9399	Government Services	
4814	Telecommunications (includes Prepaid)	New
5311	Department Stores	
6010	Financial Institutions, Manual Cash Disbursements	
6141	Personal Credit Institutions	
6153	Short Term Business Credit Institutions	
6159	Miscellaneous Business Credit Institutions	
6162	Mortgage Bankers & Loan Correspondents	
7298	Health and Beauty Spas	
7999	Recreation Service not elsewhere classified	
8931	Accounting, Auditing, Bookkeeping	
8999	Professional Services not elsewhere classified	

[NEW] NYCE PINless Bill Pay MCC Eligibility Changes

CP/CNP/eComm

The Change: NYCE has announced changes to their Bill Payment Categories. Bill Payment Interchange Fees are determined based on the category of their business (MCC) and the tier assigned to that category.

The Impact: NYCE is modifying the business categories assigned to these tiers as indicated in the table below:

BILL PAY TIER	MCC	OLD BILL PAYMENT CATEGORIES	NEW BILL PAYMENT CATEGORIES	NET CHANGE
UTILITIES				
Tier 1	4900	Utility	Utility	No change
FINANCIAL SERVICES AND PROPERTY SERVICES				
Tier 2	6012, 6051, 6531	Collections (Financial Services only); Secured/Unsecured Loans	Collections (Financial Services Only); Secured/Unsecured Loans	No Change
Tier 2	7841	Digital Media Subscriptions	N/A	Removed
Tier 2	9211, 9222, 9311, 9399	Governmental Services	N/A	Moved from Tier 2 to Tier 3
Tier 2	7997	Health Club Membership	N/A	Removed
Tier 2	8011, 8021, 8031, 8041, 8042, 8043, 8043, 8049, 8055, 8099	Healthcare Providers	N/A	Removed
Tier 2	7342,	Home Security	Home Security	No Change
Tier 2	4816	Internet Service Providers	N/A	Moved from Tier 2 to Tier 3
Tier 2	7349	Property Maintenance	Property Maintenance	No Change
Tier 2	7393	Pest Control	Pest Control	No Change
Tier 2	4111, 4112, 4784, 4789	Mass Transit and Parking	N/A	Removed
Tier 2	7273	Online Dating Services	N/A	Removed
Tier 2	5912	Prescription Refills	N/A	Removed
Tier 2	6513	Rent	Rent	No Change
Tier 2	4225	Storage Rental	Storage Rental	No Change
COMMUNICATION, EDUCATION, INSURANCE AND GOVERNMENT SERVICES				
Tier 3	4814	Telecom (Telephone/Prepaid Phone)	Telecom (Telephone/Prepaid Phone)	No Change
Tier 3	4899	Cable/Satellite; Radio; TV	Cable/Satellite, Radio, TV	No Change
Tier 3	5960, 6300	Insurance Services	Insurance Services	No Change
Tier 3	8211, 8220, 8241, 8244, 8249, 8299	Educational Services	Educational Services	No Change
Tier 3	4816	N/A	Internet Service Providers	Moved from Tier 2 to Tier 3
Tier 3	8211, 9222, 9311, 9399	N/A	Governmental Services	Moved from Tier 2 to Tier 3
Tier 3	4215	Overnight Shipping	N/A	Removed

If the business category of a Terminal Participant is not listed in one of the Bill Payment tiers above, the Terminal Participant is considered an eCommerce merchant.

The Timing: These changes apply to new business, effective February 1, 2021. Existing Terminal Participants processing Bill Payment transactions will not be affected.