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® Network, Mastercard® Worldwide and Visa® U.S.A. outlining changes to operating rules and regulations, interchange rates, compliance of network mandates, and other industry updates that may impact your business.

Except where otherwise noted, the changes described in the articles will be effective **October 12, 2018, central processing date of October 13, 2018.** 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:

- 1152-bit keys EXPIRED ON 12/31/2017 *
  - ***This key should now be removed (deadline was June 30, 2018)***
- 1408-bit keys have expiry date of 12/31/2024
- 1984-bit keys have expiry date of **12/31/2028**
  - **EMVCo changed the expiration date of the 1,984-bit Payment System Public Key to December 31, 2028**

*** UnionPay has announced the expiration date for their 1152-bit key is 12/31/2021**

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 Revises Standards for Technical Fallback from Chip to Magnetic Stripe CP

The Program: As more markets become chip-mature and issues with the use of EMV technology diminish, fallback transactions are less likely to be a result of a technical problem, and more likely to be fraudulent attempts.

The Change: Mastercard has announced a mandate to phase out the use of technical fallback in all regions with the exception of the Asia/Pacific and U.S. regions. This mandate applies to POS terminals (including mobile point-of-sale [MPOS]), cardholder-activated terminals (CATs), and ATMs.

The Impact: All issuers in the Canada, Europe, Latin America and the Caribbean, and Middle East/Africa regions must decline all technical fallback transactions when the merchant location of the transaction also resides in one of these regions. If a chip cannot be read after multiple attempts, the transaction will not move forward on that card and the merchant may ask for another form of payment.

Effective Dates:

Effective Date	Region	Requirement
February 1, 2018	Canada	Issuers must decline technical fallback transactions
October 12, 2018	Latin America/Caribbean	Issuers must decline technical fallback transactions
October 12, 2018	U.S.	Issuers **may** decline technical fallback transactions

- Fallback transactions acquired in the Asia/Pacific and U.S. regions **may continue to be approved**.
- Magstripe transactions containing a POS Entry Mode of 90 (PAN Auto-Entry via Magnetic Stripe) **may continue to be approved by issuers in all regions**

[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 Program: A contactless payment allows cardholders to make purchases via a debit or credit card by using near-field communication (NFC). To make a contactless payment, the cardholder taps their card or mobile device near a point-of-sale terminal, otherwise known as “tap-and-go”.

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	April 16, 2016	All newly deployed
Discover	August 23, 2018	Terminals that are being upgraded
Mastercard	Immediate	Newly deployed POS terminals
Mastercard	Immediate	All newly-deployed MPOS terminals
Mastercard	Immediate	All newly-deployed Integrated POS (IPOS) terminals.
Visa	April 1, 2013	Newly deployed POS terminals or terminals that are being upgraded (on or after this date)
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	April 16, 2016	All newly deployed
Discover	August 23, 2018	Terminals that are being upgraded
Mastercard	Immediate	Newly deployed POS terminals
Mastercard	Immediate	All newly-deployed MPOS terminals
Mastercard	Immediate	All newly-deployed Integrated POS (IPOS) terminals.
Visa	January 1, 2012	Newly deployed POS terminals
Visa	April 1, 2014	Terminals that are being upgraded
Visa	October 19, 2019	All POS terminals in the ecosystem, remove MSD

[REMINDER] Contactless Terminal Requirements: All Brands, All Regions (cont.)

CP

Asia Pacific Region

Brand	Effective Date	Terminal Type
Amex	December 31, 2018	All POS terminals in the ecosystem
Discover	April 16, 2016	All newly deployed
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, 2012	Newly deployed POS terminals or terminals that are being upgraded (on or after this date)
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	April 16, 2016	All newly deployed
Discover	August 23, 2018	Terminals that are being upgraded
Mastercard	October 12, 2018	Newly deployed POS terminals
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	January 1, 2012	Newly deployed POS terminals
Visa	April 1, 2014	Terminals that are being upgraded
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.

All Brands: No Signature Rule Changes Announced

[UPDATE] No Signature Rule Changes Announced by All Brands CP

The Change: Effective April 2018; Mastercard, Discover, American Express, and Visa updated their rules to allow merchants the option to choose whether to collect a cardholder's signature for all card-present point of sale transactions.

The Impact: Effective with this change, merchants will not be liable for applicable chargebacks as a result of not capturing a signature for card-present transactions. While sales transacted after April 14, 2018 are not required to have a signature, any disputed transactions that occurred prior to April 14, 2018, signatures are required to be provided.

Eliminating the requirement for signature collection **allows merchants the option to discontinue collecting signatures** for all transactions or to set thresholds for signature collection at their discretion.

Specific regions and the applicable audience for each brand are outlined below.

UPDATE – Mastercard announced effective October 12, 2018 they are expanding their no signature rule changes to both the LAC and AP regions.

NETWORK	DEMOGRAPHIC AREA	AUDIENCE
American Express	Globally	All Card Present Merchants
Mastercard	United States Canada **LAC Region** **AP Region**	All Card Present Merchants
Discover	Globally	All Card Present Merchants
Visa	Globally	Card Present Merchants- EMV Enabled POS Device

- Merchants interested in no longer requiring a signature may need to update their point of sale systems; however, the CVM settings should not be changed.
- The above information is a high level overview of the general requirements. For additional information please review the updated No Signature Reference Guide at the link below:

  No Sig All Brands Update

[UPDATE] Authorization Procedures for Credential (Card) on File [Merchant-Initiated and Cardholder-Initiated] Transactions

CP/CNP

The Program: Worldpay continues to work with the card brands to ensure we have the answers our merchants need in order to properly implement Credential on File. We've obtained additional technical details related to CoF requirements and have updated our comprehensive resource document.

The Change: UPDATE 8/24/18- Mastercard confirmed all issuers have the ability to support the POS entry mode of "10".

The Impact: Merchants may begin including this entry mode as part of the CoF framework for Mastercard transactions.

The updated Credential on File technical requirements document (for the core platform) can be retrieved through the link below.

Credential On File Core Update

[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

[UPDATE] 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	
Edit Number 13 MCC Match (Authorization MCC must match the settlement MCC)	
6/1/18 MCC Match Edit Compliance	**7/2018** Possible non-compliance assessments
Edit Number 14 Merchant DBA Name Match (Authorization DBA must match the settlement DBA)	
12/1/18 DBA Name Match Edit Compliance	**1/2019** Possible non-compliance assessments
Edit Number 16 Terminal Input Match (Authorization Terminal Input Capability Indicator must match settlement TIC)	
6/1/19 Term Input Match Edit Compliance	**7/2019** Possible non-compliance assessments
UPDATES TO EXISTING CLEARING EDITS	
Edit Number 10 POS Authorizations (Authorization POS Entry Mode must match settlement POS Entry Mode)	
6/1/19 POS Auth Edit Compliance	**7/2019** Possible non-compliance assessments
(Update) Edit Number 8 – Term POS (Improper Terminal Entry Capability value) 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)	
8/1/18 Monitoring to begin	**2/2019** Possible non-compliance assessments

[NEW] 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 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 cardholder has been notified that the refund will be completed and the cardholder provided 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, merchants 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)

Sending the Unique Identifier from the Original Purchase

Mastercard is recommending if the merchant is capable of obtaining details from the original purchase to include the original sale Trace ID (Network Data, Financial Network Code, Banknet Reference Number, and Date –Settlement) in the purchase return/refund authorization request message.

The presence of the unique identifier will assist an issuer in matching the refund to the original purchase, increasing confidence the refund authorization request is valid and potentially expediting the release of funds to the cardholder.

[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.

[UPDATE] Mastercard Introduces Transaction Integrity Classifications (TIC) for Interchange Rates

CP/CNP/eComm

The Program: Mastercard is introducing 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 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.

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

- 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 Introduces Mastercard Claims Manager (MCM) for Disputes

CP/CNP/eComm

The Program: The objectives of Mastercard Claims Manager (MCM) are to reduce chargeback volumes, expedite resolution, and improve the customer experience.

The Change:

Some of the changes expected with MCM:

- Consolidation of reason codes into 4 categories:
  1. Cardholder Dispute
  2. Point-of-Interaction Error
  3. Authorization Related
  4. Fraud
- Blocking invalid chargebacks from entering the network
- Elimination of the Arbitration Chargeback Cycle
- Reducing the time to Resolve

What remains the same?

- Time for merchants to respond to chargebacks remains 45 days

What are the time frame changes for Mastercard dispute rules?

Timeframes	Feature Reason Code	Dispute Rule Changes
	4853 Cardholder Disputes Consolidated Family	No change, max 120 days
	4808 Authorization-Related Disputes Consolidated Family	No change, max 90 days
	Fraud Dispute Reason Codes	No change, max 90 days
	4834 Point-of-Interaction Error Disputes Consolidated Family	Max 90 days
	All other legacy non-consolidated non-family reason codes	No change, max 120 days
Other	Chargeback Cycles	Change to 2 cycles
	Pre-Arbitration Requirements	Required on Fraud, Cardholder Disputes and possibly some POI Error Disputes

Additional information, including upcoming webinars to review the new Mastercard Claims Manager program, may be reviewed on our Disputes and Chargeback site: **https://www.vantiv.com/disputes**

[REMINDER] Mastercard Reminder of Requirements for Gratuities and Partial Approvals

CP/CNP/eComm

The Program: Mastercard is reminding customers about acceptance and transaction processing procedures for the addition of a gratuity to a transaction amount and the support of partial approval authorizations.

Transactions with Added Gratuities
A cardholder may add a gratuity before a payment method is selected and authorization is obtained (for example, by choosing a percentage or specific amount to be added to the purchase amount) or the merchant's POS terminal may generate a transaction receipt that contains space for a gratuity to be handwritten by the cardholder, and added to the purchase amount after authorization is obtained.

Authorization Tolerance for an Added Gratuity
An authorization tolerance of 20 percent applies in the event a gratuity has been added after authorization approval. If the addition of a gratuity causes the transaction amount to exceed the authorized amount by more than 20 percent, an additional incremental authorization should be obtained for chargeback protection.

Transaction Type	Authorization Tolerance Permitted
Chip and Pin	No
Contactless	No
Card Not Present (CNP)	No
*CNP (MCC 5812-Eating Places, restaurants or 5814 Fast food restaurants) – US Region Only	Yes
All other transactions, including signature-based contact chip and magnetic stripe transactions	Yes

* U.S. region merchants should be aware for card-not-present transactions occurring at U.S. region merchants (MCCs 5812 and 5814), the authorization-related chargeback protection afforded by the tolerance applies only to U.S. domestic transactions. A cross-border transaction may incur an authorization-related chargeback for any amount not authorized by the issuer.

Partial Approval Responses and Added Gratuities
If a merchant supports partial approval authorization responses, and the issuer's response is a partial approval for less than the requested amount, then the transaction amount submitted for settlement must not exceed the authorized amount. An authorization tolerance does not apply.

Partial Approval Support
Mastercard is reminding merchants and acquirers they must support partial approvals for all prepaid Mastercard, all Debit Mastercard, and all Maestro account ranges for merchants identified with MCC 5542 (Automated Fuel Dispenser) and merchants, globally, for the following MCCs conducting card-present transactions at attended POS terminals:

Global MCCs - Card Present
5310 Discount Stores
5311 Department Stores
5411 Grocery Stores, Supermarkets
5541 Service Stations (with or without Ancillary Services)
5621 Women's Ready to Wear Stores
5691 Men's and Women's Clothing Stores
5732 Electronic Sales
5812 Eating Places, Restaurants
5814 Fast Food Restaurants
5912 Drug Stores, Pharmacies
5999 Miscellaneous and Specialty Retail Stores

[REMINDER] Mastercard Reminder of Requirements for Gratuities and Partial Approvals (cont.)

U.S. Region Only Merchants Using the following MCCs must support partial approval
4111 Transportation - Suburban and Local Commuter Passenger, including Ferries
4812 Telecommunication Equipment including Telephone Sales
4814 Telecommunication Services
4816 Computer Network/Information Services
4899 Cable, Satellite, and Other Pay Television and Radio Services
5111 Stationery, Office Supplies
5200 Home Supply Warehouse Stores
5300 Wholesale Clubs
5310 Discount Stores
5311 Department Stores
5331 Variety Stores
5399 Miscellaneous General Merchandise Stores
5411 Grocery Stores, Supermarkets
5499 Miscellaneous Food Stores - Convenience Stores, Markets, Specialty Stores
5541 Service Stations (with or without Ancillary Services)
5542 Fuel Dispenser, Automated
5732 Electronic Sales
5734 Computer Software Stores
5735 Record Shops
5812 Eating Places, Restaurants
5814 Fast Food Restaurants
5912 Drug Stores, Pharmacies
5921 Package Stores, Beer, Wine, and Liquor
5941 Sporting Goods Stores
5942 Book Stores
5943 Office, School Supply and Stationery Stores
5999 Miscellaneous and Specialty Retail Stores
7829 Motion Picture - Video Tape Production-Distribution
7832 Motion Picture Theaters
7841 Video Entertainment Rental Stores
7996 Amusement Parks, Carnivals, Circuses, Fortune Tellers
7997 Clubs - Country Membership
8011 Doctors - not elsewhere classified
8021 Dentists, Orthodontists
8041 Chiropractors
8042 Optometrists, Ophthalmologists
8043 Opticians, Optical Goods, and Eyeglasses
8062 Hospitals
8099 Health Practitioners, Medical Services - not elsewhere classified
7999 Recreation services - not elsewhere classified
8999 Professional Services - not elsewhere classified

[REMINDER] Mastercard Canada Cross Border Fee Increase CAN

The Change: MasterCard will increase the Cross Border fees for transactions acquired in Canada.

The Impact: The Cross Border fee is assessed to transactions where the accepted card is issued outside of Canada. Merchants may recognize an increase in fees for these transactions.

Description
MasterCard Cross Border Assessment – non-CAD
MasterCard Cross Border Assessment – CAD

The Timing: November 4, 2018

[NEW] Visa Updates Service Fee Rules for Certain Transaction Types Submitted by Eligible Government and Education MCCs

CP/CNP/eComm

The Program: Previously Visa required purchases/payment amounts to be charged by government and education merchants separately from any service fee and submitted as two separate transactions.

The Change: Visa will begin to provide government and education merchants the option to submit the service fee in a separate transaction or to combine the service fee with the purchase/payment amount into a single transaction.

The Impact: The one transaction model will help support contactless payment and Consumer Device Cardholder Verification Method-authentication transactions, as only one unique cryptogram will be needed to process the transaction.

The following government and education MCCs are eligible to submit the service fee and payment amount/purchase in a single transaction for face-to-face transactions submitted by the merchant or third party processing the transaction on behalf of the merchant, or when the merchant processes the transaction in a card-not-present environment:

- MCC 9211 Court Costs, Including Alimony and Child Support
- MCC 9222 Fines
- MCC 9311 Tax Payments
- MCC 9399 Government Services (Not Elsewhere Classified)
- MCC 8220 Colleges, Universities, Professional Schools, and Junior Colleges
- MCC 8211 Elementary and Secondary Schools
- MCC 8244 Business and Secretarial School
- MCC 8249 Vocational and Trade Schools

NOTE: The service fee must continue to be submitted as a separate transaction in the card-not-present environment when a third party is processing the transaction on behalf of the merchant.

The Timing: Effective Immediately

[NEW] Visa Introduces New Merchant Category Code for Marketplaces **CNP/eComm**

The Change: Visa is introducing a specific merchant category code (MCC) dedicated to marketplace transactions.

- **MCC 5262 Marketplaces**: Entities classified with this MCC are online marketplaces that accept Visa and bring together cardholders and retailers via an ecommerce website or mobile application under a single brand, used to identify itself to cardholders.
- These entities must meet all Visa qualification requirements and be registered with Visa as a marketplace.

The Impact: Qualified and registered marketplaces must begin to use **MCC 5262** for all transactions processed by the marketplace, on behalf of retailers on the marketplace platform.

[REMINDER] Visa Canada Introduces New CVV2 Requirement for Card-Not-Present Merchants **CAN**

The Program: Visa Canada is making changes to CNP/eCommerce transactions to address fraud. Visa will require Canadian card-not-present merchants to include the Card Verification Value 2 (CVV2) with every transaction.

The Change: Canadian merchants will be required to begin capturing and passing the CVV2 (card verification value 2) in all e-commerce and mail order/telephone order authorization requests.

The Impact and Timing:
Merchants must comply with the new requirement as outlined below:

Effective October 14, 2017 - New Canadian merchants must include the CVV2 value in authorization requests for e-commerce and mail order/telephone order transactions. (Visa defines a new merchant as one that is accepting Visa payment products for the very first time)

Effective October 13, 2018 - Existing Canadian merchants will need to include the CVV2 value in authorization requests for e-commerce and mail order/telephone order transactions.

- Issuers who approve a domestic transaction with a CVV2 result code of “N” (no match) will retain liability
- Issuers retain chargeback rights when the merchant doesn’t pass any CVV2 with the authorization where the issuer cannot verify the CVV2

Exclusions:
The following scenarios are excluded from the CVV2 mandate:

- Subsequent credential on file transactions (e.g., recurring, installment, unscheduled credential on file)
- Visa Commercial Card Virtual Accounts
- Digital wallets such as Visa Checkout

[UPDATE] Visa Announces Global Rollout Plans for 3-D Secure 2.0 eComm

The Program: The 3-D Secure 2.0 specification provides a foundation for products with new cardholder authentication capabilities to be developed. Visa wants to ensure that stakeholders have time to test, pilot, and fully roll out their solutions to support 3-D Secure 2.0 prior to including merchant-attempted-to-authenticate transactions in fraud-related chargeback protection.

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:

Mid 2017
Early adoption of 3-D Secure 2.0

October 2017
Cardholder Authentication Verification Value (CAVV), the cryptographic value that is unique to each authentication request, must be present for all Visa 3-D secure transaction, globally.

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.

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

[REMINDER] 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. 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 and Timing: Visa announced **a phased approach** for merchant required support of the purchase return authorization message as outlined below:

Phase I – Effective October 2018

Merchants that meet the annualized minimum refund volume as outlined by region below are required to support the purchase return authorization message in Phase I, effective October 2018.

Region	Annualized Visa Credit/Refund Volume Minimum
U.S.	USD $10 million
Canada	USD $5 million
AP	USD $1 million
LAC	
CEMEA	

Phase II – 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. Merchants are permitted to adopt the earlier Phase I effective date. Airline merchants have the option to delay implementation until April 2019.

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.

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.

[REMINDER] 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 Clarifies Network Name Receipt Requirements in U.S. Region

CP

The Program: With the use of the Common Debit AID in the U.S., the routing decision may be made downstream, and as a result, the terminal may not know which network processed the transaction at the time the receipt was generated. For these transactions Visa may not be the network selected to route or process the transaction, which means 'Visa' cannot be printed on the physical receipt.

The Change: Visa clarified its card network name on receipts requirement in the U.S. region and U.S. territories when the Common AID is selected, and when the network is not known at the time the receipt is generated.

The Impact: Merchants may need to adjust their terminals and receipt-generation logic in order to comply with the revised network name requirements as outlined below:

Effective Dates:

October 14, 2017 New terminals

October 14, 2018 Existing terminals

Criteria:

- The merchant is in the U.S. region or U.S. territories
- The transaction is initiated using the Visa U.S. Common Debit AID from a U.S.-covered debit card
- The processing network is not known at the time the transaction receipt is generated

When the above are true, the transaction receipt must contain:

The application label of Common Debit ("**US DEBIT**") -OR- an enhanced descriptor

[REMINDER] Visa Modifies Interchange Rules for Certain Tax Exempt Charities

CP/CNP/eComm

The Change: Visa will begin to include religious organizations that are classified as tax exempt under section 501(c)(3) of the Internal Revenue Code in the CPS/Charity and CPS/Retail 2 interchange programs.

The Impact: All charitable social service organizations will also be required to have a tax-exempt status under section 501(c)(3).

Additionally, Visa will expand the Fixed Acquirer Network Fee (FANF) charitable and social service organizations rebate to tax-exempt qualified card merchants with greater than 50 percent of total Visa volume for MCCs:

- 8398 Charitable Social Service Organizations
- 8661 Religious Organizations

The Timing: October 2018

[NEW] Visa to Block Europe Contactless Magnetic-Stripe Data Transactions — CP

The Change: Visa will begin to decline all **Europe region-issued** contactless magnetic-stripe data (MSD) transactions identified by the POS Entry Mode value of 91 (contactless device-read-originated using magnetic stripe data rules).

The Impact: Merchants should be aware they will receive declines with a response code of '05' for **Europe region-issued** transactions when identified by the POS entry mode as contactless MSD.

The Timing: October 1, 2018

[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 Implements Interlink Automated Fuel Dispenser (AFD) Partial Authorization Non-Participation Fee — CP/CNP

The Program: Currently there is a $0.01 partial authorization non-participation fee in place for Visa Automated Fuel Dispenser (AFD) transactions.

The Change: Visa is introducing a new partial authorization non-participation fee of $0.01 for each Interlink Automated Fuel Dispenser (AFD) authorization that does not contain the partial authorization participation indicator.

The Impact: Merchants may realize an increase in fees for any Interlink AFD authorizations that do not contain a partial authorization participation indicator.

The Timing: October 1, 2018

[REMINDER] Visa Modifies the Assessment Fee for Credit Products

CP/CNP/eComm

The Change: Visa will be increasing the Assessment fee for credit products. The Debit product Assessment Fee will remain unchanged.

The Impact: Merchants may realize an increase in Assessment Fees for all credit products.

The Timing: January 2019

[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 **is not** U.S. dollars

[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

[NEW] Discover Introduces Acceptance of Debt Repayment — CP/CNP/eComm

The Program: Discover will permit merchants to accept debit cards for the payment of debt.

The Change: Discover is adding a new **Debt Repayment Indicator** to identify merchant participation in the program for the acquirer.

The Impact:

Merchants accepting debit cards for the repayment of debt must:

- Have a unique merchant ID assigned by the acquirer to indicate they are permitted to accept debit cards for debt repayment
- Be assigned one of the following MCCs:
  - 6012 Member Financial Institutions Merchandise and Services
  - 6051 Quasi Cash Merchant
- Ensure cardholders are aware **only debit cards** may be accepted for debt repayment

Merchants may accept debit cards for debt repayment for recurring payment transactions

[NEW] 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**

[NEW] 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] 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

The Timing: October 12, 2018

American Express

[REMINDER] American Express Offline and Online PIN Requirement and Legacy Expresspay Decommission

CP

The Program: Merchants with Chip and PIN POS Systems are required to support both Offline and Online American Express PIN transactions. Merchants are also required to decommission contactless readers utilizing Expresspay 1.0 and 2.x, and should be using American Express' ExpressPay Terminal Specifications 3.0.

The Change:

- All **existing** Chip and PIN POS Systems must be certified to support both Offline and Online PIN **December 31, 2018**.
- Contactless readers supporting **Expresspay Terminal Specification 2.x must be decommissioned by December 31, 2018.**

The Impact: Failure to support new Expresspay Terminal Specifications may result in declines or impact the cardholder experience.

[REMINDER] American Express Adds Support for Zero Value Account Verification

CP/CNP/eComm

The Program: American Express currently permits merchants to use a $1.00 authorization message to validate the cardholder account is valid and in good standing.

The Change: American Express will begin to support Zero Value Account Verification ($0.00) for merchants to validate the cardholder account is valid and in good standing.

The Impact: Merchants currently using the $1.00 authorization message to validate the cardholder account may begin using the Zero Value Account Verification Message.

The Timing: October 2018