
# Hardware/Software Compliance Update

**Spring Mandate Notification – February 2015**

## 2015 Spring Mandate Notification

CO-OP Financial Services will implement the code changes required to support card association and EFT network Spring Mandates on **Friday, April 17, 2015**, unless otherwise noted.

CO-OP has identified requirements that may impact your host processor. The requirements in support of these mandates are detailed in this update. While CO-OP forwards copies of our Hardware/Software Compliance Updates to our known software vendor contacts, it is up to each credit union to check with their software vendor to make sure their vendor has the information needed to support these changes. If a 3rd party authorizes transactions on your behalf, often referred to as a service bureau, you should forward this information to them.

Please note: **DataNavigator will be taken offline at 7 p.m. PT on April 17, 2015**, to install the code changes required to support the mandates. DataNavigator will be unavailable for approximately two hours.

Questions regarding your credit union network participation should be verified with the sponsorship or contracts administrator within your organization. Some credit unions have issued a Debit MasterCard with Plus sponsorship or a Visa Debit card with Cirrus sponsorship. In these cases, both the MasterCard and Visa changes would apply.

The changes dictated by the card associations and EFT Networks are required to remain in compliance with each of the networks. The dates for compliance have been set by each card association or network. Associations rarely offer waivers to mandates so you should pursue these changes with your vendor as quickly as possible.

Please contact Client Services at 800.782.9042, option 2, with any questions.

# Summary by Association/ Network

# Visa and MasterCard
# Account Status vs Account Check

There has been some confusion on the differences between MasterCard Account Status and Visa Account Verification vs Visa Status Check and MasterCard Account Check. We are re-publishing the attributes to help clarify.

In addition, it is important to note that the Status/Account Check has financial implications, therefore it is appropriate to respond with NSF should there be no funds in the account.

The Account Status/Verification has no financial impact and certain response codes do not pertain to this type of request. Neither Visa nor MasterCard expect an NSF response on these requests. **Responding with an NSF code to this request will impact your member's ability to provision their device if you participate in Apple Pay or other token services.**

MasterCard has also begun monitoring compliance of MasterCard Account Status Inquiry transactions to ensure the appropriate response. See MasterCard article below.

**MasterCard Account Status Inquiry** and **Visa Account Verification** have a zero dollar amount. These are the attributes:

- Verifies the account is open/valid
- Card has not been lost/stolen
- Request has no financial impact (place no holds on the account; no funds move)
- 0100 level message with a process code 00xx00
- Transaction amount is $0.00
- Messages may include Address Verification Service (AVS) and/or CVV2

**Visa Status Check** and **MasterCard Account Check** are typically one dollar and has financial impact. Here are the attributes.

- Verifies the account is valid; funds are available
- Acts as an authorization request with financial impact
- 0100 level message with a process code 00xx00
- Transaction amount is referred to as a single currency unit, typically $1.00
- Messages may include Address Verification Service (AVS)

## Visa

**Update to Enhanced Original Credit Transactions (OCT)**
*(Required for Credit, Debit)*

Visa will be adding a new field, Recipient Name, for Original Credit Transactions. Acquirers are required to include Recipient Name in all cross-border enhanced OCTs with a Business Application Identifier (BAI) value of **AA** (Account to Account) or **PP** (Person to Person). The Recipient Name will be sent in DE110-Receiver Data, under the N1 tag. Credit unions that want to begin receiving this information should submit a service request via the CO-OP Extranet and request that DE110 be enabled. DE110 does not have to be returned in the 0110/0210 response message.

It is important to note that when this data element is enabled, you may receive information in this data element from any network that passes information related to payment transfer transactions.

**Acquirer updates:**
Acquirers and originators that submit enhanced OCTs must be aware of the following changes:

- A new field, Sender Date of Birth must be included in the transaction request
- Visa will decline the 0200 financial request messages for cross-border enhanced OCTs that do not include the recipient's name
- Visa will decline domestic and cross-border 0200 financial request messages where the sender's country is on the list of U.S. Office of Foreign Assets Control (OFAC) comprehensively sanctioned countries.
- The value of the City Name in the Card Acceptor Name/Location will be changed to Visa Direct

**Issuer updates:**
Issuers that participate in enhanced OCTs must be aware of the following changes:

- DE109 may contain a new tag "DB" that will forward Sender Date of Birth in the transaction request
- Visa will decline the 0200 financial request messages for cross-border enhanced OCTs that do not include the recipient's name. Hosts that do not receive denied transactions today will not receive these denials.
- Visa will decline domestic and cross-border 0200 financial request messages where the sender's country is on the list of U.S. Office of Foreign Assets Control (OFAC) comprehensively sanctioned countries.
- The value of the City Name in the Card Acceptor Name/Location will be changed to Visa Direct

DE109 tag "DB" is an existing tag, now used by Visa.

## Visa Token Service

*(Optional for Debit, Interlink, PAVD and Credit)*

Token data is passed in DE124, using the Payment Token Data format. Visa is requiring that issuers support two new tags, Token Expiry Data (Tag 06) and Token Type (Tag 09). Token type, Tag 09, will be used to identify tokens generated from a card on file, a secure element or using host card emulation. This information will be available in DataNavigator. If you wish to receive this information in the online message, please open a work request via the CO-OP Extranet and request DE124 be enabled.

Important to note: Once DE124 is enabled you will receive DE124 Data from other networks. It will be up to your core system to determine what information is needed and extraneous data should be ignored.

See DE124, Payment Token Data format below.

## Changes to Acquirer ISA Fees

*(Required for Visa/Plus Acquirers)*

Visa will implement changes for Acquirer International Service Assessment (Acquirer ISA) charges to transactions where the merchant is in the U.S. region, and the issuer is in a different region. No

changes will be made to the values for transactions where the merchant is outside of the U.S. region, or to the values received by issuers.

These changes would apply when a credit union initiates an Account Funding Transaction (AFT) to debit the sender's account for the money transfer amount. Once funding for the money transfer is approved, the originator sends an OCT to the recipient issuer through VisaNet to credit the recipient's account.

Visa is eliminating the Charge Indicator values of "D" and "T" published in the Spring 2014 compliance document.

| Status | Value | Description |
|---|---|---|
| Eliminated | **D** | Single currency purchase including account funding Acquirer ISA assessed |
| Eliminated | **T** | Multicurrency purchase including account funding Acquirer ISA assessed |

Changes are:

- Add two new Charge Indicator values in DE111, VD format
- Add two charge types and charge amounts
- The two new charge types will be added to the VSS-140 reports

**Charge Indicator Values:**

| Status | Value | Description |
|---|---|---|
| Unchanged | C | Single currency cash Acquirer ISA assessed |
| Unchanged | S | Multicurrency cash Acquirer ISA assessed |
| New | B | Base purchase Acquirer ISA assessed |
| New | E | Enhanced purchase Acquirer ISA assessed |

**Charge Types:**

| Charge Indicator | Charge Type | Description |
|---|---|---|
| B | Base Rate | Purchase transaction or AFT where the transaction currency is the same as the merchant's local currency, and the merchant's currency is USD. |
| E | Enhanced Rate | Purchase transaction or AFT where the transaction currency is not the same as the merchant's local currency, and the merchant's currency is USD. |

# MasterCard

**New Funding/ Payment Indicator**

*(Required for Credit, Debit and Maestro)*

MasterCard has defined a new funding/payment identifier of "C67 Inter Platform Person-to-Person" in order to identify processing of new MasterCard payment and remittance services. This indicator value may only be used by institutions that have contractually agreed with MasterCard to provide a payment/remittance service where MasterCard will route all card-involved transactions. Specific processing rules will be applied to transactions identified by this indicator.

The new value, C67 indicator will be passed in DE111, MC and MD formats under Payment Type Indicator. The new value, C67 will be passed in DE111, MI format under Program Registration ID.

**MasterCard Embedded Security Service Platform Enhancements**
*(Optional for Credit, Debit and Maestro)*

MasterCard is expanding current fraud detection functionality by enhancing message formats to support future additional real-time monitoring services to combat fraud more effectively. This expansion will provide merchant acquirers, and issuers with additional tools to preempt fraud for contact and contactless transactions at the point-of-sale (POS) and card not present scenarios.

Issuers that participate in the MasterCard Expert Monitoring Fraud Scoring service must be prepared to support the addition of the new Security Services Additional Data services. This expanded information will provide security data indicators and identify security data services. There will be a variety of permitted values defined by MasterCard.

MasterCard expects processors and card issuers to support the receipt of up to sixteen occurrences of two 3 byte subfields (6 bytes per occurrence) for a total of 96 bytes. Each occurrence will contain a 3 byte Security Services Indicator subfield and a 3 byte Security Services Data subfield. With the Spring 2015 mandates, as an interim solution, we will pass the first 2 occurrences (12 bytes) of the data received from MasterCard (in whatever order received) in DE124. Passing the full 16 occurrences will take place in a future release.

A new tag of "FS" will be added to DE124 and a new MDS and CIS layout will be added. These layouts are under development and will be provided as they become available.

MasterCard's Embedded Security Service is an optional service. Credit unions interested in participating should contact MasterCard directly.

DE124 must be enabled at the switch before data is sent to issuers. If you wish to receive DE124 please open a work request via the CO-OP Extranet and request DE124 be enabled.

Important to note: Once DE124 is enabled you will receive DE124 Data from other networks. It will be up to your core system to determine what information is needed and extraneous data should be ignored.

**Multi-Clearing Enhancement**
*(Required for Debit and Credit Issuers)*

Today, there is no indicator in the completion message that would allow an acquirer to identify multiple presentments against a single approved authorization. MasterCard will be introducing a new multi-clearing indicator that can be used when a single authorized request will have multiple completions with partial amounts.

Acquirers are required to present all multi-clearing messages within seven calendar days of the original authorization request.

MasterCard has identified two multi-clearing identifiers:

- Previously approved authorization—partial amount, multi-clearing
- Previously approved authorization—partial amount, final clearing

MasterCard will send the same identifier for each partial clearing and will not indicate how many clearing items you can expect. A final clearing indicator may be received, but cannot be guaranteed. In the case where the fulfilment of the original authorization is handled by separate merchants, you may receive the 'Previously approved authorization—partial amount, multi-clearing' message from each merchant. No final clearing indicator is received because neither merchant knows if the fulfilment of the original authorization has been completed.

Because no final completion message is received, it will be important to track the dollar amount of each clearing against the original authorization amount. If a multi-clearing message is received and there is still an outstanding previously authorized amount, the outstanding balance may remain as a hold on the account for seven days.

The multi-clearing indicators will be passed in DE124, Multi-Clear Sequence Number (SN tag) and Multi-Clear Count Number (CN tag).

When MasterCard sends a 'Previously approved authorization—partial amount, multi-clearing' we will send the SN and CN tag:

**SN0201CN0202** - indicating 1 out of 2
**Note:** from an issuing perspective we do not know how many clearing records will be received.

When MasterCard sends a Previously approved authorization—partial amount, final-clearing, we will send the SN and CN tag:

**SN0202CN0202** - indicating it is the last item

## Service Provider and Merchant Identification Enhancements

*(Required for Debit, Credit and Maestro)*

MasterCard is implementing changes that will help identify the payment facilitator, sub-merchant, and/or independent sales organization that may be participating in a transaction. This will support the expansion of the payment facilitator model by enabling accurate acceptance location information, strengthening fraud monitoring and authorization screening, and providing clarity about the transaction to issuers and cardholders.

New MasterCard Merchant Data may include Payment Facilitator ID, Independent Sales Organization ID and Sub-Merchant ID and will be sent in DE111 - CIS, IPM and MDS formats. See DE111 layout below.

The Additional Merchant Data will be displayed in DataNavigator in the long format segment.

## New 2 Series MasterCard BIN Range

*(Information only)*

MasterCard is introducing a new series of bank identification numbers (BINs) that begin with "2". The 2 series BIN range is 222100–272099. The 2 series BINs will be processed in the same manner as the existing MasterCard BINs are today. Implementation of the 2 series BINs is effective October 14, 2016. This information is being provided to allow merchants, ATM

manufacturers, processors and core vendors sufficient lead time to review the impact and make the necessary changes required for processing.

### MasterCard Data Integrity Non-Compliance Warning

*(Required)*

It has come to our attention that credit unions have been identified as using non-compliant response codes when responding to a MasterCard Account Status Inquiry. An Account Status Inquiry is a 0100 level message, process code 00x00 with a $0.00 transaction amount.

The following response codes (DE039) may NOT be returned in an Account Status Inquiry:

12 - Invalid transaction
13 - Invalid Amount
30 - Format error
51 - Insufficient Funds/over credit limit
57 - Transaction not permitted to cardholder
58 - Transaction not permitted to terminal

## CO-OP

### CO-OP PIN POS Enhancements

*(Required for CO-OP PIN POS Issuers)*

CO-OP is enhancing its POS service to expand PIN-less authentication options for CO-OP PIN POS transactions to include signature and no cardholder verification method (CVM) transaction to allow participation to a broader base of eligible merchants. Support of these enhancements is required by June 1, 2015.

The eligible transactions include purchases, returns, pre-authorizations and pre-authorization completions. CO-OP PIN POS $50 or less eligible Merchant Category Codes (MCC), as well as select tip accepting merchant categories, will be eligible to participate in this enhancement. These transactions will be electronically initiated through magnetic stripe or full chip data and will not have a PIN Block (DE052)

These enhancements will utilize existing online messages and data elements. No new fields will be introduced. The Acquiring Network ID in DE63 will be “CPP” as is currently used for CO-OP PIN POS transactions.

Tip accepting merchants, MCC’s listed below, must utilize pre-authorization (0100) and pre-authorization completion (0220) message types when the final transaction amount is unknown at the time the transaction is initiated. Pre-authorization completions must be processed within two hours of the pre-authorization. CO-OP will allow a 20% tip variance between the pre-auth and completion. Issuers should take the tip variance into consideration when authorizing transactions and adjust authorization holds as appropriate.

| MCC | Eligible Tip Accepting Merchant Category |
|---|---|
| 5812 | Eating Places |
| 5813 | Drinking Places(Alcoholic Beverages) |
| 4121 | Taxi Cabs |
| 7230 | Barber Shops and Beauty Salons |
| 7298 | Health and Beauty Spas |

The following Merchant Category Codes are excluded from participation:

| Excluded MCCs | | | | |
|---|---|---|---|---|
| 4813 | 5964 | 6010 | 6531 | 9405 |
| 4829 | 5966 | 6011 | 6532 | 9700 |
| 5542 | 5967 | 6012 | 6533 | 9702 |
| 5960 | 5968 | 6050 | 6534 | 9754 |
| 5962 | 5969 | 6051 | 7995 | 9950 |

## CO-OP Tokenization Exchange Support

*(Applies to CO-OP PIN POS, STAR, NYCE and Pulse)*

CO-OP members that subscribe to a Token Service Provider (TSP) such as Visa or MasterCard to replace Primary Account Numbers (PANs) with tokens may elect to participate in other POS networks that work with your TSP to provide tokenized transactions. The POS network works with your TSP to exchange the token for the cardholder's actual PAN in order to complete the authorization of Token transactions.

To provide consistency and simplify core vendor code requirements, CO-OP will provide uniform token support for transactions routing through networks acting as a token exchange provider such as CO-OP, STAR, NYCE and Pulse.

Transactions forwarded to your host from a token exchange provider will have the following characteristics:

- DE002 will identify the actual PAN
- DE014 will contain the card expiration
- DE035 will not be present – iCVV/iCVC and dCVV/dCVC validation will not be performed
- DE124 TLV format (tag, length, variable length data) will house token data
- PIN validation optional **

Token transactions do not contain mag stripe data which presents a challenge for cards that have the PIN offset encoded on the stripe. If a PIN offset file is maintained on the switch, PIN validation will be performed on token transactions.

** CO-OP offers the option of turning off PIN validation for token transactions received from token exchange providers, eliminating the need to have a PIN offset file maintained at the switch.

# STAR

## STAR Token Exchange Service

*(Optional for STAR Issuers)*

Please see the CO-OP Tokenization Support article referenced above. **Note:** DE124, Tag T5 will be updated to with the value of "ST" for STAR Token Exchange transactions.

## STAR Access Phase I

*(Required for STAR Issuers)*

STAR Network is launching a new service, STAR Access, using a phased approached. STAR Access Phase I will expand PIN-less authentication options to include signature and no cardholder verification method (CVM) transactions and will offer STAR Network participation to a broader base of eligible merchants. Issuer support of STAR Access Phase I is required by June 1, 2015.

The eligible transactions for STAR Access Phase I include purchases, returns, pre-authorizations and pre-authorization completions. STAR RapidFlash eligible Merchant Category Codes (MCC), as well as select tip accepting merchant categories, will be eligible to participate in STAR Access. Transactions processed as STAR Access must be electronically initiated through magnetic stripe or full chip data and will not have a PIN Block (DE052)

STAR Access Phase I will utilize existing online messages and data elements. No new fields will be introduced for STAR Access Phase I. STAR Access transactions will have a new Acquiring Network ID in DE63 of "AXS".

Tip accepting merchants, MCC's listed below, must utilize pre-authorization (0100) and pre-authorization completion (0220) message types when the final transaction amount is unknown at the time the transaction is initiated. Pre-authorization completions must be processed within two hours of the pre-authorization. STAR will allow a 20% tip variance between the pre-auth and completion. Issuers should take the tip variance into consideration when authorizing transactions and adjust authorization holds as appropriate.

| MCC | Eligible Tip Accepting Merchant Category |
|---|---|
| 5812 | Eating Places |
| 5813 | Drinking Places(Alcoholic Beverages) |
| 4121 | Taxi Cabs |
| 7230 | Barber Shops and Beauty Salons |
| 7298 | Health and Beauty Spas |

The following Merchant Category Codes are excluded from participation in STAR Access Phase I:

| Excluded MCCs | | | | |
|---|---|---|---|---|
| 4813 | 5964 | 6010 | 6531 | 9405 |
| 4829 | 5966 | 6011 | 6532 | 9700 |
| 5542 | 5967 | 6012 | 6533 | 9702 |
| 5960 | 5968 | 6050 | 6534 | 9754 |
| 5962 | 5969 | 6051 | 7995 | 9950 |

## STAR Remote Transaction Enhancements

*(Required for STAR Issuers)*

STAR Network will be enhancing the authentication and security for remote (aka card not present) transactions. These transaction types include Internet, VRU and Call Center transactions. With these enhancements, those merchants will have the option of sending Address Verification Service (AVS) data, Card Verification Information 2 (CVI-2) and Card Expiration Date in an authorization request. Credit Union host must be able to accept AVS and CVI data in DE123 and expiration date in DE14 for STAR transactions. Depending on your configuration either CO-OP Network or your host performs AVS validation. In most cases, hosts do their own AVS validation and CO-OP only performs AVS in stand-in. If your host is doing AVS validation, you will need to ensure it is done for STAR transactions when AVS data is sent in DE123.

If you participate in STAR Network and CO-OP Financial Services processes your signature debit transactions and we received your CVV/CVC keys for the purposes of performing validation, CO-OP will perform the CVI-2 validation for STAR Remote transaction activity on your behalf.

Since CVI-2 validation is required and transactions can be denied if validation is not performed, we are asking STAR to exclude BINs for which we do not currently have CVV/CVC keys until we can work with credit unions to get the keys added and certified. Also, since ATM BINs generally do not have CVV/CVC keys set up, we are continuing discussions with STAR on how they will handle these transactions.

STAR Network participants who use a signature Debit processor other than CO-OP and have not set up CVV/CVC keys at CO-OP may open a work request via the CO-OP Extranet requesting the addition of CVV/CVC keys. Credit unions will need to provide their CVV/CVC keys. Database and certification fees will apply. There is no charge per transaction fee for performing CVV/CVC validation.

# PULSE

## PULSE PAY Express Enhancements Reminder

*(Required for Pulse Participants)*

PULSE is enhancing their PULSE PAY Express (PPE) program to allow additional transactions, remove $50 limit and remove Merchant Category Code restrictions, allowing signature transaction processing and Card Validation Method (CVM) requirements. In an effort to allow time for issuers to prepare for the changes, PULSE is allowing issuers to implement the enhancements in phases. The Initial PPE Participation and Full PPE Participation characteristics are detailed below.

**Initial PPE** Participation

The following components apply to the Initial PPE level of participation:

- Transaction amounts less than or equal to $50 USD
- Gratuity-eligible
- Limited transaction set
- Limited to the following Merchant Categories: General Retail, Grocery, Petroleum (in-store only) and Restaurant

**Full PPE** Participation

The following components apply to the Full PPE level of participation:

- Unlimited transaction amount
- Gratuity-eligible
- Full transaction set
- All transaction categories (MCCs)

Initial PPE Participation, which was required by October 15, 2014. Full PPE Participation is required April 15, 2015.

PULSE is requiring that CVV/CVC for card present transactions and CVV2/CVC2 for card not present transactions be validated when presented as part of the transaction request by April 15, 2015.

If you participate in PULSE and CO-OP Financial Services processes your signature debit transactions and we received your CVV/CVC keys for the purposes of performing validation, CO-OP will perform the CVV validation for PULSE PAY Express activity on your behalf.

If however, you did not have your keys available and Visa is performing the CVV validation on your behalf or if you use a signature Debit processor other than CO-OP and have not already supplied CO-OP with your CVV/CVC keys for validation on pinned transactions, you may open a work request via the CO-OP Extranet requesting the addition of CVV/CVC and CVV2/CVC2 validation on PULSE transactions. Credit unions will need to provide their CVV/CVC keys and certification will be required. Database and certification fees will apply. There is no charge per transaction fee for performing CVV/CVC validation.

Depending on your configuration either CO-OP Network or your host performs AVS validation. In most cases, hosts do their own AVS validation and CO-OP only performs AVS in stand-in. If your host is doing AVS validation, you will need to ensure it is done for PULSE PAY Express transactions when AVS data is sent in DE123.

**General Considerations - All PPE Participation Levels**

- **Card/ Cardholder Verification Method (CVM)** – PPE transactions are always PINless. Additional Card/Cardholder Verification Methods may be required depending on the transaction origination.
- **Transactions < $50** – No CVM required for card-present transactions < $50.
- **Transactions > $50** – Signature, Zip, CVV2 and/or AVS may be required. Issuers and/or their issuer processor are responsible for performing AVS validation; PULSE will not provide AVS validation services on behalf of the issuer. CVV2 validation may be performed by the issuer and/or their issuer processor.

- **Cash Back** – is not allowed on PULSE PAY Express transactions. In the event a purchase with cash back occurs, the issuer may reply with a partial approval for the merchandise amount only, following standard partial approval processing.
- **Surcharge** – PPE transactions are surcharge-eligible and will follow standard surcharge processing rules.
- **Stand-in Processing** – PULSE PAY Express transactions are never approved based on floor limits; however, PULSE may stand in for an issuer processor based on pre-defined stand-in limits in the event that the issuer processor is unavailable to respond. Because a PIN is not present, there will be no PIN validation when PULSE performs stand-in on these transactions. PPE transactions approved in stand-in will use the existing POS stand-in limit.
- **Partial Approvals** – are allowed on PULSE PAY Express transactions; however, merchants should not add gratuity to the partially approved amount.
- **Card Not Present (CNP)** and **Key-Entered Transactions** – are allowed on PULSE PAY Express transactions, following standard processing rules.
- **Address Verification Service (AVS)** – AVS data is sent to PULSE PAY Express issuers with AVS data unverified. The card-issuing financial institution must perform its own address verification by interrogating the AVS data provided by the acquirer. The results of the address verification must be returned by the issuer of the pre-authorization response. PULSE does not perform AVS validation.
- **Recurring Payments** – Recurring payment transactions will have a pre-authorization prior to the first settlement to the account, but may not have subsequent pre-authorizations. The subsequent settlement items may not contain the original authorization response.
- **E-Commerce Delayed Shipments** – PULSE PAY Express transactions originating from an e-commerce merchant are eligible for delayed shipment processing. Delayed shipment processing occurs when a cardholder purchases items that are not ready for shipment at the time of purchase. The items can be in stock and need to be prepared for shipment, or are found to be out of stock by the e-commerce merchant after the purchase is made. E-commerce merchants have the ability to avoid charging a cardholder for a purchase until the purchased items are ready for shipment. Ecommerce merchants may create multiple 0220 settlement advices for each shipment that occurs from a single 0100 pre-authorization request. All related advice messages contain a multi-clear count indicator within DE124.
- **Gratuity** – Merchants are limited to sending gratuity for no more than 20% of the original fully authorized amount on transactions originating from specified MCCs. The merchant may be liable for amounts exceeding this threshold. Issuers are encouraged to increase their hold amounts in consideration for this allowance. Gratuity may not be added to a transaction approved for a partial amount.
- **CVV/ CVC Validation** – CVV/CVC data may be present on some transactions. CVV/CVC can be validated for card-present transactions when supplied by the acquirer.
- **CVV2/ CVC2/ CID Validation** – CVV2/CVC2/CID data may be present on some transactions. The CVV2/CVC2/CID value is manually entered at the time of the transaction. This code can be validated for card-not-present transactions when supplied by the acquirer.

- **Automated Fuel Dispense (AFD)** – applies only to Full PULSE PAY Express participants. PPE transactions originating from an AFD merchant (MCC=5542) have the following processing rules:
  - **Transaction Amount** – The approval of a $1 pre-authorization on a transaction originating from an AFD merchant will hold the issuer responsible for a fuel purchase of up to $100.00. Issuers may approve the $1 pre-auth in full and be liable for the full $100.00, or may respond to the request with a partial approval in an appropriate amount.
  - **Real-Time Authorization for Automated Fuel Dispense** – AFD merchants have the option of sending a 0120 Authorization Advice within 1 hour of the original authorization request as a means of notifying the issuer of the amount of fuel actually dispensed so that the issuer can adjust the hold amount against the cardholder's account. When present, the 0120 Authorization Advice will be sent within 1 hour of the original request, and the final 0220 Settlement Advice will arrive in the standard signature timeframe at a later date. All PPE issuers must be capable of processing PPE AFD transactions with and without a 0120 Authorization Advice Message.

### Important NOTE:

If an institution cannot support the Full PULSE PAY Participation level, you must contact your PULSE representative and ask them to reset your participation level to Initial participation.

For those credit unions where CO-OP does not have your CVV/CVV2 keys, we have submitted the request to lower your BIN participation however; we recommend you still contact PULSE directly. Also, since ATM BINs generally do not have CVV/CVC keys set-up, if you have an ATM BIN you MUST contact your PULSE representative to discuss the best course of action for that BIN.

## PULSE PAY Express Transaction Set

| Process Code | Message Class | Tran Type | Settlement Mnemonic | Description | Initial | Full |
|---|---|---|---|---|---|---|
| 000000 | 010x / 0110 012x (stand-in)<br><br>042x | 85 | FPA | Purchase Pre-Authorization from Funding | ISS: M<br><br>ACQ: O | ISS: M<br><br>ACQ: O |
| 000000 | 012x | 85 | FPA | Purchase Pre-Authorization from Funding Authorization Advice<br><br>(Acquirer-generated) | ISS: M<br><br>ACQ: O | ISS: M<br><br>ACQ: O |
| 000000 | 022x | 95 | FFA | Pre-Authorized purchase from Funding | ISS: M<br><br>ACQ: O | ISS: M<br><br>ACQ: O |

| | | | | | | |
|---|---|---|---|---|---|---|
| 000000 | 020x / 0210<br>022x (stand-in)<br><br>042x | 79 | FP | Purchase from Funding | ISS: M<br><br>ACQ: O | ISS: M<br><br>ACQ: O |
| 200000 | 020x/022x<br>042x | 80 | FMR | Merchandise Return to Funding | ISS: M<br>ACQ: O | ISS: M<br>ACQ: O |
| 180000 | 0100 / 0110 | 10 | PAU | AVS Authorization Only | ISS: M<br>ACQ: O | ISS: M<br>ACQ: O |
| 500000 | 020x / 0210<br>042x | 74 | PFT | E-Commerce Payment | ISS: M<br>ACQ: O | ISS: M<br>ACQ: O |
| 550000 | 020x / 0210<br>042x | PF | FPT | E-Commerce Return/Credit | ISS: M<br>ACQ: O | ISS: M<br>ACQ: O |

**PULSE Token Exchange Service**
*(Required for PULSE Issuers)*

Please see the CO-OP Tokenization Support article referenced above. **Note:** DE124, Tag T5 will be updated to with the value of "PU" for PULSE token transactions.

## NYCE

**NYCE Tokenization Support**
*(Optional for NYCE Issuers)*

Please see the CO-OP Tokenization Support article referenced above. **Note:** DE124, Tag T5 will be updated with the value of "NY" for NYCE token transactions.

# ISO 8583 Data Elements

## 111 ADDITIONAL DATA, PRIVATE ACQUIRER (FIS-DEFINED)

**Format:** LLLVAR

**Attributes:** FIS: ans..255
ISO: ans..999

**Description:** This data element is reserved by ISO for private definition and use. FISdefines this data element as *Additional Data, Private Acquirer*, which contains additional information for Visa® DCS, Visa EVES, Visa DCS CRIS[SM], Benefits Transfer, MasterCard® CIS, MasterCard IPM and PLUS® format. The layouts for this data follow.

**Status**

**MasterCard® CIS Format**

| Subelement Name/ Contents | Data Length | MasterCard Bit No. | FINIPC Bit No. |
|---|---|---|---|
| Data Identifier. Value: **MC** | 2 | NA | NA |
| Data Length plus the variable data. | 3 | NA | NA |
| Data Byte Map. See FINIPC Bit Number. | 8 | NA | NA |
| Variable Data: (based on byte map) | | | |
| Merchant Advice Code | 2 | 48.84 | 1 |
| Fraud Data. This data contains the following three subfields for a total length of 9: | | | 2 |
| • POS Entry Mode | 3 | 22 | |
| • Response Code | 2 | 39 | |

| | | | |
|---|---|---|---|
| • POS Data - POS Terminal Attendance<br>• POS Data - POS Cardholder Presence<br>• POS Data - Card-Activated Terminal Level<br>• POS Data - POS Card Data Terminal Input Capability | 1<br>1<br>1<br>1 | 61.1<br>61.4<br>61.10<br>61.11 | |
| Advice Detail Code | 4 | 60.2 | 3 |
| Magnetic Stripe Compliance Status Indicator | 1 | 48.88 | 4 |
| Magnetic Stripe Compliance Error Indicator | 1 | 48.89 | 5 |
| Postal Code | 10 | 61.14 | 6 |
| POS Card Presence<br>0 = Present<br>1 = Not Present | 1 | 61.5 | 7 |
| Payment Type Indicator | 3 | 48.77 | 8 |
| MC Assigned ID | 6 | 48.32 | 9 |
| MC Fraud On-Behalf Result | 1 | 48.71.2 | 10 |
| MC Fraud Score Information | 3 | 48.75.1 | 11 |
| MC Healthcare IIAS Exemption | 1 | 48.61.3 | 12 |
| Processor Pseudo ICA | 7 | 48.16 | 13 |
| Authorization System Advice Date and Time | 10 | 48.15 | 14 |
| Account Data Compromise Event Messaging Service Data Result | 1 | 48.71.2 | 15 |
| Account Data Compromise Event Messaging Service Data | 30 | 48.39 | 16 |
| Partial Approval Terminal Support Indicator | 1 | 48.61.1 | 17 |
| MC Fraud Score Reason Code | 2 | 48.75.2 | 18 |
| POS Transaction Status Indicator | 1 | 61.7 | 19 |
| Remote Payments Program Type Identifier | 1 | 48.48.1 | 20 |

| | | | |
|---|---|---|---|
| Payment Initiation Channel Device Type | 2 | 48.23.1 | 21 |
| UCAF Collection Indicator | 1 | 48.42.1.3 | 22 |
| Transit Transaction Type Indicator | 2 | 48.64.1 | 23 |
| Transportation Mode Indicator | 2 | 48.64.2 | 24 |
| PPOL Identifier | 3 | 48.26.1 | 25 |
| Final Auth Indicator | 1 | 48.61.5 | 26 |
| Terminal Compliant Indicator | 2 | 48.65 | 27 |
| MC On-behalf Service | 2 | 48.71.1 | 28 |
| MC On-behalf Result 1 | 1 | 48.71.2 | 29 |
| Merchant Fraud Score | 4 | 112.28 | 30 |
| Payment Facilitator ID | 11 | 48.37.1 | 31 |
| Secondary Bit Map | 8 | N/A | 32 |
| Sales Organization ID | 11 | 48.37.2 | 33 |
| Sub Merchant ID | 15 | 48.37.3 | 34 |

**MasterCard® MDS Format**

| Subelement Name/ Contents | Data Length | MasterCard Bit No. | FINIPC Bit No. |
|---|---|---|---|
| Data Identifier. Value: **MD** | 2 | NA | NA |
| Data Length (byte map + variable data) | 3 | NA | NA |
| Data Byte Map (See FINIPC Bit No.) | 8 | NA | NA |
| Variable Data (Based on Byte Map) | | | |

| | | | |
|---|---|---|---|
| Tier Merchant ID | 6 | DE110.1 | 1 |
| Cross Border Indicator | 2 | | 2 |
| Transaction Indicator-Position 1 | | DE126, position 14 | |
| Y = Qualifies as a cross-border transaction | | | |
| N = Does not qualify as a cross-border transaction | | | |
| Currency Indicator-Position 2 | | DE126, position 15 | |
| X = Transaction does not qualify as a cross-border transaction. | | | |
| Y = Transaction was submitted in the currency of the country where the merchant is located. | | | |
| N = Transaction was not submitted in the currency of the country where the merchant is located. | | | |
| ISA Flag<br>0 = No International Fee<br>1 = International Fee Debited<br>2 = International Fee Credited | 1 | DE 110.4 | 3 |
| Financial Network Code | 2 | DE63, subfield 1 | 4 |
| Card Present | 1 | DE61, position 5 | 5 |
| Operating Environment | 1 | DE61, position 3 | 6 |
| POS Terminal Attendance Indicator | 1 | DE61, position 1 | 7 |
| POS Cardholder Presence Indicator | 1 | DE61, position 4 | 8 |
| Cardholder Activated Terminal Level Indicator | 1 | DE61, position 10 | 9 |
| POS Card Data Terminal Input Capability Indicator | 1 | DE61, position 11 | 10 |
| POS Entry Mode | 2 | DE22 | 11 |

| | | | |
|---|---|---|---|
| Payment Type Indicator | 3 | 48.77 | 12 |
| MC Assigned ID | 6 | 48.32 | 13 |
| MC Healthcare IIAS Exemption | 1 | 48.61.3 | 14 |
| POS Transaction Status | 1 | 61.7 | 15 |
| Remote Payments Program Type Identifier | 1 | 48.48.1 | 16 |
| Payment Initiation Channel Device Type | 2 | 48.23.1 | 17 |
| Transit Transaction Type Indicator | 2 | 48.64.1 | 18 |
| Transportation Mode Indicator | 2 | 48.64.2 | 19 |
| Maestro Pin-less Program Indicator | 1 | 48.81 | 20 |
| Acquiring Institution Id | 11 | 32 | 21 |
| Card Acceptor ID | 15 | 42 | 22 |
| PPOL Data | 3 | 48.26 | 23 |
| Terminal Compliant Indicator | 2 | 48.65 | 24 |
| MC On-behalf Service | 2 | 48.71.1 | 25 |
| MC On-behalf Result 1 | 1 | 48.71.2 | 26 |
| AllPoint Surcharge-Free Alliance Indicator | 1 | 43.2 | 27 |
| Merchant Fraud Score | 4 | 112.28 | 28 |
| Payment Facilitator ID | 11 | 48.37.1 | 29 |
| Sales Organization ID | 11 | 48.37.2 | 30 |
| Sub Merchant ID | 15 | 48.37.3 | 31 |

## MasterCard® IPM Format

| NOTE | This format does not apply to the MasterCard 0100 authorization messages. |
|---|---|

| Subelement Name/ Contents | Data Length | MasterCard Bit No. |
|---|---|---|
| Data Identifier. Value: **MI**. | 2 | NA |
| Data Length plus the variable data. | 3 | NA |
| Processing Code | 6 | IPM DE 3 |
| POS Condition Code. This data contains the following 12 subfields for a total length of 12. | | IPM DE 22 |
| • Card Data Input Capability | 1 | IPM DE 22-S1 |
| • Cardholder Authentication Capability | 1 | IPM DE 22-S2 |
| • Card Capture Capability | 1 | IPM DE 22-S3 |
| • Terminal Operating Environment | 1 | IPM DE 22-S4 |
| • Cardholder Present Data | 1 | IPM DE 22-S5 |
| • Card Present Data | 1 | IPM DE 22-S6 |
| • Card Data Input Mode | 1 | IPM DE 22-S7 |
| • Cardholder Authentication Method | 1 | IPM DE 22-S8 |
| • Cardholder Authentication Entity | 1 | IPM DE 22-S9 |
| • Card Data Output Capability | 1 | IPM DE 22-S10 |

| | | |
|---|---|---|
| • Terminal Data Output Capability | 1 | IPM DE 22-S11 |
| • PIN Capture Capability | 1 | IPM DE 22-S12 |
| Card Acceptor Inquiry Information. This data contains the following three subfields for a total length of 57: | | IPM PDS 0170 |
| • Customer Service Phone Number | 16 | IPM PDS 0170-S1 |
| • Card Acceptor Phone Number | 16 | IPM PDS 0170-S2 |
| • Additional Contact Information | 25 | IPM PDS 0170-S3 |
| Card Acceptor Postal Code | 10 | IPM DE 43-S4 |
| Local Date and Time | 12 | IPM DE 12 |
| Airline/Railway Ticket Number | 15 | IPM PDS 0506 |
| Program Registration ID | 3 | IPM PDS 0043 |
| Interchange Life Cycle | 15 | IPM PDS 0263 |
| Cross Border Transaction Indicator | 1 | IPM PDS 0177-S1 |
| • Y = Qualifies as a cross-border transaction | | |
| • N = Does not qualify as a cross-border transaction | | |
| Cross Border Currency Indicator | 1 | IPM PDS 0177-S2 |
| • Blank = Transaction does not qualify as a cross-border transaction. | | |
| • Y = Transaction was submitted in the currency of the country where the merchant or ATM is located. | | |

| | | |
|---|---|---|
| • N = Transaction was not submitted in the currency of the country where the merchant or ATM is located. | | |
| MasterCard Assigned ID | 6 | IPM PDS 0176 |
| Payment Transaction Initiator | 3 | IPM PDS 0192 |
| CVC 2 Validation Program Indicator | 1 | IPM PDS 0044 subfield 1 |
| QPS/PayPass Chargeback Eligibility Indicator | 1 | IPM PDS 0044 subfield 2 |
| Remote Payments Program Type Identifier | 1 | IPM PDS 0194 |
| Payment Initiation Channel Device Type | 2 | IPM PDS 0198 |
| Transit Transaction Type Indicator | 2 | IPM PDS 0210, subfield 1 |
| Transportation Mode Indicator | 2 | IPM PDS 0210, subfield 2 |
| PPOL Identifier | 3 | IPM PDS 0207 |
| Terminal Compliant Indicator | 2 | IPM PDS 0211 |
| Payment Facilitator ID | 11 | PDS208 |
| Sub Merchant ID | 15 | PDS208 |
| Sales Organization ID | 11 | PDS209 |

# 124 FIS Tags, Acquirer / Info, Text (FIS-Defined)

| | |
|---|---|
| **Format:** | LLLVAR |
| **Attributes:** | FIS: ans..255<br>ISO: ans..999 |
| **Description:** | FIS defines this data element for use in financial messages to provide additional capability for exchanging data between acquirer hosts. Data passed in these data elements must be tokenized, assuming a TLV format (tag, length, variable length data), for financial messages.<br>FIS defines this data element as *Info, Text*, additional information used for AP file update information in AP file update transactions. It is also used for administrative and network management transactions. (See "0600/0620 Administrative Message Information" on page 494.") |

### Layout for Financial Messages

DE124 (FIS Tags, Acquirer) is activated to provide acquirers the ability to pass additional information to issuer hosts on financial requests or reversals.

In order to optimize this ISO field for general purpose, this data element consists of tokenized data that conforms to the TLV format (tag-length-variable data). This is enforced via edit-checking upon receipt of this data element.

DE124 supports multiple tokens and corresponding data for up to a maximum of 255 bytes each.

The data received in DE 124 is preceded by a 3-byte length indicator - indicating the overall length of the field. The sub-elements contained in either ISO data element must conform to the following format:

**xxyyzzzz**

where:

| | |
|---|---|
| xx | Is a 2-byte arbitrary alpha-numeric tag ID. |
| yy | Is 2-bytes containing the length of data to follow. Values range from 00 to a maximum of 99. |
| zzzz | Is the data for length defined in yy. |

Following is an example for DE124 (FIS Tags, Acquirer):

**Example**

```
023T105xxxxxT210yyyyyyyyyy
```

In this example, the length of the field is "023". The Tag ID is identified as "T1" has a data length of "05" where the data contains "xxxxx". Tag ID "T2" has a data length of "10" where the data contains 10 bytes with a value of "yyyyyyyyyy".

### FIS Reserve Tag Identifiers

The following table identifies the current status of FIS, and customer, reserve tags for use in DE 124:

| Tag ID | Purpose |
|---|---|
| AA-AB | Reserve for FIS use. |
| AC | Account Compromise Data. |
| AD-F0 | Reserve for FIS use. |
| CN | Multi-Clear Counter |
| F1 | Falcon Credit Data - Part 1 (reserved for DE 125 only). |
| F2 | Falcon Credit Data - Part 2 (reserved for DE 125 only). |
| F3-FC | Reserve for FIS use. |
| FD | Fraud Data. |
| FE-NH | Reserve for FIS use. |
| IT | Interchange Tier. |
| MI | Installment Payment Information |
| ND | Network Data. |
| NI | Network Interchange Data. |
| NJ-ZZ | Reserve for FIS use. |

| | |
|---|---|
| PD | Program ID. |
| PI | PIN Indicator. |
| SN | Multi-Clear Sequence Number |
| WL | Watch List. |
| T1-T6 | Payment Token Tags. |
| 00-9Z | Reserve for customer use. |

Refer to Appendix A "Data Elements Additional Information - DE124" and "Fraud/Score Data - DE124" for more information.

## Network Data Information

The Network Data tag is used to pass general Regional Network Information to ISO issuers.

**ACCEL**

| |
|---|
| NDLLACLLxx |

where:

| | |
|---|---|
| ND | Is the 2 byte literal identifying Network Data. |
| LL | Is the length of the data that follows. |
| AC | Is the sub-tag for ACCEL network. |
| LL | Is the length of the data in the AC sub-tag. |
| xx | Is the BAI data from ACCEL. |

Example:

ND06AC02PP

| Tag | Description |
|---|---|
| ND | Is the 2 byte Tag ID |

| | |
|---|---|
| 06 | Is the 2 byte Tag data length |
| AC | Is the 2 byte sub tag for ACCEL network |
| 02 | Is the 2 byte containing length of the data to follow |
| PP | Is the BAI data from ACCEL |

## PULSE

| |
|---|
| NDxxPSwwTR<zz><xxxxxxxxxxxxxxxx> FC<zz><xxx>NR<zz><xxxxxxxxxxxxxx> |

where:

| | |
|---|---|
| ND | Is the 2 byte Tag ID.z |
| xx | Is the 2 byte Tag data Length. |
| PS | Is the 2 byte subtag for Network Data. |
| ww | Is the 2 bytes containing length of the data to follow. |
| TR | Is the 2 byte Tag ID. |
| <zz> | Is the 2 byte tag length. |
| <xxxxxxxxxxxxxxxx> | Is the TR tag data for zz length (Transaction ID) |
| FC | Is the 2 byte Tag ID for Function Code |
| <zz> | Is the 2 byte Tag Length |
| <xxx> | Is the FC Tag Data fo zz length |
| NR | Is the 2 byte Tag ID Network Reference ID. |
| <zz> | Is the 2 byte tag length. |
| <xxxxxxxxxxxxxxxx> | Is the NR tag data for zz length |

**Example:**
NDnnPSnnTRnnzzzzzzzzzzzzzzzzFCzzxxNRzzxxxxxxxxxxxxxxx

| Tag | Description |
|---|---|
| ND | Is the 2 byte Tag ID |
| nn | Is the 2 byte Tag data Length |
| PS | Is the 2 byte subtag for Network Data |
| nn | Is the 2 bytes containing length of the data to follow |
| TR | Is the 2 byte Tag ID |
| nn | Is the 2 byte tag length |
| zzzzzzzzzzzzzzzz | Is the TR tag data for zz length (Transaction ID) |
| FC | Is the 2 byte Tag ID for Function Code |
| zz | Is the 2 byte Tag Length |
| xxx | Is the FC Tag Data for zz length |
| NR | Is the 2 byte Tag ID for Network Reference ID |
| zz | Is the 2 byte Tag Length |
| xxxxxxxxxxxxxx | Is the NR Tag Data for zz length |

### Multi-Clear Sequence Number

Multi-Clear Sequence Number is a number assigned by merchant to identify the advice message out of the total expected advice messages.

| Tag | Description |
|---|---|
| SN | Multi-Clear Sequence |

The internal logging of Multi-Clear Sequence Number will conform to the following format:

| |
|---|
| SNLLXX |

where:

| | |
|---|---|
| SN | Is the 2 byte literal identifying Multi-Clear Sequence Number. |
| LL | Is the length of the data that follows. |
| XX | Is the Multi-Clear Sequence Number. |

### Multi-Clear Count Number

Multi-Clear Count Number is a number assigned by merchant indicating the total number of advices that are expected as part of the cardholder's single purchase.

| Tag | Description |
|---|---|
| CN | Multi-Clear Count Number |

The internal logging of Multi-Clear Count Number will conform to the following format:

| |
|---|
| CNLLXX |

where:

| | |
|---|---|
| CN | Is the 2 byte literal identifying Multi-Clear Count Number. |
| LL | Is the length of the data that follows. |
| XX | Is the Multi-Clear Count Number. |

### *Payment Token Data*

The Payment Token is of the following format:

| |
|---|
| T1LLzzzT2LLyyyT3LLxxxT4LLwwwT5LLvvvT6LLuuuT8LLtttT9LLsssTALLrrrTBLLqqqTPLLppp |

where:

| Tag | Description |
|---|---|
| T1 | Is the 2 byte literal identifying Token for original PAN |
| LL | Is the length of Token for Original PAN |

| | |
|---|---|
| xxx | Is the Token for Original PAN |
| T2 | Is the 2 byte literal identifying Token Assurance Level |
| LL | Is the length of Token Assurance Level |
| yyy | Is the Token Assurance Level |
| T3 | Is the 2 byte literal identifying Token Requestor ID |
| LL | Is the length of Token Requestor ID |
| zzz | Is the Token Requestor ID |
| T4 | Is the 2 byte literal identifying PAN Range (First 9 digits of the cardholder PAN) |
| LL | Is the length of PAN Range i.e. 09 |
| www | Is the PAN Range |
| T5 | Is the 2 byte literal identifying Account Number Indicator. |
| LL | Is the length of Account Number |
| vvv | Is the Account Number |
| T6 | Is the 2 byte literal identifying Device Expiration Date |
| LL | Is the length of Device Expiration Date |
| uuu | Is the Device Expiration Date |
| T8 | Is the 2 byte literal identifying Token Reference Number |
| LL | Is the length of Token Reference Number |
| ttt | Is the Token Reference Number. Token Reference Number contains the value used as a substitute for the Payment Token that does not expose information about the Payment Token or the PAN that the Payment Token replaces |

| | |
|---|---|
| T9 | Is the 2 byte literal identifying Token Type |
| LL | Is the length of Token Type |
| sss | Is the Token Type. Token Type contains how the token transaction was initiated.<br>Currently defined values for Token Type are:<br>• CF = Card on File<br>• SE = Secure Element<br>• HC = HCE (Host Card Emulation |
| TA | Is the 2 byte literal identifying Token Status |
| LL | Is the length of Token Status |
| rrr | Is the Token Status. Token status contains the current status of the token.<br>Currently defined values for Token Status are:<br>• A = Active for Payment<br>• I = Inactive for Payment (Not yet activated)<br>• S = Temporarily suspended for payments<br>• D = Permanently deactivated for payments |
| TB | Is the 2 byte literal identifying Token Lookup Tran ID |
| LL | Is the length of Token Lookup ID |
| qqq | Is the Token Lookup Tran ID. Token Lookup Tran ID contains a TSP-provided reference from the original de-tokenization process. |
| TP | Is the 2 byte literal identifying Token Service Provider (TSP) Identifier |
| LL | Is the length of Token Lookup Service Provider Identifier |
| ppp | Is the Token Service Provider Identifier. This field contains information on which network entity is the TSP. Currently defined values for TSP Identifier are:<br>• MC = MasterCard<br>• VI = Visa<br>• ST = STAR<br>• FD = FDC<br>• IS = Issuer<br>• AQ = Acquirer |