# Merchant Network Updates Winter 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.

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

**The Program**: To ensure better visibility to the cardholder that their refund is in process, and to reduce refund-related customer service burdens on merchants, acquirers, and issuers, the brands have communicated the following refund authorization support and effective dates.

### February 2021 UPDATES

#### Implementing Return Authorization Support
**Visa / Mastercard / Discover**

**CORE**
Worldpay from FIS enabled the code to send return authorizations to Visa, Mastercard, and Discover for all core merchants effective February 2, 2021

**VAP**
Visa return transactions from customers utilizing our VAP platform are also now being sent for authorization. Return authorization code for Mastercard and Discover are scheduled to be turned on in April 2021.

**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.**

**Reminders**
- Merchants should include the expiration date in return authorization messages for all card types to prevent issuer decline.
- The expiration date should 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**
- Merchants are reminded that *response code '85' is a valid approval response* and to support this value accordingly.
- Transactions that originated as Quasi Cash or Account Funding cannot submit credit refunds.

**Mastercard**
- Chargebacks associated with no authorization for returns has been delayed until further notice.

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

### Reminder – Network Fees

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.
- **MasterCard:** The NABU fee ($0.0195) will **not** apply to return transactions submitted for authorization.
- **Visa:** Integrity fees ($0.10) assessed to returns without a valid authorization.

### Important Dates by Brand

| Brand | Mandated Effective Dates | Exclusions | Proc Code Required | Chargebacks | Fees |
|---|---|---|---|---|---|
| Visa | **October 19, 2019**<br>• U.S.<br>• Canada<br>• LAC<br>**July 2020**<br>• AP<br>• CEMEA<br>**April 2022**<br>• Europe<br>○ UK<br>○ Republic of Ireland | Airlines (MCCs 3000–3350 and 4511) | 20 | July 18, 2020<br>(*excluding Europe*) | **July 1, 2021** |
| Mastercard | **July 17, 2020***<br>*mandated for Acquirers optional for merchants | Airlines (MCCs 3000–3350 and 4511) | 20 | **Chargebacks for returns date has been delayed. New date TBD** | |
| Discover | **July 17, 2020** | Airlines (MCCs 3000–3350 and 4511) | 20 | July 17, 2020 | |

## [REMINDER] Subscription Merchants Offering Free Trials or Introductory Promotions

**CNP/eComm**

**The Change:** Visa and Mastercard have published new rules for subscription merchants that offer free trials or introductory promotions in response to complaints from regulators, issuers and cardholders regarding deceptive practices.

Update: Visa has revised the Enhanced Descriptor Policy for Subscription Merchants Offering Free Trials or Introductory Promotions.

### Mastercard

Mastercard has published new rules that focus on high risk negative option billing merchants. Negative option billing refers to a business practice where a **merchant provides a free trial or sample of goods or services, requires a credit card upon sign-up and then bills the customer in the future unless they proactively cancel** with the merchant. Mastercard's new rules are applicable to all negative option merchants selling physical merchandise, with a focus on nutraceuticals.

### Visa

Visa's focus is on any business model that provides free trials or introductory promotions. Although these merchants offer free trials or introductory promotions, they may not be a negative option merchant.

### Revised Payment Network Rules

Mastercard and Visa have published new rules and criteria regarding these merchant types as outlined by brand in the table below:

| Subscription Merchants | | |
|---|---|---|
| **Requirements** | **Mastercard (April 2019)** | **Visa (April 2020)** |
| MCC | Specific to MCC 5968 (Direct Marketing- Continuity/Subscription Merchant) | Not MCC specific |
| Merchant Business Model | Merchants who collect payment card information at the time of signing up customers for full subscriptions through **free trial offer or introductory promotions AND sell physical goods** | Merchants who collect payment card information at the time of signing up customers for full subscriptions through **free trial offer or introductory promotions (includes physical and digital goods)** |
| Transaction Type | CNP (eCommerce and MOTO) | CNP (eCommerce and MOTO) |
| Recurring Payments | Recurring payments, same acquirer: Transaction must be processed under the same merchant ID and merchant name that was used for the initial payment transaction | Recurring transactions: Identify the first transaction as Recurring, even if it's not the "full" amount |
| Registration | Merchants must be registered by the acquirer through the Merchant Registration Program | |
| Unique Descriptors | | Need to add "trial, free trial, or trial period" to the end of the merchant name so that it is within the transaction and displayed on the cardholder statement.<br><br>Merchants do not have to add the enhanced descriptor to the merchant name field as long as the merchant uses transaction-specific details (for example, universal resource locator |

| Subscription Merchants | | |
|---|---|---|
| **Requirements** | **Mastercard (April 2019)** | **Visa (April 2020)** |
| | | [URL] or order number) to help the cardholder identify that their trial period, discounted introductory offer or promotional period has ended, and that the regular price now applies for the subscription.<br><br>**It is now optional to support the unique descriptors for free trials / discounted promotions.** |
| Transaction Compliance Monitoring (By Worldpay) | Ensure only one MID per merchant is assigned to prevent Load balancing | • Use of MCC(s)<br>• Recurring Indicator<br>• Statement descriptor<br>• Monitoring for excessive disputes & fraud reporting |
| Merchant Compliance Monitoring (By Network) | TBA | Mystery Shopping:<br>• Appropriate disclosures<br>• Notifications<br>• Cancellation process |
| Chargeback Liability | | Merchants may be liable for chargebacks if the cardholder was not properly notified of future billing.<br>Existing dispute conditions for cancelled recurring transactions will continue to apply. |
| Trial Period | The trial period must begin on the date the product is received by the cardholder | At the time of enrollment, merchants must require the cardholder to enter an ongoing subscription service for recurring payments.<br><br>Merchants must send an electronic copy (email or text) of the terms and conditions of the subscription service to the cardholder even if no amount is due:<br><br>• Start date of subscription<br>• Details of goods/services<br>• Ongoing transaction amount and billing frequency/date<br>• Link or other simple mechanism to enable the cardholder to easily cancel any subsequent transactions online |
| eCommerce merchants | Card acceptor name must include the website URL where the cardholder requested the product.<br><br>Merchant's website must display a customer service phone number on the website maintenance page for periods in which the website Is offline (e.g., software updates, scheduled maintenance, or technical difficulties) | |
| MoTo merchants | Customer service phone number must contain a number that is valid for the cardholder to contact the merchant and must be accessible by all consumers worldwide | |

| Subscription Merchants | | |
|---|---|---|
| **Requirements** | **Mastercard (April 2019)** | **Visa (April 2020)** |
| Cancellation Procedures | • Must provide a direct link to an online cancellation procedure for recurring payment transactions on the website where the cardholder made the initial purchase.<br><br>• Merchant must send written confirmation to the cardholder when the cardholder's trial period and/or high-risk negative option billing plan has been canceled | Online cancellation to apply regardless of how the cardholder originally signed up (e.g. door-to-door sales, pop-up store in a shopping mall, SMS/text from a TV ad). Should be like "unsubscribing" from an email distribution list.<br><br>Note: This rule is already in effect for recurring subscriptions in the Europe region |
| After trial period ends | but prior to any additional payments are made by the cardholder, the merchant must perform the following:<br><br>• Provide the cardholder with the payment transaction amount, payment transaction date, merchant name as it will appear on the cardholder's statement, and instructions for cancelling the subscription at the cardholder's choice<br><br>• Request and obtain the cardholder's consent for the payment amount before submitting an authorization request. Consent can be obtained via e-mail, telephone or text. | Merchants must provide electronic notification at least 7 days before initiating a new transaction if:<br><br>• A trial period, introductory offer or promotional period has ended<br>• The nature of the agreement has changed e.g. transaction amount or frequency<br><br>Note: This rule is already in effect for recurring subscriptions in the Europe region |
| Receipts | Merchant must send a receipt to the cardholder by e-mail or another electronic method (e.g., text message) each time the merchant attempts to authorize the transaction.<br><br>The receipt sent the cardholder must also contain instruction on how the cardholder can cancel the subscription service or recurring billing<br><br>If a merchant creates a receipt for authorization transaction attempt that was declined, the reason for the decline must be included | Merchants must disclose the following on transaction receipts upon establishment of the agreement:<br><br>• Length of trial period, introductory off or promotional period, including clear disclosure that the cardholder will be charged unless the cardholder takes steps to cancel any subsequent transactions<br><br>• Transaction amount and date for the initial transaction (even if no amount is due) and for subsequent recurring transactions<br><br>• Link or other simple mechanism to enable the cardholder to easily cancel any subsequent transactions online via SMS/text message |

- As a result of these new rules FIS will not board new high-risk negative option billing merchants.
- Any subscription merchants impacted by these changes should work with their relationship manager to confirm their compliance of these requirements.
- FIS continues to work with both Visa and Mastercard to ensure our subscription merchants comply with required criteria as defined by brand.

# EMV

## [NEW] 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] Mastercard Contactless EMV Terminal Entry Capability (TEC) Value Requirement CP

**The Change:** Mastercard requires a unique TEC value of '8' to identify Mastercard Contactless EMV transactions.

**The Impact:** Effective January 1, 2021 any merchant newly certifying for contactless EMV or recertifying must code to send the required Mastercard TEC value of '8'.

## [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:

- **Visa / Interlink** has announced a delay in the EMV AFD liability shift date until **April 17, 2021.**
- **Mastercard / Maestro** has announced a delay in the EMV AFD liability shift date until **April 16, 2021.**
- **Discover** has announced a delay in the EMV AFD liability shift date until **April 16, 2021.**
- **American Express** has announced a delay in the EMV AFD liability shift date until **April 16, 2021**.
- **Voyager** has announced a delay in the EMV AFD liability shift date until **April 17, 2021**.
- **WEX** has maintained an EMV AFD liability shift of **October 2020.**
- PIN Debit Network, **ACCEL,** has announced a delay in the EMV AFD liability shift until **April 1, 2021.**
- PIN Debit Network, **STAR,** has announced a delay in the EMV AFD liability shift until **April 1, 2021.**
- PIN Debit Network, **CULIANCE,** has announced a delay in the EMV AFD liability shift until **April 16, 2021.**
- PIN Debit Network, **JEANIE,** has announced a delay in the EMV AFD liability shift until **April 16, 2021.**
- PIN Debit Network, **NYCE,** has announced a delay in the EMV AFD liability shift until **April 16, 2021.**
- PIN Debit Network, **AFFN**, has announced a delay in the EMV AFD liability shift date until **April 17, 2021**.
- PIN Debit Network, **PULSE**, has announced a delay in the EMV AFD liability shift date until **April 19, 2021**.
- PIN Debit Network, **SHAZAM**, has announced a delay in the EMV AFD liability shift date until **April 2021**.

*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.**

## [UPDATE] 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

## [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 |
|---|---|---|
| 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 only |
| 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<br>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 will decline. |
| 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 |

## Asia Pacific

| Brand | Effective Date | Terminal Type |
|---|---|---|
| Visa | January 1, 2018 | All POS terminals in the ecosystem, remove MSD |
| Discover | August 23, 2018 | Terminals that are being upgraded must also support EMV contactless |
| Amex | December 31, 2018 | All POS terminals in the ecosystem must support EMV Contactless |
| Mastercard | October 12, 2018 | All newly deployed POS and CAT terminals (Excludes Mobile POS (MPOS)) must support EMV Contactless |
| Discover | October 18, 2019 | All newly deployed point-of-sale (POS) terminals that support contactless acceptance must only support EMV mode contactless transactions. Mag-stripe mode contactless must not be supported. |
| Mastercard | October 18, 2019 | All newly deployed MPOS terminals must also support EMV contactless |
| Mastercard | July 1, 2020 | Any new contactless-enabled terminal submitted for M-TIP testing must only support EMV mode contactless transactions |
| Mastercard | April 1, 2023 | All POS and CAT terminals. All contactless-enabled terminals must only support EMV mode contactless transactions. |

## Latin Caribbean and Caribbean Region

| Brand | Effective Date | Terminal Type |
|---|---|---|
| Discover | August 23, 2018 | Terminals that are being upgraded must also support EMV contactless |
| Amex | December 31, 2018 | All POS terminals in the ecosystem must also support EMV contactless |
| Discover | October 18, 2019 | All newly deployed point-of-sale (POS) terminals that support contactless acceptance must only support EMV mode contactless transactions. Mag-stripe mode contactless must not be supported. |
| Mastercard | October 18, 2019 | All newly deployed MPOS terminals must also support EMV contactless |
| Visa | October 19, 2019 | All POS terminals in the ecosystem must only support EMV contactless (remove MSD) |
| Mastercard | July 1, 2020 | Any new contactless-enabled terminal must only support EMV mode contactless transactions |
| Mastercard | October 20, 2020 | All contactless-enabled terminals must only support EMV mode contactless transactions |
| Visa | April 1, 2025 | All mobile devices, AFDs, ECRs and ATMs in the ecosystem must only support EMV contactless |

## [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.**<br><br>**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,<br>Service Providers |

## [REMINDER] 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.

**Background**

- Mastercard transactions will be downgraded to standard interchange rates if the TIC value does not match between the authorization response and settlement message, effective no earlier than April 2021.
- 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.
- Merchants should continue in their efforts to test and certify for support of the Mastercard TIC to avoid future interchange downgrades.

**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 |

### Reminders

- 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.

## [REMINDER] Mastercard Revises Pre-Arbitration Fees

**CP/CNP/eComm**

**The Program:** As previously announced, MasterCard eliminated second chargebacks in July 2020 and permitted issuers to send pre-arbitrations instead. A pre-arbitration may occur after a merchant represents a first chargeback.

**The Change:** Along with this change, MasterCard revised an existing pre-arbitration fee. The fee will be assessed to the merchant who receives the pre-arbitration as outlined below.

**The Impact:**

**Scenario 1**
The merchant receives a pre-arbitration and decides to accept it.

**Effective January 1, 2021:** This will create a debit for the disputed amount along with the $15.00 fee.

**Scenario 2**
The merchant receives a pre-arbitration and declines it or fails to respond.

The fee will be assessed to the issuer instead of the merchant; however, if the issuer escalates the dispute to arbitration and wins, the fee *($15.00 eff. 1/1/2021*) will be included in arbitration fees passed to the merchant.

## [NEW] 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

## [NEW] 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

## [NEW] 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

## [NEW] 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 |

## [NEW] 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.

## [NEW] 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<br>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<br>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<br>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)<br>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<br>MCC 4829-Money Transfer, for digital wallets with most transactions as person-to person (P2P)<br>MCC 6012-Financial Institutions-Merchandise, Services, and Debt Repayment, if eligible<br><br>If the DWO enables transactions with certain high-risk sellers, (e.g., gambling), seller MCC[3] | Pre-load: MCC 6051<br><br>Back-to-back funding transaction: Seller's line of business<br><br>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 Changes to VIP Response Source/Reason Code and Base II Authorization Source Code Field

**eComm/CNP/CP**

**The Change:** Visa has announced changes to the existing response source/reason code field and the base II authorization source code field to identify where an authorization originated. Visa's goal with this change is to help protect consumers, merchants, issuers and acquirers from evolving fraud trends. Visa is also making changes to the values allowed to be sent to Visa on settlement records. The updated values are outlined below.

**The Impact:** Visa will begin to return a new value of V (authorization obtained through Visa issuer or STIP) on all transactions that are authorized online through Visa's authorization system. A space is no longer a valid value for the authorization source code field.

Merchants must retain the VIP Response Source/Reason Code that was returned on all authorization responses and send in all settlement messages. If the merchant sends a Force Post transaction (e.g., authorization not obtained, authorization decline, or was authorized over the phone) they must send a valid authorization source code to avoid possible settlement rejects.

**Valid Authorization Source Code Values**

- 6 – Offline approval – POS device-generated
- 7 – Acquirer approved (not valid for merchant use)
- 9 – No authorization source code/non-authorized transaction
- B – Auth code provided by Visa Advisor Service
- E – Offline approval – authorization code manually entered
- F – CAFIS generated response (valid in Japan only)
- G – Issuer approval (valid in Japan only)
- N – No authorization code – below floor limit (not valid in the US region)
- L – Late clearing – authorization code previously obtained (settlement beyond 30 Days)
- V – Authorization obtained thorough Visa (issuer or STIP)

- Worldpay from FIS authorization and settlement systems can receive and accept any auth source code value

- Merchant authorization and settlement specs support the source code field. The merchant specs will be updated to contain a list of valid values.

**Deleted Values**

The following values are no longer valid for the authorization source code field. If an authorization code is obtained through a source other than Visa, merchants are required to indicate the source of the authorization code by providing a valid authorization source code in settlement messages.

- Space
- 8 – Acquirer approval: referral
- D – Referral: authorization code manually entered

**New Visa Return Reason Code AA- Card Recovery Bulletin**

If a transaction is not authorized through Visa and an authorization code or transaction identifier contains spaces in the settlement record, Visa will check to see if the PAN is listed on the card recovery bulletin (CRB). If it is found in the CRB, Visa will return using return reason code of 'AA" and the transaction cannot be resubmitted in settlement by the merchant or acquirer.

## [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.

## [REMINDER] Visa 3DS 1.0.2 Will No Longer Receive Fraud Liability Protection eComm

**The Program:** Merchants that authenticate transactions using 3DS 1.0.2 are generally protected from issuer card-not-present (CNP) fraud-related dispute claims.

**The Change:** Due to the upcoming transition from 3D-Secure (3DS) 1.0.2 to EMV 2.0, merchants using 1.0.2 will no longer be protected from issuer card-not-present fraud-related dispute claims. Fraud liability protection will no longer apply for fully authenticated or attempted authentication transactions.

**The Impact:** Effective October 17, 2021 Visa will remove fraud liability protection for merchants on **all** 3DS 1.0.2 fully authenticated or attempted authentication transactions (electronic commerce indicators [ECIs] 05 and 06, respectively).

Once this change has taken effect, Visa will continue to support 3DS 1.0.2 transaction processing, including the 3DS 1.0.2 Directory Server and 3DS 1.0.2 attempts processing.

Merchants will be able to submit transactions through 3DS 1.0.2 for cardholder authentication and will continue to receive ECI 05 and 06 in the authentication response with a Cardholder Authentication Verification Value (CAVV), however, these transactions will be open to fraud-related disputes raised by Issuers.

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

| Visa Secure Using 3DS 1.0.2 | Prior to October 17, 2021 | Effective October 17, 2021 |
|---|---|---|
| Fully Authenticated - Electronic Commerce Indicator (ECI) 05 | Merchant ***receives*** fraud-related dispute protection | Merchant is ***liable*** for fraud-related disputes |
| Attempted Authentication - Electronic Commerce Indicator (ECI) 06 | Merchant ***receives*** fraud-related dispute protection | Merchant is ***liable*** for fraud-related disputes |

## [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 | 31 December 2022 | • Sunset / retire devices<br>• Replacement required |
| Pre-PCI Approved Encrypting PIN Pad (EPP) Devices | N/A | 31 December 2022 | • Sunset / retire devices<br>• Replacement required |
| PCI PED or EPP PED V1.x | 30 April 2014 | 31 December 2022 | • Sunset / retire devices<br>• Replacement required |
| PCI PED or EPP PED V2.x | 30 April 2017 | 31 December 2022 | Clear-key injection is prohibited |
| 31 December 2027 | • Sunset / retire devices<br>• Replacement required | | |
| PCI PTS Point of Interaction (POI) V3.X1 | 30 April 2020 | 31 December 2030 | • Sunset / retire devices<br>• Replacement required |
| All versions of PCI HSMs | V1.0—30 April 2019<br>V2.0—30 April 2022<br>V3.0—30 April 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 can 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

**Effective through April 16, 2021**

**Decline Transaction Resubmissions**

Merchants that receive a decline response may resubmit the transaction for authorization for certain decline response codes, to receive an approval response.

| US, Europe, LAC and Canada Regions | |
|---|---|
| **Criteria** | **Current (through April 16th, 2021)** |
| **Merchant Type Permitted to Perform Retries (Resubmissions)** | All Merchant Types |
| **Number of Retries (Resubmissions)** | 15 retries within 30 days (excludes Debt Repayment and Transit) |
| | 3 retries within 14 days (Debt Repayment) |
| | 4 retries within 14 days (Transit) |

| Criteria | Current (through April 16th, 2021) |
|---|---|
| **Retry Permitted when the Decline Reason Code is:** | 19 (Re-enter transaction)<br>51 (Insufficient funds<br>59 (Suspected fraud)<br>61 (Exceeds withdrawal amount limits)<br>65 (Exceeds withdrawal frequency)<br>75 (Allowable PIN entry tries exceeded)<br>86 (ATM malfunction)<br>91 (Issuer or switch is inoperative)<br>96 (System malfunction)<br>N3 (Cash service not available)<br>N4 (Cash request exceeds issuer limit)<br>14 Invalid account number)<br>54 (Expired card)<br>55 (Incorrect PIN)<br>82 (Neg. Online CAM, dCVV, iCVV, or CVV results)<br>N7 (Decline for CVV2 failure [Visa])<br>1A Europe only- PIN data required |

| Criteria | Current (through April 16th, 2021) |
|---|---|
| **Retry NOT Permitted when the Decline Reason Code is: (Excludes Debt Repayment)** | 04 (Pickup card, no fraud)<br>07 (Pickup card, special conditions fraud account)<br>12 (Invalid transaction)<br>14 (Invalid account number, no such number)<br>15 (No such issuer, first 8 digits of account number do not relate to an issuing identifier)<br>41 (Pickup card, lost card)<br>43 (Pickup card, stolen card)<br>46 (Closed account – NEW effective 4/17/21)<br>57 (Transaction not permitted to cardholder)<br>62 (Restricted card)<br>78 (No account)<br>93 (Transaction cannot be completed)<br>R0 (Stop payment order)<br>R1 (Revocation of authorization order)<br>R3 (Revocation of all authorizations order) |
| **Retry NOT Permitted when the Decline Reason Code is: (Debt Repayment)** | 04 (Pickup card)<br>14 (Invalid account number (no such number))<br>41 (Pickup card (lost card))<br>43 (Pickup card (stolen card))<br>52 (No checking account)<br>57 (Transaction not permitted to cardholder)<br>75 (Allowable PIN-entry tries exceeded)<br>78 (Blocked, first used)<br>82 (Negative Online CAM, dCVV, iCVV, or CVV results) |

| AP & CEMEA Regions | |
|---|---|
| **Criteria** | **Current and Ongoing**<br>**(will NOT be impacted by Visa's rules on regrouping of decline codes and rule for retries)** |
| **Merchant Type** | Recurring<br>Installments Preauthorized Healthcare<br>Unscheduled credential on file |
| **Amount of Retries** | 4 retries within 16 days |
| **Retry Permitted when the Decline Reason Code is:** | 05 (Authorization declined) 51 (Insufficient funds)<br>61 (Exceeds withdrawal amount limits) 65 (Exceeds withdrawal frequency) |

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

CP/CP/eComm

### Visa Grouping of Decline Codes and Rules for Retries

**Effective April 17, 2021**

**NOTE**: Worldpay from FIS is evaluating our authorization response code mapping to determine the exact response codes that are provided to our merchants. 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.

**US, Europe, LAC and Canada 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 partyfraud
- New Fees will be introduced for non-compliance

**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.

Visa has created a solution that groups the decline response codes into four categories as outlined in the table below.

- A merchant may resubmit an authorization request following a decline for response codes listed in categories two, three and four only.
- Retries are limited to 15 in 30 days and applies to all transaction types, except transit.
- For transit transactions, resubmission retries are limited to 4 attempts in 14 days.

**Effective April 17, 2021 – Decline Response Code Use**

| 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.<br><br>As such, there are no circumstance in which the issuer will ever grant an approval. | 04 - Pickup card, no fraud<br>07 - Pickup card, special condition<br>12 - Invalid transaction<br>14[1] – Invalid account number (no such number)<br>15 - No such issuer, first 8 digits of account number do not relate to an issuing identifier<br>41 - Pickup card, lost card<br>43 - Pickup card, stolen card<br>46 - Closed Account (NEW effective 4/17/21)<br>57 - Transaction not permitted to cardholder<br>R0 - Stop payment order<br>R1 - Revocation of authorization order<br>R3 - Revocation of all authorizations order | 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.<br><br>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<br>19 - Re-enter transaction<br>51 - Not sufficient funds<br>59 - Suspected fraud<br>61 - Exceeds approval amount limit<br>62 - Restricted card (card invalid in region or country)<br>65 - Exceeds withdrawal frequency limit<br>75 - Allowable number of PIN-entry tries exceeded<br>78 - Blocked, first used - transaction from new cardholder, and card not properly unblocked (NEW effective 4/17/21 – Brazil only)<br>86 - Cannot verify PIN<br>91 - Issuer or switch is inoperative<br>93 - Transaction cannot be completed – violation of law<br>96 - System malfunction<br>N3 - Cash service not available<br>N4 - Cash request exceeds issuer or approved limit | Yes.<br><br>Limit retries to 15 in 30 days.<br><br>Exception: transit transactions, limit retries to 4 in 14 days |
| 3 | Data quality: revalidate payment information.<br><br>This category represents decline codes indicating the issuer cannot approve based on the details provided.<br><br>Examples include incorrect Card Verification Value 2 (CVV2) or expiration date. | 14[1] - Invalid account number, no such number<br>54 - Expired card or expiration date missing<br>55 - PIN incorrect or missing<br>6P- Verification data failed (NEW effective 4/17/21)<br>70 - PIN data required (Europe region only)<br>82 - Negative online CAM, CAVV, dcVV, iCVV, or CVV results or offline PIN authentication interrupted<br>1A - Additional customer authentication Required (Europe region only)<br>N7 - Decline for CVV2 Failure | Yes.<br><br>Limit retries to 15 in 30 days.<br><br>Exception: transit transactions, limit retries to 4 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.<br><br>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.<br>Limit retries to 15 in 30 days.<br><br>Exception: transit transactions, limit retries to 4 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
- Electronic commerce indicator (ECI)
- Merchant Category Code
- POS environment field
- POS entry mode

**Visa Fees and Effective Dates by Region for Non-Compliance**

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

| U.S. \| Canada \| Europe<br>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<br>APRIL 1, 2022 | | |
|---|---|---|
| **Transaction Criteria** | **Domestic Fee** | **Cross-border Fee** |
| Issuer will never approve - reattempt | USD 0.10 | USD 0.15 |

## [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**

## [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

## [REMINDER] American Express and Support of PAR

**CP/CNP/eComm**

**The Program:** The introduction of tokenization provided increased security of digital payments against fraud and data compromise; however, it created challenges for merchants and other stakeholders' value-added services that rely upon the PAN to identify the original account. To solve for these challenges, EMVCo has introduced a new transaction element called the Payment Account Reference (PAR) number.

A PAR is a value intended to allow acquirers and merchants to link tokenized transactions to transactions based on the originating PAN. The PAR is generated and linked to a PAN (and successor PANs associated with the underlying issuer customer account) and will also be associated with all affiliated Payment Tokens when a PAN is tokenized. PAR cannot be used to originate a transaction.

**The Impact:** Acquirers must be able to support the PAR for American Express transactions beginning April 2021. PAR is a fixed-length, 35-character alphanumeric value that links multiple tokenized payment methods (e.g., phone, PC, tablet) to the original card that was used. Worldpay from FIS merchant specs will be updated accordingly.

Merchants may choose to receive the PAR in their authorization responses.

- If planning to support, merchants must provide the certified request flag value in Amex data field 112, subfield 1. Flag value = C