Omni Merchant Network Updates Spring 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.

Except where otherwise noted, all changes will be **implemented on April 13, 2018, central processing date of April 14, 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 Automated Fuel Dispenser (AFD) Liability Shift Update CP

The Program: In 2011 and 2012, the Brands (Visa, Mastercard, American Express and Discover) announced an October 2017 EMV liability shift for U.S. acquired AFD transactions under Merchant Category Code 5542 – Automated Fuel Dispensers.

The Change: As a result of the complexities and challenges of implementing EMV at AFDs, a delay in the U.S. Automated Fuel Dispenser (AFD) EMV Liability Shift was announced (in early December) by Visa, MasterCard, American Express and Discover.

The Impact: The new EMV Automated Fuel Dispenser Liability Shift date for Visa, MasterCard, American Express and Discover is **October 2020.**

At this time Vantiv now Worldpay is aware of the following PIN Debit networks that have also announced an October 2020 EMV AFD liability shift date:

- Accel
- AFFN
- Interlink
- Jeanie
- Maestro
- MoneyPass
- NYCE
- PULSE
- Shazam
- STAR

[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 Reminder 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** *
  - ***Must be removed by June 30, 2018***
- 1408-bit keys have expiry date of 12/31/2024
- **1984-bit keys have anticipated lifetime to 12/31/2027**

**** UnionPay has announced that 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] Visa and American Express Chargeback Blocking Edits for Counterfeit Fraud Expiring

CP

The Program: Previously, Visa and American Express implemented temporary EMV chargeback liability changes to provide relief for merchants that did not have POS devices enabled to read a contact chip card due to delayed EMV certification.

The Change: The existing blocking edits, previously introduced by Visa and American Express, for EMV liability shift chargebacks for counterfeit fraud in the U.S. **will be removed effective April 13, 2018**.

The blocking edits below will be removed and as a result merchants may see an increase in these chargeback reason codes:

- 10 Chargeback Maximum per Account
  - Visa currently blocks Reason Code 62 and Interlink Reason Code 2462 chargebacks over 10 per account in a 120-day period
  - American Express currently blocks Reason Code 4798 chargebacks over 10 per account while this restriction is in effect
- $25 Minimum Transaction
  - Visa currently blocks Reason Code 62 and Interlink Reason Code 2462 chargebacks for amounts up to $25
  - American Express currently blocks Reason Codes 4798 and 4799 (lost/stolen) chargebacks for amounts up to $25

[NEW] 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	
October 12, 2018	Latin America/Caribbean Region	Issuers must decline technical fallback transactions
October 12, 2018	U.S. Region	

- 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**

[NEW] 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 Reminder of 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 Updates 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

Security

[REMINDER] Vantiv now Worldpay Ending Support of Legacy Encryption Methods and Weak Encryption Cipher Suites

CP/CNP/eComm

Providing efficient and secure methods of processing payment transactions to our clients is a top priority for Vantiv now Worldpay. As part of these efforts Worldpay will be discontinuing support of legacy encryption methods, such as Secure Socket Layer version 3 (SSLv3) and early versions of Transport Layer Security (TLS).

The PCI Security Standards Council has declared that SSLv3 and early versions of TLS no longer meet minimum security standards, due to security vulnerabilities for which there are no fixes. SSLv3 and early versions of TLS are network protocols that are used to encrypt and protect Internet communications. **Worldpay will end support of legacy network protocols June 30, 2018 (eComm will end support April 30, 2018)**

When Worldpay ends its support of SSLv3 and early TLS, customers that continue to use these protocols will no longer be able to connect to Worldpay using Internet-based services or eCommerce-type applications. In addition, Worldpay will stop supporting weak encryption cipher suites, such as Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES or TDEA).

Merchants and Partners should be in the process of disabling legacy protocols and enabling support of TLSv1.2 for communication with Worldpay platforms prior to the June 2018 date.

To minimize any disruption to processing, Worldpay recommends that our partners and merchants using an ISV solution test TLS-only connectivity to our test host (https://testssl.protectedtransactions.com/auth) to verify you are able to support required protocols.

Certification Environment Update

As part of our TLS remediation efforts, Worldpay made changes to our certification environment (certssl.protectedtransactions.com) on Wednesday, March 28, 2018 to no longer allow connections using legacy protocols (sslv3 and early TLS).

As a result of this change, certssl.protectedtransactions.com will support only TLS 1.2 encryption. In order to prevent connectivity issues to our certification environment, merchants and partners should disable SSLv3 and early versions of TLS accordingly.

[REMINDER] Vantiv now Worldpay Ending Support of Legacy Encryption Methods and Weak Encryption Cipher Suites (cont.)

For encryption, Worldpay will only support cipher suites based on Elliptic Curve Diffie-Hellman (ECDHE) and RSA key exchange, Advanced Encryption Standard (AES), and Secure Hash Algorithms (SHA).

A list of supported ciphers in order of preference is below:

Cipher ID	Cipher Name
c030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
c02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
c028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
c014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
c027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
c013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
009d	TLS_RSA_WITH_AES_256_GCM_SHA384
009c	TLS_RSA_WITH_AES_128_GCM_SHA256
003d	TLS_RSA_WITH_AES_256_CBC_SHA256
003c	TLS_RSA_WITH_AES_128_CBC_SHA256
0035	TLS_RSA_WITH_AES_256_CBC_SHA
002f	TLS_RSA_WITH_AES_128_CBC_SHA

Terminal Merchants

For terminals identified as requiring a software download in order to support the minimum network encryption protocol, merchants should visit https://www.vantiv.com/download and follow the Full Download steps for their specific terminal model. If merchants require assistance with the download process, they may contact our technical support team at 888-720-6822.

It's important that merchants complete the terminal download process as soon as possible. Merchants that have not completed the necessary software download prior to the deadline will not be able to communicate with Worldpay processing platforms.

Worldpay is committed to maintaining a high level of security for our customers and aligning with industry standards and best practices for information security. If you have any questions regarding these changes please contact your Relationship Manager.

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. 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.

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	U.S. Region Canada U.S. Territories	Card Present Merchants- EMV Enabled POS Device
* Locations in Puerto Rico are still required to obtain a signature		

- 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. We will communicate additional details and updates as we receive information from the networks.
- **A comprehensive document outlining the technical requirements and chargeback impact for each network is being developed and will be shared with merchants when completed.**

Mastercard®

[REMINDER] Mastercard New 2-Series MasterCard BIN Range — CP/CNP/eComm

The Program: MasterCard has added new primary account **BIN ranges 222100-272099** to be processed in the same manner as existing range 510000-559999. Merchants are encouraged to visit www.mastercard.us/2-series for additional information.

The Impact: Merchants should now be able to accept the new MasterCard BIN range in ALL payment acceptance channels.

To ensure merchant compliance, Mastercard has implemented acquirer reporting for merchants identified as not being able to support the new 2-Series BIN.

- Mastercard is currently reporting to Vantiv now Worldpay merchants that have been identified as being unable to support the new 2-Series BIN
- Vantiv now Worldpay is working directly with merchants to address non-compliance
- A 'cure period' is being provided to merchants to resolve the acceptance issue
- **Merchants must demonstrate the acceptance issue is resolved by successfully processing a 2-Series BIN transaction from the identified acceptance location to avoid non-compliance assessments**

[REMINDER] Mastercard Eliminates CVC2 at Chip POS or MPOS Terminals for Chip Transactions — CP

The Change: Mastercard will discontinue their CVC2 validation program in lieu of a card imprint for chargeback purposes for U.S. domestic transactions, effective April 21, 2018**.**

The Impact: Merchants may not prompt or otherwise require a cardholder to enter CVC2 information when a chip card or contactless payment device is used to complete a chip transaction. This includes any contactless transaction at a POS terminal or MPOS terminal.

The Timing: April 21, 2018

[NEW] Mastercard Announces Support of New Authorization Procedures for Credential (Card) on File [Merchant Initiated and Cardholder-Initiated] Transactions CP/CNP/eComm

The Program: In an effort to improve authorization approvals, Mastercard is mandating support of new authorization procedures for credential on file merchant-initiated and cardholder-initiated transactions applicable to primary account number (PAN) and network token transactions.

The Change: Mastercard will require acquirers and merchants to support authorization and settlement changes to clearly identify subsequent credential on file transactions to improve authorization approvals. These changes apply to Primary Account Number (PAN) and network token transactions. Merchants that do NOT store the consumers' payment credentials are not impacted by these changes.

Effective Dates:

June 12, 2018	All regions excluding Canada (Mastercard non-compliance assessment may begin in October 2018)
October 12, 2018	Canada

Initial Storage of a Payment Credential (Card present, mail order/phone order, e-commerce, Account Status Inquiry

- During a purchase (e.g., e-commerce or during a phone order) when the merchant is instructed to store the payment credential for future purchases
- Cardholder contacts the merchant to store their payment credential for the next time goods/services are purchased

Mastercard is NOT requiring merchants to identify the intent to store the payment credential in initial transactions.

Subsequent Transactions Using a Stored Payment Credential
A merchant or cardholder may initiate a transaction using a stored credential.

Cardholder Initiated Example: The cardholder shops from a mobile device by accessing the merchant's app or website. When it's time to check-out, the merchant has the cardholder's payment credentials, shipping and billing address on file.

These transactions must contain the following Mastercard fields/values:
- POS Entry Mode of '10' in authorization requests
- POS Entry Mode of '7' in settlement

Merchant Initiated Example: The cardholder has an agreement with a merchant to process a transaction based on the conditions of the agreement. The transaction is related to a previous consumer-initiated transaction, but is conducted without the consumer being present or validation (mag-stripe data, chip cryptogram data, CVC2 or 3DS authentication).

Standing Instructions - Recurring, Installment

Transactions must contain the following Mastercard fields/values:
- POS Entry Mode of '10' in authorization requests
- POS Entry Mode of '7' in settlement

Mastercard is updating the Account Status Inquiry ($0.00) to include the POS Entry Mode of 10, if the merchant wants to use the message to check the status of the account in conjunction with an already stored payment credential.

Merchants are not required to submit an Account Status Inquiry if they intend to store the payment credential.

[NEW] 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.

NEW CLEARING EDITS

- **Edit Number 13 – MCC Match** (The authorization MCC must match the clearing/settlement MCC)
  - *June 1, 2018* Compliance of MCC Match Edit
  - *July 2018* Possible non-compliance assessments

- **Edit Number 14 – Merchant DBA Name Match** (The authorization DBA must match the clearing/settlement DBA)e
  - *December 1, 2018* Compliance of Merch_DBA_Name_Match Edit
  - *January 2019* Possible non-compliance assessments

- **Edit Number 16** - **Terminal Input Match** (The authorization Terminal Input Capability Indicator must match the clearing/settlement Terminal Input Capability Indicator).
  - *June 1, 2019* Compliance of Term_Input_Match Edit
  - *July 2019* Possible non-compliance assessments

UPDATES TO EXISTING CLEARING EDITS

Edit Number 10 – POS Authorizations

- POS Authorization message value (**data element 22, subfield 1**) and POS Clearing message value (**data element 22, subfield 7**) for ***POS Entry Mode data*** are not in agreement.
  - *June 1, 2019* Compliance of POS_Auth Edit
  - *July 2019* Possible non-compliance assessments

Criteria added: Clearing/Settlement POS Entry Mode, when compared to Authorization POS Entry Mode, has one of the following mismatch conditions:

- Clearing value is 0 (unspecified) and Authorization value is not 00 (PAN entry mode unknown)
- Clearing value is 1 (manual input; no terminal) and Authorization value is not 01 (PAN manual entry)
- Clearing value is 2 (Magnetic stripe reader input) and Authorization value is not 02 (PAN auto-entry via magnetic stripe- track data not required)
- Clearing value is 0 (unspecified) and Authorization value is not 03 (PAN auto-entry via bar code reader)
- Clearing value is 0 (unspecified) and Authorization value is not 04 (PAN auto-entry via optical character reader)
- Clearing value is C (Online Chip) and Authorization value is not 05 (PAN auto-entry via chip)
- Clearing value is M (PAN auto-entry via contactless M/Chip) and Authorization value is not 07 (PAN auto-entry via contactless M/Chip)
- Clearing value is R (PAN entry via electronic commerce, including remote chip) and Authorization value is not 09 (PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55)
- Clearing value is 6 (Key entered input) and Authorization value is not 79 (Hybrid terminal with an online connection to the acquirer failed in sending a chip fallback transaction to the issuer)

[NEW] Mastercard Updates Existing Edits and Adds New Edits to Data Integrity Monitoring Program (cont.)

CP/CNP/eComm

- Clearing value is B (Magnetic stripe reader input; track data captured and passed unaltered) and Authorization value is not 80 (Chip card at chip-capable terminal was unable to process transaction using data on the chip; therefore, terminal defaulted to the magnetic stripe-read PAN)
- Clearing value is S (electronic commerce) and Authorization value is not 81 (PAN/Token entry via electronic commerce with optional SecureCode-AAV or DSRP cryptogram in UCAF.
- Clearing value is T (PAN auto entry via server) and Authorization value is not 82 (PAN auto-entry via Server)
- Clearing value is B (Magnetic stripe reader input; track data captured and passed unaltered) and Authorization value is not 90 (PAN auto-entry via magnetic stripe)
- Clearing value is A (PAN auto-entry via contactless magnetic stripe) and Authorization value is not 91 (PAN auto-entry via contactless magnetic stripe)
- Clearing value is C (Online Chip) and Authorization value is not 95 (Visa only. Chip card with unreliable Card Verification Value (CVV) data)

[NEW] Mastercard Updates Interchange Programs for Government Owned Lottery Transactions, MCC 7800

CP/CNP/eComm

The Change: Mastercard is making a change to allow government owned lottery transactions under MCC 7800 to qualify for more preferred rates on consumer credit, debit, and prepaid card transactions.

The Impact: Eligible merchants will see a change in the interchange programs their transactions qualify for.

Current Eligible Interchange Programs for MCC 7800	Eligible Interchange Programs for MCC 7800 Effective April 13, 2018*
Merit I Core	Convenience Purchases Core & Enhanced
Merit I Enhanced	Convenience Purchases World, World High Value & World Elite
Merit I World	Convenience Purchases Core & Enhanced Tier 1
Merit I World High Value & World Elite	Convenience Purchases World Tier 1
Merit I Debit	Convenience Purchases World High Value & World Elite Tier 1
Merit I Prepaid	Public Sector Core, Enhanced, World, World High Value & World Elite
Merit III Core	Small Ticket Debit & Prepaid
Merit III Enhanced	Small Ticket Debit & Prepaid Tier 1
Merit III World	Emerging Markets Debit & Prepaid
Merit III World High Value & World Elite	
Merit III Debit	

*Convenience Purchase and Small Ticket interchange programs are for card present/swiped transactions only. Public Sector and Emerging Markets are for both card present and card not present transactions

Visa®

[REMINDER] Visa Modifies Timing for Prohibiting Card Verification Value 2 (CVV2) in Authorization of Card-Present Key-Entered Transactions

CP

The Program: Visa currently permits merchants to request cardholders provide their Card Verification Value 2 (CVV2) for additional verification of card-present key-entered transactions.

The Change: Visa announced they will no longer permit merchants to collect CVV2 data from cardholders or to submit CVV2 data in the authorization request for a card-present key-entered transaction.

The Impact:

Effective April 14, 2018

- Merchants cannot collect the CVV2 value from the cardholder for card-present key-entered transactions
- Merchants cannot submit the CVV2 value in card-present key-entered authorization requests
- CVV2 in lieu of imprint will no longer be supported for chargeback reason code 81. Merchants will be required to obtain a manual imprint of the card when the transaction is key-entered
- Visa will prohibit the use of CVV2 for all electronically read card-present transactions unless the merchant complies with all of the criteria below:
    - U.S. merchant has an EMV chip enabled POS device
    - U.S merchant has an agreement with the issuer
    - The transaction payment product was electronically read (magnetic stripe, contactless or contact)

[REMINDER] Visa Updates Chargeback Rules for Card-Not-Present Transactions Approved with CVV2 Mismatch

CNP

The Program: Merchants are encouraged to use CVV2 as part of their fraud prevention efforts for processing card-not-present transactions.

The Change: Issuers in all regions will no longer be able to chargeback U.S. card-not-present transactions (fraud) that have been approved with a card verification value (CVV2) mismatch response.

The Impact: Visa will block U.S. chargebacks (Reason Code 83) when the original card-not-present transaction was approved with a CVV2 mismatch response. Merchants are protected from Reason Code 83 when:

- Domestic or International transaction
- Card-not-present transaction
- CVV2 result is a mismatch
- Issuer approves the authorization

Chargeback rights will remain the same for transactions submitted for authorization without CVV2.

Merchants may receive declines with auth response code of N7 when the CVV2 is a mismatch. Merchants will have the opportunity to collect the correct CVV2 and try the authorization again.

[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 will 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 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 identified with Electronic Commerce Indicator = 06.

[REMINDER] Visa Updates Rules and Testing Requirements for Verified by Visa (VbV) and Clarifies MCCs Ineligible for Chargeback Protection in the U.S.

eComm

The Change: Visa is updating their rules and testing requirements for their Verified by Visa program to address new functionality and ensure global consistency. Visa has also identified Merchant Category Codes (MCCs) that will not be eligible for chargeback protection for Transaction Not Recognized and Fraud: Card Absent Environment.

The Impact and Timing:

October 14, 2017
The current VbV information security requirement that prohibits merchants from storing VbV verification data subsequent to authorization will be updated to clarify that *VbV verification data refers to the Cardholder Authentication Verification Value (CAVV).*

October 14, 2017
VbV data requirements will be updated to require merchants and issuers using 3-D Secure 2.0 to provide the following information in 3-D Secure 2.0 messages:

- Transaction Type
- 3-D Secure Service Operation ID
- ACS Operator ID

April 14, 2018
The data exchanges between VbV participants should only be used for purposes associated with the VbV program. A new rule clarifies that cardholder confidential information must not be used for marketing purposes or disclosed to a third party.

3-D Secure 2.0 Testing Requirements
Clients that participate in Visa's 3-D Secure 2.0 program must ensure its 3-D Secure 2.0 solutions have successfully met EMVCo's 3-D Secure 2.0 functional requirements and have successfully completed Visa's 3-D Secure 2.0 Test Suite requirements.

April 14, 2018
The following MCCs are not eligible for chargeback protection for Transaction Not Recognized and Fraud: Card Absent Environment:

- MCC 4829—Wire Transfer Money Orders
- MCC 5967—Direct Marketing: Inbound Teleservices Merchant
- MCC 6051—Non-Financial Institutions: Foreign Currency, Money Orders [not Wire Transfer], Stored Value Card / Load, and Travelers Cheques
- MCC 6540—Non-Financial Institutions: Stored Value Card Purchase / Load NEW
- MCC 7801—Government Licensed On-Line Casinos (On-Line Gambling) NEW
- MCC 7802—Government-Licensed Horse / Dog Racing NEW
- MCC 7995—Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks

[REMINDER] Visa Enforces Verified by Visa (VbV) Transaction Data Integrity eComm

The Program: In an effort to improve transaction data integrity and effectively manage chargeback liability, Visa will begin to change the Cardholder Authentication Verification Value (CAVV) Result Code and Electronic Commerce Indicator (ECI) value when the CAVV is missing or cannot be verified in the authorization request for Verified by Visa (VbV) transactions.

The Change: Visa will change the CAVV Result Code Value to a value of '0' (CAVV could not be verified or CAVV data was not provided when expected) and will also change the eCommerce indicator (ECI) to a value of '07' (non-authenticated security transaction) based on the following authorization request criteria:

- A transaction is Verified by Visa (VbV) identified with an eCommerce indicator of 05 (fully authenticated) or 06 (attempted cardholder authentication)
- Cardholder Authentication Verification Value (CAVV) is not present in the authorization request
- Transaction initiated with a primary account number or token

Vantiv will accept the CAVV Result Code and the changed ECI value in the authorization response.

The Impact:

- Merchants participating in VbV must ensure that they are passing the proper ECI value and valid CAVV data for fully authenticated and attempt to authentication transactions
- Merchants processing In-app transactions (e.g., Apple Pay, Samsung Pay) must ensure that they are passing the proper ECI values and CAVV data

Effective October 2017:	AP and Canada Region
Effective April 2018:	U.S. Region
TBA:	LAC

Merchants must be aware that transactions that contain an eCommerce indicator of '07' are not eligible for VbV chargeback protection.

[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:

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.

- 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

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

CP/CNP/eComm

The Program: In an effort to improve authorization approvals, Visa has mandated support of new authorization procedures for credential on file merchant-initiated and cardholder-initiated transactions applicable to network token transactions.

The Change: Visa mandated that acquirers and merchants support various authorization and settlement changes to clearly identify initial and subsequent credential on file transactions to improve authorization approvals. These changes are **required for network token transactions** and are *recommended for Primary Account Number (PAN) and transactions.*

Initial Storage of a Payment Credential

- During a purchase (e.g., e-commerce or during a phone order) when the merchant is instructed to store the payment credential for future purchases
- Cardholder contacts the merchant to store their payment credential for the next time goods/services are purchased

Visa requires merchants that intend to store the payment credential to submit an Account Number Verification Request ($0.00) or a financial authorization request and receive an authorization approval prior to storing the payment credential.

The Account Number Verification Request ($0.00) and financial authorization request must contain the **POS Environment Field and one of the following indicators:**

- R - (Recurring Payment)
- I - (Installment Payment)
- C - (Credential on File)

Merchants (e.g., lodging, vehicle rentals, cruise lines, transit, transportation, restaurants, bars, eligible rental merchants, amusement parks) participating in initial and estimated authorizations will be required to send the Additional Authorization Indicator (previously named the Partial Auth Indicator) to identify the authorization as initial/estimated authorization in the authorization request.

- 2- Estimated amount
- 3- Estimated amount and terminal accepts partial authorization responses

Subsequent Transactions Using a Stored Payment Credential

Cardholder Initiated- the cardholder shops from their mobile device by accessing the merchant's app or website and when it's time to pay for the purchase, the merchant has the cardholder's payment credentials, shipping and billing address on file.

Transactions must contain the following:

- POS Entry Mode of 10- sent in authorization requests and settlement; values must match from authorization to settlement

[REMINDER] Visa Authorization Procedures for Credential (Card) on File [Merchant-Initiated and Cardholder-Initiated] Transactions (cont.) CP/CNP/eComm

Merchant Initiated- the cardholder has an agreement with the merchant to process a transaction based on the conditions of the agreement. The transaction is related to a previous consumer-initiated transaction, but is conducted without the consumer being present or validation (mag-stripe data, chip cryptogram data, CVV2 or VbV authentication).

Transactions must contain the following:

- POS Entry Mode of 10- sent in authorization requests and settlement; values must match from authorization to settlement
- Transaction ID must be sent in the authorization request

Standing Instructions - Recurring, installment, unscheduled credential on file

Transactions must contain following:

- POS Entry Mode of 10- send in authorization requests and settlement; values must match from authorization to settlement
- POS Environment Field- send in authorization requests and settlement; values must match from authorization to settlement
    - R - (Recurring Payment)
    - I - (Installment Payment)
    - C - (Credential on File)

* U.S. merchants must continue to also send the existing bill payment indicators to meet CPS interchange qualification requirements.

Industry Practice-Incremental, resubmission, reauthorization, no show and delayed charges authorization requests

Transactions must contain following:

- POS Entry Mode of 10- send in authorization requests and settlement; values must match from authorization to settlement.
- Transaction ID must be sent in the authorization request
- Reason Code- send in authorization requests and settlement; values must match from authorization to settlement. Auth reversals must contain a valid value for the reversal and not the message reason code.
    - 3900- Incremental (optional for U.S. merchants, required for non-U.S. merchants)
    - 3901- Resubmission
    - 3902- Delayed charges
    - 3903- Reauthorization
    - 3904- No show

[REMINDER] Visa Authorization Procedures for Credential (Card) on File [Merchant-Initiated and Cardholder-Initiated] Transactions (cont.) CP/CNP/eComm

- Merchants that do not send the proper authorization indicators for credential on file transactions may receive declined authorization responses
- Merchants engaged in initial, estimated, or incremental authorizations will be required to submit the applicable authorization indicator in the first authorization request.
- These changes do not apply to merchants that do NOT store the consumers' payment credential
- These changes are *recommended* for merchants that store the Primary Account Number (PAN) only
- Merchants must ask the cardholder if they would like to have their payment credential stored prior to the submission of the authorization request

The Credential on File technical requirements document (core platform) is available for merchant review and can be accessed through this link: **Credential On File_Core032018**

[REMINDER] Visa Changes to Minimum Disclosure and Cardholder Agreement Requirements for Partial and Full Prepayment Transaction Types

CP/CNP/eComm

The Change: Visa is introducing minimum requirements for merchants when establishing prepayment and credential on file agreements with cardholders. This should help to minimize cardholder confusion, chargebacks, complaints, and potential subscription traps.

The Impact: Merchants that establish prepayment agreements should:

- include proper disclosure requirements at the point of sale, separate from the general terms and conditions of sale
- obtain the cardholder's express and informed consent to the terms related to each transaction type below
- clearly present the requirements related to the transaction types listed below at the time the cardholder provides consent

Prepayment (Partial)
Visa Definition for Prepayment (Partial) Payment for merchandise or services paid in advance which are to be provided at an agreed time that is later than the time of the transaction. • Partial prepayment is less than the cost of merchandise or services purchased and must be applied to total obligation.
Use Case- Cardholder preorders merchandise from the merchant. Prepays for half, and then pays the remaining half when the merchandise is ready to be picked up. Cardholder pays merchant for services (half before the job starts and half when the job is completed)
Disclosure to Cardholder and Cardholder Consent- Prepayment (Partial) When entering into a Cardholder agreement, all requirements below must be clearly displayed at the time that the Cardholder gives their consent and must be displayed separately from the general purchase terms and conditions. Where required by applicable laws or regulations, the merchant or its agent must also provide to the cardholder a record of the cardholder's consent.
The Merchant must provide, and the cardholder must consent to, all of the following in writing at the time of the first or only partial prepayment: • Description of promised merchandise or services • Terms of service • Timing of delivery to Cardholder • Transaction amount • Total purchase price • Terms of final payment, including the amount and currency • Cancellation and refund policies • Date and time that any cancellation privileges expire without prepayment forfeiture • Any associated charges

[REMINDER] Visa Changes to Minimum Disclosure and Cardholder Agreement Requirements for Partial and Full Prepayment Transaction Types (cont.) CP/CNP/eComm

Prepayment (Full)
Visa Definition for Prepayment (Full) Payment for merchandise or services paid in advance which are to be provided at an agreed time that is later than the time of the transaction. • Full prepayment must be equal to the cost of merchandise or service purchased
Use Case- Custom merchandise or services, Face-to-face environment, where not all items purchased in the transaction are immediately available but will be shipped or provided later, recreational services or activities related to tourism and travel, T&E. (Ex. Cardholder purchase shoes from a merchant but they don't have their size. Cardholder can pay for the shoes and have them shipped to their house when they become available.)
Disclosure to Cardholder and Cardholder Consent- Prepayment (Full) When entering into a cardholder agreement, all the requirements below must be clearly displayed at the time the cardholder gives their consent and must be displayed separately from the general purchase terms and conditions. Where required by applicable laws or regulations, the merchant or its agent must also provide to the cardholder a record of the cardholder's consent.
The Merchant must provide, and the cardholder must consent to, all of the following in writing at the time of the first or only partial prepayment: • Description of promised merchandise or services • Terms of service • Timing of delivery to Cardholder • Transaction amount • Refund policies • Date and time that any refund privileges expire without prepayment forfeiture • Any associated charges

[NEW] Visa Updates Chip Debit Interchange Program in Canada CAN

The Change: Visa is eliminating the existing Chip Debit interchange program in the Canada region.

The Impact: Transactions currently qualifying for the Visa Chip Debit interchange program will shift to the existing Standard Debit Interchange program. There is no financial impact as the rates for both interchange programs are the same.

Current Interchange Program	Effective April 13, 2018
Chip – Debit	Standard - Debit

[NEW] Visa Implements Interlink Automated Fuel Dispenser (AFD) Partial Authorization Non-Participation Fee — CP

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.

Effective Date: October 1, 2018

[REMINDER] Visa Introduces New Credit Integrity Fee — CP/CNP/eComm

The Change: Visa will introduce a new $0.10 transaction integrity fee applicable to credit transactions that do not meet the CPS qualification standards.

The Impact: Merchants will see the new credit integrity fee will be assessed on Consumer Credit, Corporate and Purchasing, and Business non-CPS qualified transactions.

[REMINDER] Visa Outlines FANF Fee Changes — CP/CNP

The Change: Visa will modify select tiers of the Fixed Acquirer Network Fee (FANF) applicable to Customer Not Present, Unattended Terminals and Fast Food Restaurant merchants. There will be no changes to the other FANF tables.

The Impact: Merchants with more than $199,999.99 in gross monthly sales volume will see an increase in their monthly FANF fees.

Discover®

[NEW] Discover Updates Rates for PSL Recurring Interchange Program — CP/CNP/eComm

The Change: Discover is modifying the rate for the PSL Recurring interchange program on Premium consumer credit card transactions.

The Impact: Merchants may realize an increase in interchange fees for transactions in the Discover PSL Recurring Premium Program.

[NEW] Discover Introduces New International Interchange Programs CP/CNP/eComm

The Change: Currently they have one International Electronic interchange program and rate for consumer credit, consumer debit and commercial. Discover is introducing new International Electronic interchange programs.

The Impact: The International Electronic interchange programs will be assessed when a U.S. merchant accepts a non-U.S. issued card.

Current Interchange Program	Effective April 13, 2018
International Electronic	International Electronic Consumer Debit/Prepaid
	International Electronic Consumer Credit
	International Electronic Commercial

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.

[NEW] American Express Updates Prohibited Industry List, Approving Opt Blue Eligibility

CP/CNP/eComm

The Change: American Express has made changes to their prohibited industry list. American Express will remove two merchants segments from the prohibited list, and as a result, these segments will now be eligible for signing under the Opt Blue Program. American Express has also added a new MCC to their prohibited list.

The Impact: Merchant segments that have been removed from the prohibited list (eligible MCCs) are now able to participate in the Opt Blue program. MCCs added to the prohibited list are not eligible for the Opt Blue program.

MCCs removed from the prohibited list, now eligible for Opt Blue:

- 5172 – Petroleum & Petroleum Products – Wholesale (U.S. and Puerto Rico)
- 5818 – Digital Goods, Large Digital Goods Merchant (U.S. and Puerto Rico)

Newly added prohibited MCCs:

- 6540 – Non-Financial Institutions – Stored Value Card Purchase/Load

[NEW] 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 that 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 that the 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 will need to begin using the Zero Value Account Verification Message.

The Timing: October 2018