Omni Merchant Network Updates Summer 2018

We are committed to working closely with you on achieving your business goals. As a part of this commitment, we carefully monitor Network changes and summarize them for your convenience. Following is the summary of information from American Express®, Discover® Network, MasterCard® Worldwide and Visa® U.S.A. regarding changes or updates to interchange rates, operating rules and regulations, and other changes that may impact your company.

Each article has been tagged or categorized by 'CP' (Card Present), 'CNP' (Card not Present) 'eComm' (eCommerce), or 'Can' (Canada). This notation has been added to better identify the environment the specific article impacts. In order to take advantage of the new category tags and quickly navigate to specific articles, we recommend that you '*show bookmarks*' in your preferred PDF viewer.

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 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.

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

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

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)**
  - *** UnionPay 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 anticipated lifetime to 12/31/2027**

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:

February 1, 2018	Canada Region	Issuers must decline technical fallback transactions
October 12, 2018	Latin America/Caribbean Region	Issuers must decline technical fallback transactions
October 12, 2018	U.S. Region	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 Announces Rule Changes for POS Terminals to support EMV and Contactless in the AP and LAC Regions

CP

The Change: Mastercard is announcing rule changes that will apply to the Asia/Pacific (AP) and Latin America/Caribbean (LAC) regions for POS Terminals.

The Impact: Merchant terminals will be required to support both EMV and contactless technology as outlined in the chart below:

Effective Date	Requirement
October 12, 2018	**All newly-deployed POS terminals***, in the AP and LAC regions, must support both EMV and contactless technology [excludes mobile point-of-sale (MPOS) and integrated POS (IPOS)].
October 18, 2019	**All newly-deployed mobile point-of-sale (MPOS) terminals**, in the AP and LAC regions, must support both EMV and contactless technology.
October 1, 2020	**All newly-deployed Integrated POS (IPOS) terminals**, in the LAC region, must support both EMV and contactless technology.
April 1, 2023	**All deployed terminals** in the LAC region must support both EMV and contactless technology.

* The term POS terminal refers to both attended point-of-sale (POS) and unattended point-of-sale (cardholder activated terminals [CAT]). It does not include ATMs or financial institutions (bank) branch terminals.

[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 that effective January 1st 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 that EMV mode terminals that support CDCVM must also support CDA.

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

[REMINDER] Visa U.S. Contactless Terminal Payment Acceptance Requirements CP

The Program: Current Visa Rules require EMV contactless terminals deployed and activated in the U.S. after April 1, 2013 comply with Visa Contactless Payment Specification (VCPS) Version 2.1.1 or later and be capable of processing transactions using both the magnetic stripe data (MSD) and EMV paths. As of January 1, 2015, the MSD transaction path became optional at these terminals.

Because this requirement only applied to terminals deployed after April 2013, a number of contactless MSD-only terminals remain at U.S. merchant locations. These older terminals have caused contactless processing issues and declines at the point of sale. Many of the terminals cannot be upgraded to EMV due to outdated hardware or other reasons and many are out of compliance with Visa's requirements.

The Change: Merchant terminals in the U.S. region that support contactless MSD payments must:

- Comply with the Visa Contactless Payment Specification (VCPS) 2.1.1 or later
- Actively enable the Quick Visa Smart Debit and Credit (qVSDC) transaction path

– These changes apply to merchants currently accepting contactless payments and merchants that enable contactless acceptance in the future. This requirement does not affect liability.

– Visa may assess non-compliance fees if contactless terminals do not meet technology standards

The Timing: Effective **April 13, 2019**

All Brands: No Signature Rule Changes Announced

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

The Change: Mastercard, Discover, American Express, and Visa have all announced effective **April 2018**; their rules will be updated 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. Sales transacted after April 14, 2018 are not required to have a signature. Signatures are still required to be provided for any disputed transactions that occurred prior to April 14, 2018,

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.

NETWORK	DEMOGRAPHIC AREA	AUDIENCE
American Express	Globally	All Card Present Merchants
Mastercard	United States* Canada	All Card Present Merchants
Discover	United States Canada Mexico Caribbean	All Card Present Merchants
Visa**	**Globally**	Card Present Merchants- **EMV Enabled POS Device**
* Locations in Puerto Rico are still required to obtain a signature		
** Effective October 2018 Visa's no signature rule applies globally		

- Merchants are still required to certify their terminals for signature if the device supports signature as a CVM. Once certified, signature support can be suppressed in production without any additional certification requirement.
- 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. Merchants should consider potential implications to your business practices when determining whether or not to collect signatures. Merchants may choose to continue collecting signatures for verification of additional terms and conditions of a purchase or refund (ex: limited refund policies, travel industry, cancellation policy, accepting tips).

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

CP/CNP

The Credential on File technical requirements document (for the Core platform) has been updated with additional details from the networks and is available for merchant review.

Some of the updates include:

All
- Explanation of the "Pay" products
- Transaction Type Examples

Visa
- Clarification of compliance dates

Mastercard
- POS Entry mode for subsequent transactions
- Requirement for PANs and Network Token clarified

Discover
- Details outlined for POS Entry Mode requirements

The updated document can be viewed on our website, accessed through this link: Credential On File Update

NOTE: For Mastercard transactions we are advising merchants not to implement the Mastercard COF framework until further notice. Currently not all issuers are prepared to support entry mode '10', which may result in transaction declines.

[NEW] 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 work that will be necessary to update their various systems, used for either processing or reporting, ensuring support of the eight digit BIN prior to the APRIL 2022 deadline.

The Timing: April 2022

Mastercard®

[NEW] Mastercard Revises Standards for Multiple Authorization Requests for Card-Not-Present Transactions

CNP/eComm

The Change: Mastercard will update their standards for card-not-present transactions to prohibit subsequent authorization requests when the original authorization response includes any of the decline responses below:

04 - Capture Card
14 - Invalid Card Number
15 - Invalid Issuer
41 - Lost Card
43 - Stolen Card
54 - Expired Card

The Impact: Merchants receiving one of these decline response codes should request a different Mastercard account number from the cardholder for payment.

Note – Mastercard has implemented a process to allow Issuers the ability to report violations.

[NEW] 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 Changes:

- Consolidation of reason codes into 4 categories:
  - Cardholder Dispute
  - Point-of-Interaction Error
  - Authorization Related
  - No Cardholder Authorization
- Blocking invalid chargebacks from entering the network
- Elimination of the Arbitration Chargeback Cycle
- Reducing the time to Resolve.
  - First chargebacks time lines will change from 120 days to 90 days

What remains the same:

- No questionnaires
- Time for merchants to respond to chargebacks remains 45 days

More information, including upcoming webinars to review the new Mastercard Claims Manager program, will be shared with merchants as it becomes available.

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

CP/CNP/eComm

The Change: Mastercard will update their Data Integrity Monitoring Program. Three new edits will be implemented in the Acquirer Clearing Dual Message Program and additional criteria will be added to the existing POS Authorization Edit 10.

The Impact: The edits, along with their compliance dates and potential assessment dates, are listed in the table.

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

[NEW] 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

Visa®

[UPDATE] Visa Introduces Deferred Authorization Indicator — CP/CNP/eComm

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 to identify deferred (store and forward) authorizations.

- Deferred authorizations must be obtained within one (1) day of the transaction date
- MCCs 4111 (Local and Suburban Commuter Passenger Transportation including Ferries) and 4131 (Bus Lines) must obtain an authorization within four (4) days of the transaction date

The Timing: TBD UNTIL FURTHER NOTICE FROM VISA

[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 pass the Card Verification Value 2 (CVV2) for 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 need to 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
- The following 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

[REMINDER] 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 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 identified with Electronic Commerce Indicator = 06.

[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. 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 Change: Visa announced a phased approach for merchant required support of the purchase return authorization message as outlined below:

- Merchants must ensure the data fields below are included for return authorizations and must be submitted with a processing code of "20" in order to properly identify as a credit/refund transaction. Any additional data fields submitted by merchants may be reviewed by the issuer for authorization decisioning and may result in a decline.
    - Primary Account Number
    - Processing Code- 20
    - Transaction Amount
    - Transaction Date
    - Merchant Type (MCC)
    - Country Code
    - POS Entry Mode
    - POS Cond Code
    - Card Acceptor ID (Merchant ID)
    - Card Acceptor name and Location
    - Currency Code
    - Terminal Type
    - Terminal Entry Capability
    - Field 55 ICC Data/EMV Data (when applicable)
- 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.
- 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.

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.

Effective April 13, 2019 Chargebacks

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 and code 11.3, No Authorization.

Effective July 1, 2019 Fees

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

Visa Rules will be updated effective April 13, 2019 with the following clarifications and updates 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 refund 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

[NEW] 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 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 (fDDA). All contactless-only acceptance readers will also be required to support only fDDA. 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

[NEW] 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

[NEW] 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 will realize an increase in Assessment Fees for all credit products.

The Timing: January 2019

[NEW] 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

[NEW] 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.

Discover®

[NEW] 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] 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.

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

[NEW] 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 that all point-of-sale devices are able to identify, accept, and process the expanded JCB BIN ranges. The new BINS are expected to be in market October 2022.

New JCB BIN ranges

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

The Timing: October 2022

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 a 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 a cardholder account is valid and in good standing. (*Merchant support of Zero Value Account Verification is optional*.)

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

The Timing: October 2018

[NEW] American Express Opt Blue Introduces New Emerging Markets Industry Program

CP/CNP/eComm

The Change: American Express is introducing a new tiered Emerging Markets industry program.

The Impact: The new Emerging Markets industry program will apply to the following merchant categories:

- 5960 – Direct Marketing Insurance Services
- 5968 – Direct Marketing Continuity/Subscription Merchant
- 6300 - Insurance
- 8211 – Elementary Schools
- 8220 – Colleges
- 8351 – Child Care Services
- 9211 – Court Costs
- 9222 – Fines
- 9399 – Government Services Not Elsewhere Classified

Current Program	Program Effective October 12, 2018
MCC 5960 & 6300	
B2B/Wholesale Tier 1	
B2B/Wholesale Tier 1 Card Not Present	Emerging Market Tier 1
B2B/Wholesale Tier 2	
B2B/Wholesale Tier 2 Card Not Present	Emerging Market Tier 2
B2B/Wholesale Tier 3	
B2B/Wholesale Tier 3 Card Not Present	Emerging Market Tier 3
MCC 8211, 8220, & 8351	
Education Tier 1	
Education Tier 1 Card Not Present	Emerging Market Tier 1
Education Tier 2	
Education Tier 2 Card Not Present	Emerging Market Tier 2
Education Tier 3	
Education Tier 3 Card Not Present	Emerging Market Tier 3
MCC 9211, 9222, & 9399	
Government Tier 1	
Government Tier 1 Card Not Present	Emerging Market Tier 1
Government Tier 2	
Government Tier 2 Card Not Present	Emerging Market Tier 2
Government Tier 3	
Government Tier 3 Card Not Present	Emerging Market Tier 3
MCC 5968	
Mail/Internet Tier 1	
Mail/Internet Tier 1 Card Not Present	Emerging Market Tier 1
Mail/Internet Tier 2	
Mail/Internet Tier 2 Card Not Present	Emerging Market Tier 2
Mail/Internet Tier 3	
Mail/Internet Tier 3 Card Not Present	Emerging Market Tier 3