

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<sup>®</sup>, Discover<sup>®</sup> Network, Mastercard<sup>®</sup> Worldwide and Visa<sup>®</sup> 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.

## EMV

---

### **[REMINDER] EMV Fraud Liability Shift Update for JCB and Union Pay**

CP

**The Change:** Discover Network, upon direction of both JCB and UnionPay, has communicated that both brands have updated their EMV fraud liability shift policies to include both JCB and UnionPay card transactions respectively. This fraud liability shift update applies to transactions acquired in the U.S. and processed via Discover Network and PULSE where a contact chip payment device is utilized and a counterfeit card using JCB or UnionPay BIN ranges were used to conduct the transaction.

#### **The Impact and Timing:**

##### **October 2019**

When a JCB or UnionPay contact chip payment device is utilized and a counterfeit card using the JCB or UnionPay BIN ranges was used to conduct the transaction at a POS or ATM, *except at an Automated Fuel Dispenser, in the U.S.*

##### **October 2020**

When a JCB or UnionPay contact chip payment device is utilized and a counterfeit card using the JCB or UnionPay BIN ranges was used to conduct the transaction at an Automated Fuel Dispenser in the U.S.

---

**[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.

Public keys are distributed to acquirers, merchants and solution providers to load into their terminals. Each of the brands' key sets is comprised of keys of varying lengths. 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 the point where it may become vulnerable to attacks, they will set that key's expiration date. While the individual brands are free to set their own expiration dates, they traditionally follow EMVCo's advice.

**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 expiry date of 12/31/2024
- 1984-bit keys have an anticipated expiry date of **12/31/2028**

**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] Mastercard M/Chip Requirements for Contactless Terminals**

---

**CP**

**The Change:** Mastercard will require all contactless terminals to support the Consumer Device Cardholder Verification Method (CDCVM) for transactions greater than the cardholder verification method (CVM) limit. In addition, terminals that operate as contactless CAT (Cardholder Activated Terminal) Level 1 must also support CDCVM. (Note: Effective January 1, 2016, new contactless terminals submitted for M-TIP testing must support CDCVM for transactions greater than the CVM limit.)

**The Impact:** Merchant contactless terminals must be able to support the Consumer Device Cardholder Verification Method (CDCVM) for transactions greater than the CVM limit. A **CDCVM is a Consumer Device Cardholder Verification Method** – A cardholder device that supports both a key pad or other customer input option and customer display, such as a mobile phone, that support CDCVM such as PIN, pattern, biometric solution, or another form of verification. Examples are the 'Pay' touch fingerprint IDs, which is used as the passcode to unlock the phone or payment application. Note: EMV mode terminals that support CDCVM must also support CDA.

**The Timing:** Effective **January 1, 2019**

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

CP

**The Change:** To support more secure transactions and increase the acceptance of contactless transactions within the payment ecosystem, the card brands have published contactless terminal mandates.

**The Impact:** These terminal mandates will result in older terminals being removed from the payment ecosystem, as older devices have created processing issues and declines at the point of sale. Additionally, many older terminals are unable to support EMV due to outdated hardware. Terminal vendors and merchants should plan accordingly to ensure compliance with the dates below, by brand and by region.

**United States**

| Brand      | Effective Date    | Terminal Type  |
|------------|-------------------|--|
| Amex       | December 31, 2018 | All POS terminals in the ecosystem                         |
| Discover   | August 23, 2018   | Terminals that are being upgraded                          |
| Mastercard | Immediate         | Newly deployed POS, MPOS and IPOS terminals (MSD optional) |
| Mastercard | April 1, 2023     | All POS and CAT terminals                                  |
| Visa       | April 13, 2019    | All POS terminals in the ecosystem, remove MSD             |

**Canada**

| Brand      | Effective Date    | Terminal Type                                  |
|------------|-------------------|--|
| Amex       | December 31, 2018 | All POS terminals in the ecosystem             |
| Discover   | August 23, 2018   | Terminals that are being upgraded              |
| Mastercard | Immediate         | Newly deployed POS, MPOS and IPOS terminals    |
| Mastercard | April 1, 2023     | All POS and CAT terminals                      |
| Visa       | October 19, 2019  | All POS terminals in the ecosystem, remove MSD |

**Asia Pacific Region**

| Brand      | Effective Date    | Terminal Type   |
|------------|-------------------|---|
| Amex       | December 31, 2018 | All POS terminals in the ecosystem                                    |
| Discover   | August 23, 2018   | Terminals that are being upgraded                                     |
| Mastercard | October 12, 2018  | All newly deployed POS and CAT terminals (Excludes Mobile POS (MPOS)) |
| Mastercard | October 18, 2019  | All newly-deployed MPOS terminals                                     |
| Mastercard | April 1, 2023     | All POS and CAT terminals   |
| Visa       | January 1, 2018   | All POS terminals in the ecosystem, remove MSD                        |

**Latin Caribbean and Caribbean Region**

| Brand      | Effective Date    | Terminal Type  |
|------------|-------------------|--|
| Amex       | December 31, 2018 | All POS terminals in the ecosystem                     |
| Discover   | August 23, 2018   | Terminals that are being upgraded                      |
| Mastercard | October 18, 2019  | All newly-deployed MPOS terminals                      |
| Mastercard | October 1, 2020   | All newly-deployed Integrated POS (IPOS) terminals     |
| Mastercard | April 1, 2023     | All terminals in the ecosystem                         |
| Visa       | October 19, 2019  | All POS terminals in the ecosystem, remove MSD         |
| Visa       | April 1, 2025     | All mPOS devices, AFDs, ECRs and ATMs in the ecosystem |

---

**[REMINDER] Visa and Mastercard Announce Support of Eight (8) Digit BINs**

---

**CP/CNP/eComm**

**The Program:** Increasing BIN demand across the electronic payments ecosystem has brought about the need for the extension of BINs from the first six digits of a primary account number (PAN) to the first eight digits of a PAN.

**The Change:** The International Organization for Standardization (ISO) published the new standard for the use of an 8-digit Issuer identification number (IIN). As a result, Visa and Mastercard have announced initiatives to update their systems to support the new ISO standard by 2019. In order to make the most efficient use of BINs, both networks will also use account ranges.

Account ranges enable an issuer to use a single BIN to support many programs of the same type. The use of account ranges allow an issuer to segment programs, define different product codes, and provide other capabilities and benefits.

**The Impact:** Merchants should begin prioritizing the necessary updates to ensure their various systems, used for either processing or reporting, are updated to support the eight digit BIN prior to the 2022 deadline.

**The Timing: April 2022**



---

**[NEW] Mastercard Updates Symbol Branding on Physical and Digital Cards**

---

CP/CNP/eComm

**The Change:** Effective November 1, 2019, the full color (red and yellow) Mastercard Brand Mark will be featured on cards without the word “mastercard”. This will be referred to as the “Mastercard Symbol”.



**Note:** The transition to Mastercard Symbol branding will not apply to the use of Mastercard branding in marketing materials.

**The Impact:** Cardholders may begin to present cards with the Mastercard Symbol without the word “mastercard” at merchant locations.

**The Timing:** November 1, 2019

---

**[NEW] Mastercard Revises Standards – Signature Panel on Cards**

---

CP

**The Change:** Mastercard will revise its Standards globally to allow issuers to choose whether or not to include the signature panel on the back of all Mastercard and Maestro cards (the signature panel is already optional for Cirrus cards).

**The Impact:** The card validation code (CVC) 2 value will continue to be required on the back of the card. When a signature panel is not present, the exact location of the CVC 2 value is up to the issuer. However, the CVC 2 value must be labeled as “CVC,” “CVC 2,” “Security Code,” or the equivalent wording in any language. The signature will continue to be present when required by local law or regulation.

Staff at merchant locations should be aware of these changes to ensure a seamless experience at the point of sale when presented with a Mastercard or Maestro card for payment by a consumer.

**The Timing:** April 12, 2019

---

## **[NEW] Mastercard Revises Standards – Use of Mastercard Sourced BIN Tables**

---

CP/CNP/eComm

**The Program:** Mastercard is reminding acquirers and merchants about the importance of maintaining and using accurate BIN tables. When accurate BIN table information is not used it can result in erroneous declines on the Mastercard network.

The declines can occur due to:

- Failure to update BIN table information in a timely manner
- Using websites or third-party sources for BIN table information that is outdated or inaccurate

**The Change:** Mastercard will mandate the use of accurate BIN tables for authorizations and clearing messages:

**The Impact:**

- Worldpay will update and maintain accurate BIN and issuing account range information using current files made available by Mastercard
- Merchants or third parties utilizing a BIN file to make authorization or routing decisions (including Worldpay's Master Merchant BIN File) **must utilize the most current BIN file available within six calendar days from the date that each update file is made available**

**The Timing:** June 30, 2019

---

## [NEW] Mastercard Revises Standards and Provides Clarification on the Mastercard Biometric Card

---

CP

**The Program:** The Mastercard Biometric card allows a cardholder to use their fingerprint to authenticate a transaction at the POS as an alternative to a PIN or signature. The Biometric card is the same length, width, and thickness as a standard payment card. The solution requires no changes for acquirers or to merchant hardware or software. This is not a CVM but a standalone technology for POS authentication that does not require any changes to the terminal.



Embedded fingerprint sensor to capture and match the cardholder's fingerprint to the digital fingerprint image stored on the card.

### POS Experience for the cardholder

- The cardholder inserts his or her biometric card into the merchant's terminal while holding his or her finger on the embedded fingerprint sensor.
- The fingerprint image is compared against the stored biometric template on the card.
- If the biometric data points match, then the transaction is authenticated without the cardholder needing to enter a PIN or write a signature and the transaction is sent to the issuer for authorization. An issuer host system or processor will be able to identify a successful biometric authentication and use that information as input for the approval decision.
- The issuer receives the authorization request with the biometric match results and will be able to approve the transaction, if appropriate.

### Biometric process

- The cardholder fingerprint is converted to binary
- When there is a successful match, the application interchange profile (AIP) of the card indicates cardholder verification is not supported by setting the "cardholder verification is supported bit" to zero. When this bit is set to zero the terminal will skip CVM processing altogether.
- If the biometric authentication match fails or is not completed the transaction will appear as a typical PIN or signature-based transaction.

**The Impact:** Worldpay will be able to see if biometric authentication has been used by confirming the Application Interchange Profile tag is set to zero. If this field is populated with a zero, then the transaction has a successful biometric match and is treated as a NO CVM transaction.

**Note:** This does not change any dispute rights.

---

**[NEW] Mastercard Retires MCC 9754 – Gambling – Horse Racing, Dog Racing, Non-Sports Intrastate Internet Gambling**

---

**CP/CNP/eComm**

**The Change:** Mastercard is life cycling MCC 9754 (Gambling – Horse Racing, Dog Racing, Non-Sports Intrastate Internet Gambling).

**The Impact:** In the U.S. Region merchants must discontinue use of MCC 9754 and use one of the following MCCs:

- MCC 7801 (Internet Gambling [U.S. Region Only]) for non-sports intrastate Internet gambling activity
- MCC 7802 (Government Licensed Horse/Dog Racing [U.S. Region Only]) for horse or dog racing gambling activity

**The Timing:** Effective April 2019 MCC 9754 will be deleted and may not be used for authorizations, first presentments or chargeback processing.

---

**[NEW] Mastercard Introduces New Data Integrity Edits to Monitor Use and Acceptance of Credential-On-File Indicator**

---

**CP/CNP/eComm**

**The Program:** Mastercard will update their Data Integrity Monitoring Program to include new edits to ensure transactions are using the Credential-On-File (POS Entry Mode 10) properly in authorization messages.

**The Impact:** The following new edits will be added to existing Data Integrity Monitoring Edits:

- **Edit Number 10 Electronic Commerce fields are invalid or blank**  
Mastercard will monitor to ensure when an Ecommerce transaction contains the POS Entry Mode of 10 (Credential on File) that the other point-of-sale fields/values consistently identify Ecommerce
- **Edit Number 21 (Dual Message) and 14 (Single Message) COF Indicator for Recurring Payments**  
Mastercard will monitor recurring transactions to ensure the transactions contain the POS Entry Mode of 10

**Effective Dates:**

|                  |  |
|------------------|--|
| January 1, 2019  | Monitoring begins                              |
| February 1, 2019 | Reports become available                       |
| April 1, 2019    | Edit 10 Comply by date                         |
| May 1, 2019      | Edit 10 Noncompliance assessments begin        |
| April 1, 2019    | Edit 21 and 14 Comply by date                  |
| May 1, 2019      | Edit 21 and 14 Noncompliance assessments begin |

**[REMINDER] Mastercard Updates Existing Edits and Introduces New Edits to Data Integrity Monitoring Program**

CP/CNP/eComm

**The Change:** Mastercard has updated their Data Integrity Monitoring Program with three new edits and added criteria to the existing POS Authorization Edit 10 and **also to Term POS Authorization Edit 8.**

**The Impact:** The edits, along with the compliance date and possible assessment dates, are listed below.

| NEW CLEARING EDITS   |   |
|--|---|
| <b>Edit Number 14</b>  |   |
| <b>Merchant DBA Name Match (Authorization DBA must match the settlement DBA)</b>   |   |
| <b>12/1/18</b> DBA Name Match Edit Compliance  | <b>1/2019</b> Possible non-compliance assessments |
| <b>Edit Number 16</b>  |   |
| <b>Terminal Input Match (Authorization Terminal Input Capability Indicator must match settlement TIC)</b>  |   |
| <b>6/1/19</b> Term Input Match Edit Compliance   | <b>7/2019</b> Possible non-compliance assessments |
| UPDATES TO EXISTING CLEARING EDITS   |   |
| <b>Edit Number 10</b>  |   |
| <b>POS Authorizations (Authorization POS Entry Mode must match settlement POS Entry Mode)</b>  |   |
| <b>6/1/19</b> POS Auth Edit Compliance   | <b>7/2019</b> Possible non-compliance assessments |
| <b>(Update) Edit Number 8 – Term POS (Improper Terminal Entry Capability value)</b>  |   |
| A transaction will fail the Data Integrity Authorization Edit 8 if the POS TEC is a value of '9' (Terminal supports EMV contact chip input only)   |   |
| Worldpay merchants should not be using a TEC value of '9', as the U.S. region is required to continue to support magnetic swipe transactions. Worldpay EMV certified merchants should be using the TEC value of '5' (Terminal supports EMV contact chip input and magnetic stripe input) |   |
| <b>8/1/18</b> Monitoring to begin  | <b>2/2019</b> Possible non-compliance assessments |

---

## **[REMINDER] Mastercard Introduces Online Authorizations of Refund Transactions**

---

CP/CNP/eComm

**The Program:** Currently, refund transactions to a Mastercard or Debit Mastercard card do not involve issuer authorization. Because there is no authorization request, the issuer is not aware a merchant has given a refund to a cardholder until the issuer receives the clearing message. Until this occurs, cardholders may inquire with the merchant, the issuer, or both about the status of their refund, which can lead to frustration and unnecessary “Credit Not Processed” chargebacks.

**The Change:** To encourage faster refund processing and reduce refund-related customer service burdens on merchants, acquirers, and issuers, Mastercard is introducing refund authorization support.

### **Merchant Support Requirement and Considerations**

All merchants, except airlines (MCCs 3000–3350 and 4511), must initiate an online authorization request for each refund transaction conducted on or after **April 17, 2020**.

#### **Merchants initiating refund transaction authorization requests:**

- Are strongly recommended to have a return policy that limits the time frame for processing a refund to no more than six months after the date of the original purchase.
- In a card-present environment, should ask the cardholder for the transaction receipt from the original purchase, identifying a truncated primary account number (PAN) for the payment card used, in order to ensure that the refund is submitted to that card. If a non-card payment device such as a contactless-enabled mobile phone was used for the purchase, the truncated PAN on the receipt may represent a device token that differs from the PAN on a physical card linked to the same account.
- Must submit the refund transaction authorization request no later than 24 hours after the merchant has notified the cardholder that the refund will be completed and provided the cardholder with a refund transaction receipt.
- Should be aware that refunds may not be supported by the issuer for certain cards (including non-reloadable prepaid cards) or transaction types.
- If a refund authorization request is declined, the merchant should refer to store policy to manage the return of the goods or services.

#### **Identification of Refund Transactions**

- Refund transactions are identified with a Processing Code value of 20 (Purchase Return/Refund)

---

## **[NEW] Mastercard Introduces Online Authorizations of Refund Transactions (cont.)**

---

CP/CNP/eComm

### **Reversal Messages**

A refund transaction reversal must only be submitted when the acquirer host system is unable to communicate an authorization response to the point-of-sale (POS) terminal, or following settlement, to correct a documented clerical error with the agreement of the issuer.

Any reversal or adjustment to correct an error must occur within one calendar day of the date the refund transaction was submitted

- Reversible clerical errors include: the erroneous capture of transaction data, a duplicate transaction, or an error caused by the transposition of data.

### **Chargebacks**

Currently chargeback rights are available to an issuer if the merchant has agreed to accept a return of goods or cancellation of services but a refund transaction has not been processed to the cardholder's account. A "Credit Not Processed" chargeback may be submitted 15 calendar days after the return or cancellation date.

### **Effective for refund transactions occurring on or after April 17, 2020**

An issuer may also exercise a valid authorization-related chargeback right.

An authorization-related chargeback may be submitted when one of the following has occurred:

- Authorization was required but not obtained
- The primary account number (PAN) does not exist
- The authorization chargeback protection time period had expired for the presentment (the time period is seven calendar days following a refund transaction authorization, which must be submitted as a final authorization) and one of the following:
  - For a transaction occurring at a merchant located in the Europe region, the account was permanently closed before the chargeback was processed
  - For a transaction occurring at a merchant located in any other region, the issuer deemed the account not to be in good standing before filing the chargeback

**The Timing: Effective April 17, 2020**, all merchants, except airlines, must support online authorization requests for refund transactions.

*Support of authorization requests for refund transactions prior to April 17, 2020 is optional for merchants.*

**Note:** None of these changes affect a merchant's ability to establish its own refund/return policy, which includes the ability to refuse or restrict refunds, returns, cancellations or exchanges; provided that the policy is disclosed to the customer at the point and time of purchase.

---

## **[REMINDER] Mastercard Introduces Transaction Integrity Classifications (TIC) for Interchange Rates**

---

CP/CNP/eComm

**The Program:** Mastercard has introduced 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.

**The Change:** MasterCard will review transaction characteristics to assess the validity of the card and the cardholder and will provide these results to issuers to assist them in making authorization decisions.

**The Impact:** The implementation of the TIC indicator is being rolled out in a phased approach.

### **Phase I: April 2016**

MasterCard begins to populate the TIC Indicator (DE 48, sub-element 52) in the authorization response message for credit and debit card purchases and purchase with cashback transactions.

### **Phase II: April 2019**

The second phase will require merchants to receive the TIC indicator value in the authorization response message. Merchants will then be required to return the TIC indicator value in the clearing message in order to qualify for the appropriate interchange. The TIC indicator will be mandatory for specific interchange programs in the U.S. region.

### **Required: October 2019**

Mastercard will be mandating the use of the TIC value in all settlement messages, chargebacks and arbitration chargebacks. Mastercard may override interchange rates based on the TIC indicator, with the October 2019 Release.

| <b>Valid Values for the Transaction Integrity Class</b> |  |    |
|---|--|----|
| 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 |

- Worldpay currently receives the TIC in the authorization response message and is logging the value for future use
- Worldpay is making system updates to send the TIC indicator in the auth response message to merchants
- Merchant specifications will be updated to support the TIC indicator in both auth response messages and clearing messages between merchants and Worldpay
- Worldpay is updating our systems to ensure proper interchange qualification based upon the TIC indicator received

---

**[REMINDER] Mastercard Claims Manager (MCM) for Disputes**

---

CP/CNP/eComm

**The Program:** Mastercard announced plans to make changes to their disputes resolution process for its network participants in the first half of 2019, followed by additional changes in April 2020.

**The Change:** For 2019 Worldpay will enhance systems to facilitate real-time processing with Mastercard. With these enhancements merchants will be able to self-serve and the following dispute deliverables will be updated:

**Reporting updates**

- Dispute Reports
- Dispute Notices (DMMD version)

**Core iQ updates**

- Questionnaire added for Mastercard
- Population of the Case Status and Ownership field
- One new action code (RRER- Retrieval Request Refusal)

**The Timing:** These changes will go into effect on May 9, 2019.

Worldpay will continue to provide updates and schedule training sessions prior to the go-live date. Additional information may also be viewed by visiting: [www.vantiv.com/disputes](http://www.vantiv.com/disputes)

---

**[UPDATE] 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 that 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:** Effective **October 2019** merchants will be required to send the Deferred Authorization Indicator

---

**[REMINDER] Visa Announces Global Rollout Plans for 3-D Secure 2.0**

---

eComm

**The Change:** 3-D Secure 2.0 participants should be aware of the phased approach for chargeback protection for merchant-attempted transactions.

**The Impact and Timing:****Prior to April 12, 2019 - Fraud Related Chargebacks**

- **3-D Secure 2.0 Merchant-attempted to authenticate** transactions will not receive fraud related chargeback protection when the issuer BIN does not yet support 3-D Secure 2.0 in the authentication request. These transaction will be treated like unauthenticated e-commerce transactions (Electronic Commerce Indicator = 07)
- **3-D Secure 2.0 Issuer-authenticated** transactions will receive fraud-related chargeback protection or when a 3-D Secure 2.0 issuer is temporarily unavailable and Visa stands in.

**April 12, 2019 - Global program activation date\***

- Visa 3-D Secure 2.0 Merchant-attempted to authenticate transactions will begin to have chargeback protection. These transactions will be identified with Electronic Commerce Indicator = 06.

\*Visa has moved the activation date for the **Asia Pacific Region** to **April 18, 2020**.

---

## [UPDATE] Visa Updates Rules to Streamline Cardholder and Merchant Interaction at the Point of Sale

---

CP

**The Change:** Visa has announced acceptance policy changes that will provide an opportunity to streamline requirements for merchants, to identify and verify cardholders at the point of interaction in face-to-face environments. These updates will remove outdated requirements and practices, reduce friction and clarify a merchant's responsibility for verifying cardholders at the point of interaction. The changes do not add any new requirements for merchants and acquirers.

### The Impact:

#### Merchants are no longer required to:

- Check one or more security features on the card:
  - Specifically verify the signature on the receipt matches that on the card
  - Treat cards with unsigned / blank signature panels differently from other transactions

#### Updates to Rules and Policies:

- Update Visa's Honor All Cards rule to clarify merchants must not refuse transactions based on the form factor the cardholder presents for payment if the merchant is technically capable of accepting the transaction. As an example; a contactless-capable merchant cannot choose to only accept NFC-enabled mobile devices but not accept contactless-enabled Visa cards.
- Update the definition of CVM to include consumer device cardholder verification method (CDCVM) alongside PIN and signature as valid CVMs.
- CDCVM may be a valid CVM alongside PIN for cash-back transactions (where cash-back is permitted).
- Clarify merchants must not perform cardholder verification before the cardholder knows the final amount. Existing exceptions continue to apply as outlined in the Visa Rules.
- Visa's Uniform Services policy (merchants must process all transactions the same way except discounts, promotions, or incentives offered to a subset of Visa cards) applies to all cards and payment devices accepted by a merchant.
- Merchants and acquirers will be able to accept mobile payment devices and Visa Micro Tags for both manual cash disbursements and quasi-cash transactions.
- Removal of requirements for deployment of account number-verifying terminals for manual cash disbursements.

**The Timing:** All of the updates listed above are effective immediately.

April 13, 2019 - special agreements between acquirers and issuers to permit merchants to collect a Card Verification Value 2 at the POS for fallback transactions will be removed.

---

## [UPDATE] Visa Outlines Phased Approach for Required Support of New Purchase Return Authorization Messages

---

CP/CNP/eComm

**The Program:** Visa will require merchants to support authorization for credit/refunds transactions. The credit/refund authorization request will be displayed to the cardholder as a pending credit/refund when approved by the issuer. The credit/refund settlement transaction will continue to be used by merchants, acquirers, and issuers to return the funds back to the cardholder.

### UPDATE

As a reminder, Visa approved an extension until April 12, 2019 for all Worldpay merchants. All merchants should continue working towards this date if they have not already started submitting returns for online authorizations.

### Effective April 2019

All remaining merchants in all regions will be required to send an authorization for all credit/refunds in Phase II, effective April 2019.

Credits/refunds/purchase returns that do not receive a valid authorization may be charged back by the issuer using VCR code 11.2, Declined Authorization (*formerly reason code 71*) and code 11.3, No Authorization (*formerly reason code 72*).

### Effective July 2019

Credit vouchers will be included in the Zero Floor Limit “non-authorized settlement” and Authorization Misuse Processing Integrity Fee Assessment

- Merchants should submit existing Processing Code ‘20’ in authorization requests to identify credit/refund transactions. Merchants may continue to generate the fields they send today for sale transactions with the Processing Code of ‘20’ in the authorization request; **however, to avoid unnecessary declines, Visa strongly advises that only mandatory fields be sent by merchants.**
- Merchants should prepare to add the approval code on their receipts as a best practice for credit/refund transactions. Visa is planning to update their rules to require the approval code on receipts.

---

**[UPDATE] Visa Outlines Phased Approach for Required Support of New Purchase Return Authorization Messages (cont.)**

---

CP/CNP/eComm

**Effective April 13, 2019 Visa Rules will be updated with the following clarifications and revisions to the credit refund processing requirements:**

- Merchants must first attempt to process a refund (credit transaction) to the same Visa account that was used for the original purchase transaction.
- Clarify the circumstances under which a merchant may choose to process the refund onto a different Visa account (along with proof that the original sale took place on a Visa account), as follows:
  - The original account is no longer available or valid (e.g., the original card has been replaced due to expiration or being reported lost / stolen, or was a Visa Prepaid card that has since been discarded).
  - The authorization request for the credit transaction was declined.
- Clarify the scenarios where a merchant is permitted to offer an alternate form of credit (cash, check, in-store credit, prepaid card, etc.) when a refund cannot be processed to the original Visa account or to an alternate Visa account, because of one or more of the following conditions:
  - The cardholder does not have a receipt or other proof of purchase from the original sale.
  - The refund is made to a recipient of a gift (instead of to the cardholder who made the original purchase).
  - The original sale took place on a Visa Prepaid card, which has since been discarded.
  - The authorization request for the credit transaction was declined.
- Clarify that a refund to a Visa account must only take place when the original purchase took place on a Visa account, i.e., if the original purchase was made with a non-Visa method, such as cash or a non-Visa general purpose payment card, then the credit transaction should be an original credit transaction.
- Remove the requirement for a merchant to identify the original sale on the refund transaction receipt.
- Globalize the existing regional rules requiring refunds to be processed within five calendar days from the transaction date.

None of these changes affect a merchant's ability to establish its own refund/return policy, which includes the ability to refuse or restrict refunds, returns, cancellations or exchanges, provided that the policy is disclosed to the customer at the point and time of purchase.

---

**[REMINDER] Visa Sunsets Static Data Authentication (SDA) for Mass Transit Merchants**

---

**CP/CNP**

**The Change:** Visa will sunset the use of Static Data Authentication (SDA) for all clients operating in the transit sector. This will be done in a phased approach to minimize cardholder impact.

**The Impact:** Visa will require all NEW contactless cards to support only fast dynamic data authentication (DDA). All contactless-only acceptance readers will also be required to support only DDA. These changes enable transit operators to better manage risk for cards presented at a reader.

Transit merchants that deploy contactless-only acceptance devices at the turnstile, fare gate, or point of boarding, if configured to always perform offline data authentication (ODA) before allowing the cardholder to access their services, must support Visa contactless dynamic data authentication using fDDA.

**The Timing:** April 15, 2023

---

**[REMINDER] Visa Modifies the U.S. Network Acquirer Processing Fee (NAPF)**

---

**CP/CNP/eComm**

**The Change:** Visa is modifying the pricing for the U.S. Network Acquirer Processing Fees (NAPF).

**The Impact:** Visa will be increasing the NAPF rate for **international** credit and debit Authorizations and Returns. The NAPF rates for domestic credit and debit authorizations and returns will remain unchanged.

**The Timing:** April 2019

---

**[REMINDER] Visa Updates U.S. Acquirer International Service Assessment (AISA) Fee**

---

**CP/CNP/eComm**

**The Change:** Visa is updating the U.S. Acquirer International Service Assessment (AISA) fee.

**The Impact:** Visa will increase both the base AISA and the Enhanced AISA rate. These fees also apply to Interlink and PAVD transactions.

**The Timing:** April 2019

| Type     | AISA Description   |
|----------|--|
| Base     | Issuer location is non-U.S. and merchant transaction currency is U.S. dollars            |
| Enhanced | Issuer location is non-U.S. and merchant transaction currency <b>is not</b> U.S. dollars |

---

**[NEW] Discover Revises Arbitration and Representment Timeframes** CP/CNP/eComm

---

**The Change:** Discover is changing the timeframe to initiate a dispute arbitration request from 30 to 10 days from the notice date of a Pre-Arbitration Inquiry decision.

The timeframe for the Acquirer/merchant to initiate representment is being reduced from 45 to 30 days after the Chargeback Dispute Notice issue date.

**The Impact:** Merchants should be aware of the changes and update processes to ensure adherence with the new timeframes.

**The Timing:** October 18, 2019

---

**[REMINDER] Discover Introduces Return Authorization Requirements** CP/CNP/eComm

---

**The Change:** Discover will require merchants to support authorization for credit/refunds transactions. This will enable the credit/refunds to be visible real-time on cardholder communications as a pending transaction, providing better visibility into the refund status.

**The Impact:** Merchants will need to adhere to Discover Refund Rules as outlined below:

- Merchants should submit processing code '20' in authorization requests to identify credit/refund transactions
- Merchants may not give cash refunds for returns of goods or unused services purchased using a Discover Card
- Merchants may issue a credit to a Discover card account only for a sale originally made with a Discover card
- The credit amount may not exceed the amount of the original sale or the original value of the prepaid card in the case of non-reloadable prepaid cards

**The Timing:**

**October 2018** Merchants are *permitted* to submit an authorization request for a return/credit

**April 2019** Merchants will be **required** to submit an authorization request for a return/credit

---

## [REMINDER] Discover Introduces Transaction Level Indicators for Incremental Authorizations

---

CP/CNP/eComm

**The Change:** Discover is mandating a new POS Transaction Status Indicator value of “I” (Incremental authorization) to be sent for each incremental authorization or reversal. This value must also be populated in each subsequent request with the same value as the initial authorization request.

**The Impact:** For merchants that support Discover incremental authorization transactions

- For each incremental authorization card sale or reversal merchants must also populate the **Retrieval Reference Number** with the value from the initial authorization request.
- Discover is also adding a **new** additional amount type, **Cumulative Amount**, in support of incremental authorizations. If a transaction has been identified as an incremental authorization this amount type must also be present.
- Discover has also clarified rules related to incremental authorizations that the settlement (clearing) data must contain the data from the original authorization for the following fields:
  - **Approval Code**
  - **System Trace Audit Number**
  - **Network Reference ID**

Eligible MCCs for Incremental Authorizations are listed below

| MCC       | Description   |
|-----------|---|
| 3501-3999 | Hotels  |
| 7011      | Hotels, Motels and Resorts  |
| 3351-3441 | Car Rental  |
| 4411      | Cruise Lines  |
| 4111      | Local/Suburban Commuter Passenger Transportation, including Ferries                   |
| 4112      | Passenger Railways  |
| 4121      | Taxi Cabs/Limousines  |
| 4131      | Bus Lines – Charter, Tour   |
| 4457      | Boat Rentals & Lease  |
| 5812      | Eating Places and Restaurants (excludes gratuities)                                   |
| 5813      | Drinking Places (excludes gratuities)   |
| 7512      | Automobile Rental Agency  |
| 7513      | Truck and Utility Trailer Rentals   |
| 7519      | Motor Home and Rec. Vehicle Rentals   |
| 7033      | Trailer Parks & Campgrounds   |
| 7996      | Amusement Parks, Circuses & Fortune Tellers   |
| 7394      | Equip/Tool/Furn/Appl Rental & Leasing   |
| 7999      | Recreation Services (Not Classified) (Includes Aircraft Rental, Bicycle Rental, etc.) |

---

**[REMINDER] Discover Reminders for Partial Shipment Transactions**

---

CP/CNP

**The Program:** Partial shipments allow a merchant to send multiple settlement (clearing) messages for a single authorization request.

**The Change:** Discover is providing clarification for partial shipment authorization and settlement (clearing) messages.

**The Impact:**

- Merchants are reminded all clearing records must be submitted within seven (7) calendar days of the authorization.
- If it is not possible to fulfill all shipments within this timeframe the merchant must submit a reversal or partial reversal and submit a reauthorization for the new amount
- Discover requires the following fields from the original authorization be sent in the clearing message for all partial shipment transactions
  - **Approval Code**
  - **Network Reference ID**

---

**[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**.

---

**[REMINDER] China Union Pay Launches New 8-Series BIN**

---

CP/CNP/eComm

**The Change:** China Union Pay is launching a new 8-Series BIN range in January 2019.

**The Impact:** Merchants and partners should ensure all point-of-sale devices are able to identify, accept, and process these new BINs. Merchants who currently accept Discover are required to honor all China Union Pay cards and BIN ranges. **Note:** PANs (Personal Account Numbers) can be 19 digits in length.

**Existing Ranges**

| Start    | End      | Issuing Network |
|----------|----------|-----------------|
| 62109400 | 62109499 | Union Pay       |
| 62212600 | 62292599 | Union Pay       |
| 62400000 | 62699999 | Union Pay       |
| 62820000 | 62889999 | Union Pay       |

**New Ranges**

| Start    | End      | Issuing Network |
|----------|----------|-----------------|
| 81000000 | 81099999 | Union Pay       |
| 81100000 | 81319999 | Union Pay       |
| 81320000 | 81519999 | Union Pay       |
| 81520000 | 81639999 | Union Pay       |
| 81640000 | 81719999 | Union Pay       |