Omni Merchant Network Updates Winter 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 in your Network Updates 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 this information.

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 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

[NEW] 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.

[REMINDER] 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**

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**.

[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

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

The Program: Current Visa Rules require that 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 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

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

The Timing: Effective April 13, 2019

All Brands: No Signature Rule Changes Announced

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

The Change: Mastercard, Discover, American Express, and Visa have all announced that 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 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.

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

Network	Regions	Audience
Mastercard	United States Canada	All Card Present Merchants
Discover	United States Canada Mexico Caribbean	All Card Present Merchants
American Express	Globally	All Card Present Merchants
Visa	North America	EMV Enabled Merchants (contact or contactless chip)

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. 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 Timing: **April 2018**

MasterCard®

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

The Program: MasterCard is adding 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 must be able to accept the new MasterCard BIN range in ALL payment acceptance channels.

All merchant locations should now be able to accept the new MasterCard 2-Series BIN ranges.

MasterCard has implemented a compliance process for merchants identified as not being able to support the new 2-Series BIN.

- MasterCard has begun identifying Vantiv merchants that are unable to support the new 2-Series BIN based upon their field testing
- Vantiv 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 previously communicated the discontinuance of the CVC2 validation program in lieu of a card imprint for chargeback purposes for U.S. domestic transactions, effective April 21, 2017. **MasterCard has announced a delay in the effective date until 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

The CVC2 validation program in lieu of a card imprint for chargeback purposes for U.S. domestic transactions (merchants and issuers are both within the U.S. region) ***will remain in effect until April 21, 2018***

[NEW] MasterCard Assessment Fee Increase

CP/CNP/eComm

The Program: MasterCard periodically reviews and evaluates their fee structures in an effort to accommodate system enhancements and improvements. As a result, MasterCard will increase their Assessment fee, which will continue to be assessed based on gross MasterCard sales volume.

The Change: MasterCard will increase the assessment for consumer and commercial credit transactions less than $1000.

The Impact: Merchants will see an increase in the MC assessment fee billing for April on the invoice received in early May.

The Timing: April 1, 2018

[NEW] MasterCard Introduces New Global Wholesale Travel B2B Transaction Fee

CP/CP/eComm

The Program: The Commercial Global Wholesale Travel interchange program, introduced in April 2015, is available to merchants in the travel related MCCs listed in the table below.

3000-3299 – Airlines	7011 – Lodging
3351 – 3441 – Car Rental	7012 – Timeshares
3501 – 3999 – Lodging	7032 – Sporting Camps
4112 – Passenger Railways	7033 – Trailer Parks
4131 – Bus Lines	7298 – Beauty Spas
4411 – Cruise Lines	7512 – Car Rental
4511 – Airlines	7513 – Truck Rental
4582 – Airports	7519 – Motor Home Rentals
4722 – Travel Agencies	7991 – Tourist Attractions
5962 – Direct Marketing – travel services	7997 – Membership Clubs
6513 – Rental Agencies	7999 – Recreation Services

The Change: Mastercard will assess the new Global Wholesale Travel B2B Transaction Fee on transactions qualifying for the Commercial Global Wholesale Travel interchange program. The rate for the new Global Wholesale Travel B2B fee will vary by region (US, LAC, and AP)

Interchange will not be impacted by the new fee and will continue to be assessed.

The Timing: **January 1, 2018**

Visa®

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

The Program: Visa previously announced that merchants would no longer be permitted to request a cardholder to provide their Card Verification Value 2 (CVV2) for a card-present key-entered transaction effective April 22, 2017.

The Change: On December 8, 2016, Visa announced an extension to their previous announcement prohibiting a merchant from collecting the CVV2 data from the cardholder and entering CVV2 data in the authorization request for a card-present key-entered transaction as of April 22, 2017.

The Impact: Merchants are permitted to collect and include the Card Verification Value 2 (CVV2) information in the authorization request for U.S. domestic **card-present, key entered transactions until April 14, 2018**.

** The original date of April 22, 2017 will still apply to the AP, Canada, CEMEA, Europe and LAC regions*

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 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:

- Merchant and Issuer in the U.S.
- Card-not-present transaction
- CVV2 result is a match
- 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.

The Timing: April 2018

[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

[NEW] 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 (Reason Codes 75 and 83)

- *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.

[NEW] Visa Updates Rules and Testing Requirements for Verified by Visa (VbV) and Clarifies MCCs Ineligible for Chargeback (reason codes 75 and 83) Protection in the U.S.

eComm

The Change: Visa is updating their rules and testing requirements for Verified by Visa program to be more consistent globally and to address new functionality. Visa has also identified Merchant Category Codes (MCCs) that will not be eligible for chargeback protection for reason codes 75 and 83.

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 under reason codes 75 (Transaction Not Recognized) and 83 (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

[UPDATE] 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.

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

CP/CNP/eComm

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

The Change: Visa previously communicated an effective date of April 2018 for merchants and acquirers to begin submitting authorizations for purchase returns and credits. Visa has recently announced **a new 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 chargeback reason code 71 (declined Authorization) and 72 (No Authorization, as applicable)
- **Effective April 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.

Vantiv continues to work directly with Visa to further define the requirements associated with this change. Updates will continue to be shared through your Relationship Manager.

[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 has 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 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 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

[NEW] 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 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

The Timing: **April 14, 2018**

[NEW] Visa Modifies U.S. Debt Repayment and Interchange Program — CP/CNP

The Change: Visa will replace the existing U.S. Consumer Debt Repayment program with two new Debt Repayment programs.

The Impact: The new programs will include all eligible loan types and will require priority routing.

Debt Repayment 1 Program – No fees, will not allow for cardholder fees
Debt Repayment 2 Program – Will permit the use of convenience fees (as outlined in Visa's rules)

The following requirements apply to participants of either Debt Repayment program:

- Register for the program(s)
- Send a Merchant Verification Value (MVV) in the transaction
- Use the debt repayment indicator in the auth and clearing
- Use priority routing for as long as they are in the program

The Timing: Effective Immediately

Interested merchants should contact their Relationship Manager to review the full list of registration requirements.

[NEW] Visa Introduces New B2B Virtual Service Fee — CP/CNP/eComm

The Program: The Commercial B2B Virtual Payments interchange program, introduced in April 2017, is available to merchants in the travel related MCCs listed in the table below.

3000-3299 – Airlines	7011 – Lodging
3351 – 3441 – Car Rental	7012 – Timeshares
3501 – 3999 – Lodging	7032 – Sporting Camps
4112 – Passenger Railways	7033 – Trailer Parks
4131 – Bus Lines	7298 – Beauty Spas
4411 – Cruise Lines	7512 – Car Rental
4511 – Airlines	7513 – Truck Rental
4582 – Airports	7519 – Motor Home Rentals
4722 – Travel Agencies	7991 – Tourist Attractions
5962 – Direct Marketing – travel services	7997 – Membership Clubs
6513 – Rental Agencies	7999 – Recreation Services

The Change: Visa will assess the new B2B Virtual Service Fee on transactions qualifying for the Commercial B2B Virtual Payments interchange program. The rate for the new B2B Virtual Service fee will vary by region (US, LAC, and AP). Interchange will not be impacted by the new fee and will continue to be assessed.

The Timing: January 1, 2018

[NEW] Visa Introduces New Credit Integrity Fee — CP/CP/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.

The Timing: April 2018

[NEW] 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.

The Timing: April 2018

American Express®

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

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

The Change:

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

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

[REMINDER] Vantiv Ending Support of Legacy Encryption Methods, SSLv3 TLS 1.0 and Weak Encryption Cipher Suites June 2018

CP/CNP/eComm

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. As a result, **Vantiv will end its support of these two network protocols by June 30, 2018**. When Vantiv ends its support of SSLv3 and early TLS, customers that continue to use these protocols will no longer be able to connect to Vantiv using Internet-based services or eCommerce-type applications.

Merchants and Partners should be in the process of disabling legacy SSLv3 and TLSv1.0 protocols and enabling support of TLSv1.2 for communication with Vantiv platforms prior to the June 2018 date.

In addition, Vantiv will stop supporting weak encryption cipher suites, such as Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES or TDEA). **While Vantiv will continue support of TLSv1.1, we strongly recommend TLSv1.2 as a long-term solution.**

For encryption, Vantiv 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

To minimize any disruption to processing, Vantiv 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 TLSv1.1 or greater protocol.

For merchants using a stand-alone terminal solution, you will receive information directly if your terminal requires a software download in order to connect via TLS 1.1 or above.

Vantiv is committed to maintaining a high level of security for our customers and aligning with industry standards and best practices for information security, and we thank you for your support of these efforts.