Pinless Transaction Clarifications

April, 2017

First Data®

Agenda

- Definition Level Set
- Application Selection Overview and Scenario Explanation
- EMV No CVM
- PIN Bypass
- Debit Expansion Programs
  - PINless POS Product
  - Signature Debit Product
- PAVD – PIN Authenticated Visa Debit
- Specification Information

First Data

Definitions

- **Dual Message** – Two messages used to complete a transaction. Message one is the authorization request. If approved, a second message is created and sent via offline batch process to ultimately charge the consumer.
- **Single Message** – One message for authorization and settlement.
- **Traditional PIN Debit Networks** – STAR, NYCE, Pulse, etc.
- **Global Network –** Visa, MasterCard, Discover, Amex
- **Pinless Debit** – A single message transaction sent to a traditional PIN debit network that does not include a PIN.
- **CVM** – Cardholder Verification Method

First Data.

Application Selection Overview

- All EMV debit cards issued in the United States contain two or more Application Identifiers (AIDs):
  - A “Global AID” that *only* allows the transaction to be processed over the Global Network that appears on the front of the card (e.g.Visa or Mastercard,); and
  - A “Common AID” that allows the transaction to be processed over *any* of the networks for which the card is enabled – *including* Visa or Mastercard and all of the other networks on the card. Note that these other networks frequently offer better terms to merchants than the Global Networks.
- During the course of each EMV transaction, the terminal must select – based on its programming – which of these two AIDs will be used for the transaction.
- It is strongly recommended that terminals be programmed to always select the Common AID when it’s available, as only the Common AID allows the merchant or its acquirer to route the transaction to any of the networks available on the debit card.
  - If the Global AID is selected by the terminal automatically or with cardholder input, the transaction can only be routed to the single Global Brand that appears on the front of the card. The merchant loses the ability to route to any other network.
  - In contrast, if the Common AID is selected, the merchant – or the merchant’s acquirer on its behalf – can choose the network it desires. It can choose the Global Brand if it desires. Or it can choose another network that is less expensive.

First Data.

Application Selection Overview

- It is critical to understand that selection of the Global AID takes away the ability of the merchant or the acquirer to route the transaction. It simply limits the merchant's available network options. The Common AID, on the other hand, does not limit the merchant's options.
- Any terminal manufacturer, ISV/VAR, Gateway, or Middleware provider that is programming terminals to select the Global AID over the Common AID is blocking their customer – the merchant – from being able to determine how to route the debit transaction.
- Despite this, we are seeing three types of AID selection configurations in the field that are routing some or all of the merchant's transactions to the Global AID.
- In order to ensure that merchants' maintain their ability to choose how debit transactions are routed, you should make sure that you are not programming any of these three AID selection configurations, shown on the following slides, into your merchants' terminals.

First Data.

Examples of Not Utilizing Application Selection

- Configuration #1: AID Selection Screens
  - Cardholder presented with display of available AIDs
- Configuration #2: AID Selection Based on Issuer Priority
  - Solution auto selects the first priority AID listed on chip
- Configuration #3: Credit/Debit Selection Screens Used to Select the AID
  - Solution prompts cardholder for ‘Credit/Debit in order to select AID

It is imperative to note that all three scenarios do not allow the merchant to select how the debit transaction is routed.

First Data.

Configuration #1: AID Selection Screens

- Under the first configuration, the cardholder is presented with an AID selection screen, which requires *the cardholder* to select the AID before the transaction may proceed.
- The terminal displays a screen with the two AID labels—for example, “Visa Debit” and “US Debit”—and requires the cardholder to choose one.
- The cardholder, of course, does not know what an AID is, and does not understand the meaning of these labels. They do not understand, for example, that pressing “Visa Debit” takes away the merchant’s choice of network and makes the transaction more expensive for the merchant. And they have no idea what “US Debit” means, since it is not a real brand name and they’ve never heard of it.
- As a result, the vast majority of cardholders press the “Visa Debit” button, since they are at least familiar with the “Visa” brand. The result is that the transaction will be processed over the Visa network and the merchant will lose the ability to choose any other network, resulting in higher costs to the merchant.
- This terminal configuration is relatively easy to identify at the POS, as the AID selection screen will appear when an EMV debit card issued in the US is used for a transaction at the terminal.
- On November 2, 2016 the Federal Reserve updated its FAQs, stating networks that require merchants to deploy screens that prompt the cardholder to choose between applications, one that routes to at least two unaffiliated networks and another that routes to a single network, are not compliant with Regulation II (aka the Durbin Amendment).

Configuration #2: AID Selection Based on Issuer Priority

- The second configuration identified is where the terminal is programmed to automatically select the AID based upon the priority assigned to each AID by the card issuer.
- Per Visa's rules, every issuer in the US is mandated to prioritize Visa's proprietary Global AID over the Common AID on every debit card. [Visa Rule 4.1.23.51]
- Any terminal that is configured to automatically select the AID based on issuer priority will *always* select the Global AID, since the issuer is required to *always* prioritize the Global AID over the Common AID on the card, and the terminal will therefore route 100% of the merchant's debit EMV transactions to the Global AID. Merchants and their acquirers lose any ability to route transactions to a different network.
- To determine if a terminal is configured to automatically select the AID based upon issuer priority, conduct a transaction on the terminal. If prompted by the terminal to select a form of authentication (such as "Debit/Credit" buttons, or a PIN prompt that allows for PIN bypass through a "Cancel" or "Signature" button), conduct one transaction using each form of authentication. Do *not* ask for "cash-back" on any of your transactions.
- Once you are done, examine the AIDs printed on the receipt or receipts that were printed.
- If you only conducted one transaction because the terminal did not prompt you to select a form of authentication, the AID printed on the one receipt should be the Visa U.S. Common Debit AID (A0000000980840) or the Mastercard U.S. Common Debit AID (A0000000042203). This indicates that the terminal is configured properly. If the receipt instead refers to the Visa Debit Global AID (A0000000031010) or the Mastercard Debit Global AID (A0000000041010), this means that the terminal is configured to select the AID based on issuer priority. As a result, the merchant will not have routing choice on any of its debit transactions, as these will all be routed to the Global AID and one of the Global Brands.
- If you have two receipts because the terminal prompted you to select a form of authentication, the Visa U.S. Common Debit AID (A0000000980840) or the Mastercard U.S. Common Debit AID (A0000000042203) should be printed on both receipts. This indicates that the terminal is configured properly. If instead *both* receipts reference the Visa Debit Global AID (A0000000031010) or the Mastercard Debit Global AID (A0000000041010), this means that the terminal is configured to select the AID based on issuer priority. As a result, the merchant will not have routing choice on any of its debit transactions, as these will all be routed to the Global AID and one of the Global Brands.
- If you have two receipts and they refer to *different* AIDs, this indicates that the terminal is configured to select the AID based on the cardholder's chosen form of authentication. We will discuss this third terminal configuration next.

First Data.

Configuration #3: Debit/Credit Selection Screens Used to Select the AID

- The final incorrect configuration we have seen is where the terminal presents the cardholder with the traditional “Debit/Credit” selection buttons. But *instead* of using these buttons to select the form of authentication, as has historically been done, the terminal is configured to *also* use these buttons to select the AID.
- Specifically, if the cardholder selects “Debit,” indicating that they wish to enter a PIN for the transaction, the terminal selects the Common AID and prompts the cardholder for a PIN. But if the cardholder selects “Credit,” indicating that they wish to sign for the transaction, the terminal routes the transaction to the Global AID and prompts the cardholder for a signature.
- This means that *every one* of the merchant’s signature-authenticated EMV transactions are routed over the Global AID and locked-in to one of the Global Brands – Visa or MasterCard. The merchant and its acquirer are unable to route the transaction over any of the other networks on the debit card that can facilitate signature-authenticated transactions (such as STAR and PULSE).
- The easiest way to determine if the terminal is configured to use the “Debit/Credit” buttons to select the AID is to process two transactions on the terminal using the same US-issued EMV card. In the first transaction, press the “Debit” button to complete the transaction. In the second, press the “Credit” button. In both transactions, if asked, do *not* ask for “cash-back.”
- Next, compare the AIDs used for each of the two transactions (which should be printed on the receipts). If the terminal is configured properly, the AID printed on *both* receipts should be the Visa U.S. Common Debit AID (A0000000980840) or the Mastercard U.S. Common Debit AID (A0000000042203).
- If pressing the “Credit” button resulted in selection of the Visa Debit Global AID (A0000000031010) or the Mastercard Debit Global AID (A0000000041010), this indicates that the “Debit/Credit” buttons are being used to select the AID, taking away the merchant’s routing choice whenever the “Credit” button is selected.
- If *both* receipts reference the Visa Debit Global AID (A0000000031010) or the Mastercard Debit Global AID (A0000000041010), this means that the terminal is configured to select the AID based on issuer priority, which we discussed earlier.

First Data.

Contactless Readers

- It also is important to understand that many terminals are configured to handle contact-based cards differently than contactless cards. In particular, we understand many terminals have been programmed to automatically route all contactless transactions based upon AID priority, even if they route contact-based transactions using the Common AID. This means that all contactless transactions will be routed to the Global AID and the Global Brands, taking away merchant network choice whenever a contactless card or device is used.
- In programming terminals, it is important to ensure that both contact and contactless debit transactions utilize the Common AID, to ensure that the merchant is not losing their routing choice on either type of transaction.

First Data.

EMV No CVM Transactions

- No CVM is a CVM method that the terminal and the card can support. Although it does not employ verification of the cardholder like signature or PIN it is still a CVM.
  - Unlike failed CVM which means that no CVM method was used or agreed upon between the card and the terminal. Perhaps a minor distinction, but *No CVM will pass front end edits on the values in the CVM Results field, failed CVM does not always depending on the front end.*
- If No CVM is used then the transaction could be routed to a debit network if:
  - The merchant is participating in the PINless POS Product and
  - The POS device supports the PINless POS Product and
  - The final amount is known and the amount is under the No CVM limit set by the networks.
- If the transaction or merchant does not qualify for PINless POS and the transaction includes one of the common AID's the transaction will be routed to Visa, Mastercard or Discover.
  - Amex does not support a common debit AID.

First Data.

PIN Bypass

- PIN bypass is recommended to be supported in order to allow cardholders the option to not enter a PIN value when the merchant allows.
- Common AID's only support online PIN and No CVM as potential CVM methods. PIN bypass functionality may be allowed at the merchants discretion. CAID Transactions where PIN bypass is utilized will result in No CVM as the CVM method used.
- PIN Bypass is supported in most kernel configurations. During the Intake process, be sure to know definitively whether the kernel configuration and the POS Solution will support PIN Bypass or not. If PIN bypass is not supported during the initial certification a recertification may be required. Please see EMVco Bulletin #11.
- **PIN Bypass is NOT allowed on International Maestro, Interlink or Interac**
  - PIN Bypass is NOT allowed on Maestro (A0000000043060), Interlink (A0000000033010) and Interac (A0000002771010) Global AIDs. In the event that PIN bypass is allowed and the transaction is sent to the host, it will be declined as the transaction cannot be sent to these networks without a PIN.

First Data.

Debit Expansion Program

First Data.

PINless POS Product

First Data.

PINless POS Product

- By accepting PINless POS Debit transactions merchants can enable their customers to pay for their transactions with their debit card without using a PIN.
  - The transaction is $50.00 or less.
  - The entry mode can be magswipe, contact or contactless EMV.
    - For EMV transactions only the Common AIDs will support the PINless POS Product
  - Manual entry or eCommerce is not supported
- PINless POS Debit is a type of transaction where a consumer can pay with the same card they otherwise would use at the ATM with a PIN or at the POS with a signature or a PIN.
- Each individual merchant location must agree to participate in the PINless POS Product and they must be set up for traditional debit processing (STAR, NYCE, Pulse etc.)
- There are indicators on both the North and Buypass platform that need to be set at the merchant location level that tell the front end the merchant is participating in the PINless POS Product.
- The Omaha front end does not currently support the PINless POS Product.

First Data.

PINless POS Product

- **Retailer Value – Improving Time, Control, and Economics**
  - A cost effective routing replacement for signature and no-signature debit transactions
  - Speeds up checkout
  - Improves cardholder convenience by allowing a simple swipe, avoiding confusion and the extra steps of entering a PIN for transactions under $50
  - Potentially improves overall checkout experience translating to higher loyalty and sales
  - A convenient new, no PIN required payment solution targeted at certain merchant categories

- **The Challenge**
  - There are multiple choices available when it comes to debit networks that offer PINless programs currently.
  - Fundamental changes are taking place in the payments industry, creating greater value for merchants
  - Maintaining a healthy competitive playing field which is essential to preserve a healthy US payments environment
  - Losing customers who are in line for too long
  - Losing customers because they are not PIN-enabled
  - Losing customers because they are not swipe-and-go enabled

First Data.

PINless POS Product

- The POS device must be coded to send in the indicators that tell the front end that it supports the PINless POS Product and is configured to accept the response back that the transaction routed single message debit as well as print the network label ID on the receipt.
- For any debit card transaction without a PIN, the following are the current **requirements** for coding consideration (excludes PINless Bill Payment transactions which remain constrained to the legacy requirements):
  - Submission as a Dual/Credit message type
  - If EMV, and the US Common Debit AID is present, the Common AID **MUST** be chosen for the transaction. (Global AIDs cannot be routed as PINless / No CVM to any other Network than the one on the front of the card.)
  - If EMV and Common AID, the priority CVM will be PIN. In the event the transaction does not have a PIN either because it was bypassed or the device selected 'No CVM' there is an opportunity for the transaction to route either PINless or Signature.
  - Regardless of EMV or Mag-Stripe **no** PIN Block data is sent because the transaction is sent as dual message – specific requirements for populating the PIN Block data element vary by specification.

- *Regardless of EMV or Mag-Stripe one of the following must be **submitted** in a request message:*
  - *A transaction level indicator **submitted** in request message, defining that the transaction can be alternately routed to a single message debit network (PINless Debit Indicator) – specific field varies by specification*
  - *A transaction level indicator **submitted** in request message, defining that the transaction can only be routed to a dual message network. (IE: transactions that are not the final amount/ TIP).*
- Reconciliation to include batching and reporting of transactions based on the network label / id and/or the other indicators as returned in the authorization response message.

First Data.

PINless POS Product

- *The following MCC's cannot be flipped to single message in support of the PINless POS Product*

MCC	Merchant Description
4813	Key-entry Telecom Merchant providing single local and long distance phone calls using a central access number in a non-face-to-face environment using key entry
4829	Money Transfer
5542	Fuel Dispenser Automated
5960	Direct Marketing Insurance
5962	Direct Marketing Travel-Related Arrangement Service
5964	Direct Marketing Catalog Merchants
5966	Direct Marketing Outbound Telemarketing Merchants
5967	Direct Marketing Inbound Telemarketing Merchants
5968	Direct Marketing Continuity/Subscription Merchants
5969	Direct Marketing Other Direct Marketers not elsewhere classified
6010	Member Financial Institution- Manual Cash Disbursement

MCC	Merchant Description
6011	Member Financial Institution-Automated Cash Disbursements
6012	Financial Institution- Merchandise and Services
6050	Quasi Cash – Member Financial Institution
6051	Quasi Cash – Merchant
6531	Payment Service Provider – Money transfer for a purchase
6532	Payment Transaction – Member Financial Institution
6533	Payment Transaction – Merchant
6534	Money Transfer – Member Financial Institution
7995	Gambling Transactions
9405	Intra-Government Purchases – Government Only
9700	International Automated Referral Service
9702	GCAS Emergency Services
9754	Gambling – Horse Racing, Dog Racing, State Lotteries
9950	Intra-company purchases

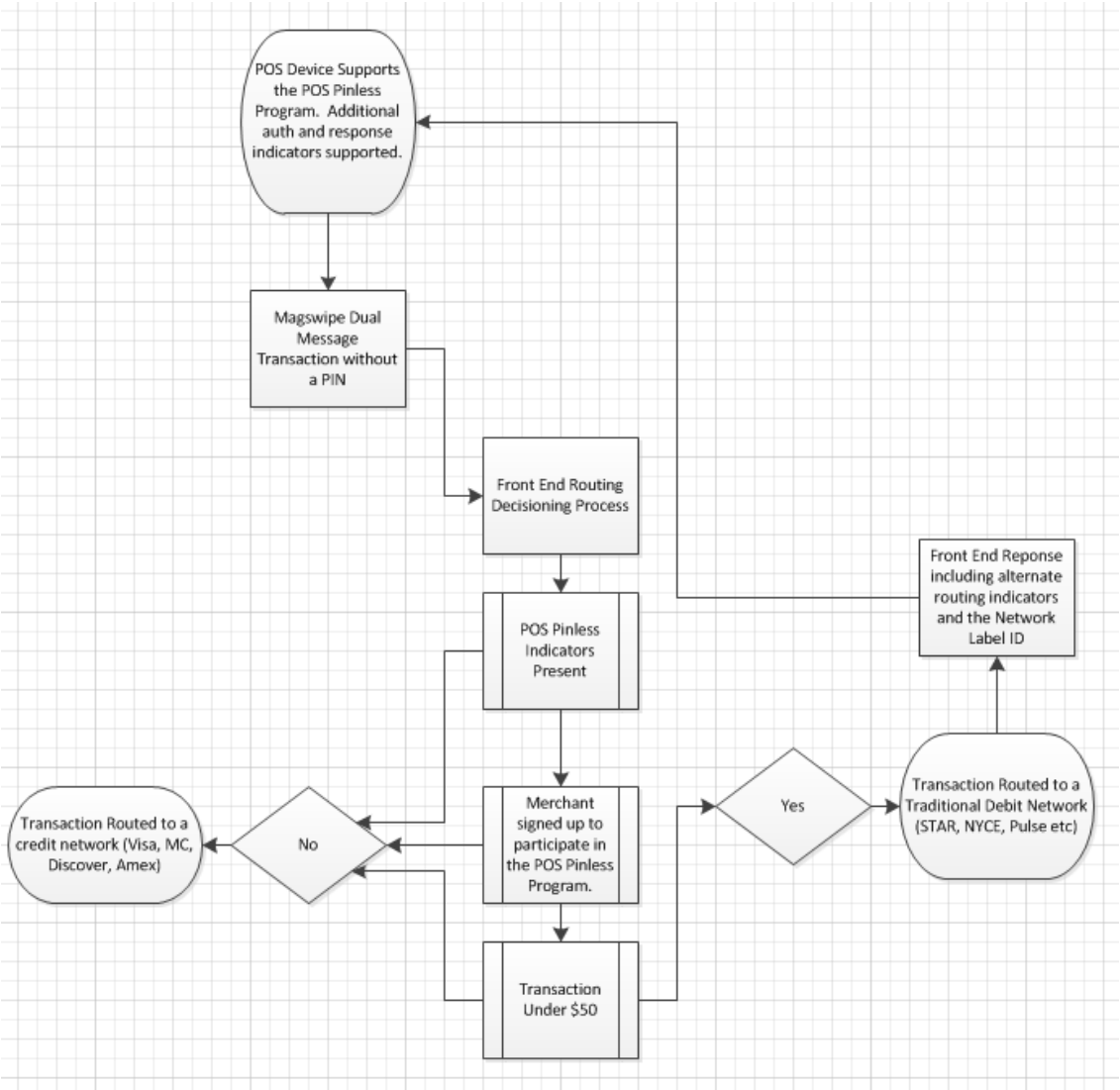
First Data.

Scenarios Where a No CVM Transaction Doesn't Qualify as PINless POS

- Single message formatted transaction.
- Merchant does not participate in PINless POS
- POS device does not support PINless POS
- Transaction amount is over $50
- EMV transaction includes one of the Global Credit or Global Debit AIDs
- EMV transaction was initiated with the Interac AID
- Online PIN, Offline PIN, ODCV (On Device Cardholder Verification) or signature were present
- Final amount is not known

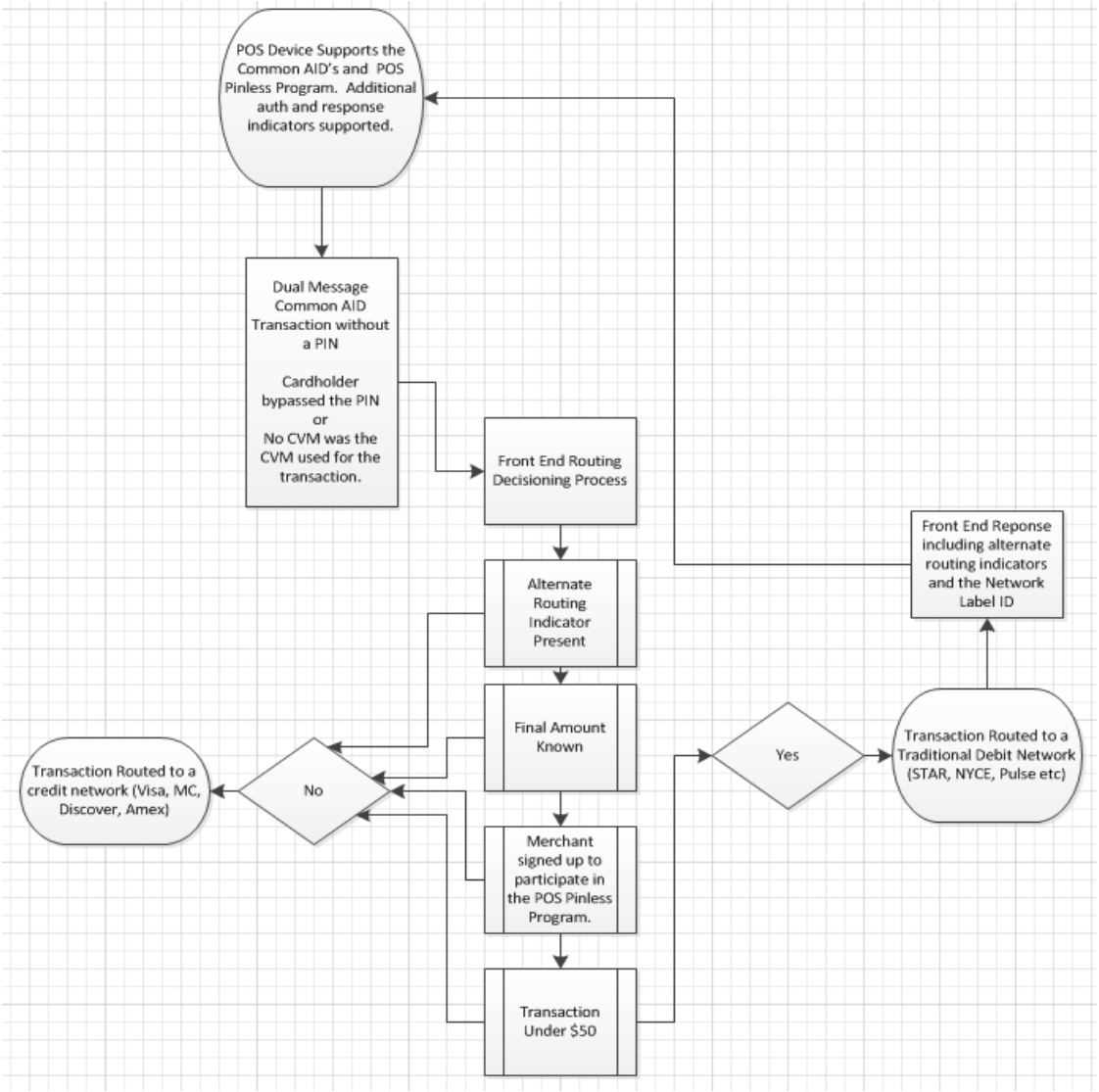
First Data.

PINless POS Magswipe No PIN Transaction Flow



First Data.

PINless POS No PIN EMV Common AID Transaction



First Data.

Signature Debit Product

First Data.

Signature Debit Product

- **Description**
  - First Data has introduced a new Signature Debit Product offering that will enable expanded authentication options including signature, no-signature and no cardholder verification method (No CVM). The new Signature Debit Product reinforces First Data's ongoing strategy to provide its members with support for all debit transactions, through all payment channels, using all payment devices.
- **Signature Debit Product Provides Choice**
  - The Signature Debit Product will provide greater convenience and choice for debit transactions for financial institutions, cardholders, acquirers, and merchants. The Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act gave merchants the right to determine routing and required issuers to provide a routing choice for debit products. First Data's Signature Debit Product offers an alternative solution by expanding functionality to include full signature debit and no-CVM capabilities.

First Data.

Signature Debit Product Offers New Benefits

- The infrastructure to support the Signature Debit Product will provide the following benefits:
  - Helps issuers in meeting their Durbin compliance obligations by enabling additional networks as an alternative routing choice on the card for use on transactions without a PIN.
  - Provides alternate routing options for larger merchants, not just PIN and PINless-based transactions
  - A cost effective routing replacement for signature and no-signature debit transactions
  - Improves cardholder convenience by allowing a simple dip/tap/swipe, avoiding confusion and extra steps for selection of debit/credit or PIN/Signature
  - Providing choice allows merchants to have more control over their payments environment and gives consumers more ways to pay.

First Data.

Signature Debit Product - Functionality

- EMV chip processing for our Signature Debit Product depends on the implementation of the common AID's; only common AIDs can be routed as Signature Debit as the global AIDs do not support alternate routing.
- Participating merchants must obtain a signature and record it on the transaction receipt for each transaction processed as signature debit, if the transaction amount is greater than $50 (transactions up to $50 do not require a signature).
- Coding changes are required to support the Signature Debit Product and alternate routing indicators as specified in the First Data specifications.
- Support of a new entitlement. (Entitlement = MasterCard, Visa, Signature Debit etc..)
- Signature Debit Product transactions must be bucketed or reported separately from traditional debit or credit transactions.
- Support for receiving a network label ID in the response and printing the network label on receipts and reports.

First Data.

Visa PIN-Authenticated Visa Debit Single Message System Processing Requirement – US Region

First Data

Visa PIN-Authenticated Visa Debit Single Message System Processing Requirement – US Region

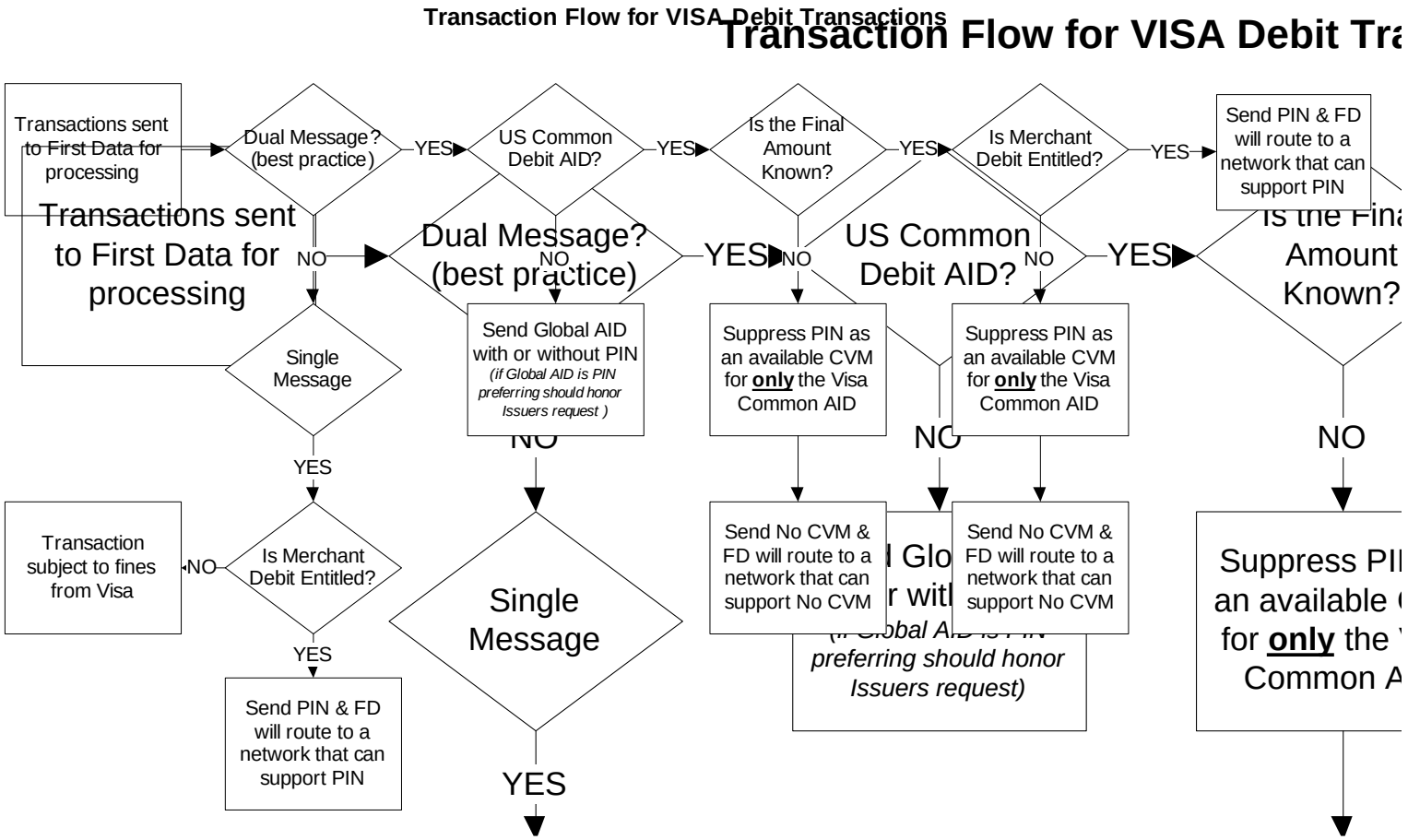
- *Visa Rule ID# 0027085: PIN-Authenticated Visa Debit Transaction Single Message System Processing Requirement – US Region - "A US Acquirer must ensure that a PIN-Authenticated Visa Debit Transaction is processed as an Online Financial Transaction through the Single Message System." Visa Core Rules and Visa Product and Service Rules*
- The priority cardholder verification method (CVM) on the Visa Common AID is PIN MasterCard and Discover allow and are encouraging the capture of a PIN for EMV transactions regardless of the processing method used to submit the authorization request - single or dual message.
- Visa cannot accept CAID transactions with a PIN into their dual message / credit network. In order to comply with that rule if the Visa CAID is selected and the merchant is either not entitled for debit (i.e. STAR, NYCE, Pulse) or the final amount is not known at authorization time (i.e. the transaction is forced to route to a credit network) the terminal must not prompt for PIN. The POS solution must know that in these situations it must not prompt for PIN at the time of authorization and must revert to a No CVM kernel configuration.
- The No CVM Visa CAID dual message transaction will be routed to Visa and the POS device must print a signature line if the transaction amount is above the No Signature program limits determined by the merchant category code (MCC) as set by Visa.

First Data.

Visa PAVD

- All POS devices must be coded to not prompt for an Online PIN if:
  - The merchant is not entitled for traditional debit processing
  - The final amount of the transaction is not known, regardless if the merchant is entitled for traditional debit processing or not.
  - These transactions do not qualify for the PINless POS Product.
- The Visa Common Debit AID (CAID) is the only AID that is required to have special logic to ensure a transaction with an online PIN is not sent to the Visa dual message network.

Transaction Flow for PAVD



First Data

PAVD At Risk Transaction Scenarios

Transaction scenarios that could lead to a PAVD violation.

CAID Entitlement Scenarios and PAVD Impact: Recap

CAID SCENARIO	ENTILEMENT	CAID	9F33	SENT DUAL	PIN BYPASS	CVM	AMOUNT	FINAL AMOUNT INDCATOR	FE DELVERY NETWORK	COMMENT
1	Credit Only	DSC/MC/Visa	All CVM	Y	N	Online PIN	Any	NA	Credit	PAVD violation for Visa CAID
2	Debit/Credit Only	DSC/MC/Visa	All CVM	Y	N	Online PIN	Any	Y	Credit	PAVD violation for Visa CAID
3	Debit/Credit with PINless	DSC/MC/Visa	All CVM	Y	N	Online PIN	Any	Y	Credit	PAVD violation for Visa CAID

NOTE:

This grid is a high level snap shot of potential transaction scenarios that may lead to a PAVD violation.

The key assumptions are that an EMV POS Solution that supports:

- Common Debit AID
- Dual Message
- Online PIN CVM

The key parameters that can lead to a violation are:

- Entitlement
- Support of PIN ByPass
- Use of Final Amount Indicator (Card Type Indicator set to 'T' (Tip) or 'C' (Credit) for Omaha)

PAVD violation occurs when a Visa Common Debit AID is sent down a credit path with Online PIN CVM

First Data.

Specification Information

For Informational Purposes Only – please refer to the latest specification document to make sure you have the latest information.

First Data.

First Data ISO 8583 Global Spec (North & Nashville)

Specifications		First Data ISO 8583 Global Spec (North & Nashville)
PINless POS (Alternate Routing Indicator)	Field Descriptor	TAG OC Position = 1 Subfield Name = Alternate Routing Indicator
	Value Sets	0 -Terminal does not support Alternate Routing 1 - Terminal supports
Signature Debit	Field Descriptor	TAG OC Position = 2 Subfield Name = Signature Debit
	Value Sets	0 - Signature Debit Not Supported 1 - Signature Debit Supported
Final Amount Indicator	Field Descriptor	Table SD TAG PF
	Value Sets	Supplemental Data Table Pre/Final Authorization Indicator (Message Format 0100/0120)

First Data

Buypass ISO 8583 Spec

Specifications		Buypass ISO 8583 Spec	
PINless POS (Alternate Routing Indicator)	Field Descriptor	PINless POS Debit Acceptance	Card Accepted as Processing Code
	Value Sets	Mandatory in a PINless POS Debit 0200 Transaction Request and Time-out Reversal 0420 Transaction Request. Identifies the acceptance of PINless POS Debit transaction processing. Valid Codes/Values: Code Description 0 - Device does not accept PINless POS Debit transactions 1 - Device accepts PINless POS Debit transactions 2 - Device accepts non-traditional Signature Debit transactions X - Original transaction was processed via non-traditional Signature Debit processor Note: Value 'X' is applicable for follow-up transactions (such as, 0220, 0420, Incremental Authorization) ONLY. Note: Table 29 is not returned on a Time-out Reversal 0430 Transaction Response. Note: This field is echoed from the PINless POS Debit Transaction Request.	Mandatory in a PINless POS Debit Transaction Request: Fixed Value: 999999 Indicates how the transaction was processed. Valid Codes/Values (Code Description): 003000 - Transaction processed as Credit 000000 - Transaction processed as Debit
Signature Debit	Field Descriptor		
	Value Sets	(pinless and sig in one feature today)	
Final Amount Indicator	Field Descriptor	Table ID: n2 Table Length: n3 Table Data: an1	
	Value Sets	Fixed value: 039 Fixed value: 001 Indicates that the Settlement Amount may differ from the original Authorization Amount. Note: This data element should NOT be sent in transactions where the final Settlement Amount will be the same as the original Authorization Amount. Valid Codes/Values: Code: 1 Description: Final transaction amount may change on EMV transactions only	

First Data.

Buypass ATL105 Spec

Specifications		Buypass ATL105 Spec
PINless POS (Alternate Routing Indicator)	Field Descriptor	PINless Debit Acceptance
	Value Sets	This field is mandatory for requests in which the POS device will accept PINless debit. Valid Values: 0 = Device does not accept PINless Debit 1 = Device accepts PINless Debit 2 = Device accepts non-traditional Signature Debit X = Original transaction was processed as non-traditional Signature Debit (follow up transactions only
Signature Debit	Field Descriptor	
	Value Sets	(pinless and sig in one feature today)
Final Amount Indicator	Field Descriptor	Table ID: n3 Table Length: n3 Table Data: an1
	Value Sets	Fixed value: 040 Fixed value: 001 Indicates that the Settlement Amount may differ from the original Authorization Amount. Allowed on EMV initial transactions where the final Settlement Amount may be different from the original Authorization Amount. Note: This data element should NOT be sent in transactions where the final Settlement Amount will be the same as the original Authorization Amount. Value: 1 Description: Final transaction amount may change on EMV transactions only

First Data.

Rapid Connect (North/Nashville)

Specifications		Rapid Connect (North/Nashville)
PINless POS (Alternate Routing Indicator)	Field Descriptor	XML Tag Name: PLPOSDebitFlg
	Value Sets	Request Values: 1 – PINLess POS Debit is supported Response Values: C – Processed as Credit D – Processed as Debit
Signature Debit	Field Descriptor	XML Tag Name: NetAccInd
	Value Sets	Request Values: 1 – Routing as STAR Signature Debit is supported C – Routed through STAR Signature Debit Note: The value of 'C' must be present in subsequent transactions only when the Response Value of 'C' was returned in the original transaction response. Response Values: C – Routed through STAR Signature Debit
Final Amount Indicator	Field Descriptor	XML Tag Name: FinAmtInd
	Value Sets	Request Values: The following values are defined for this field: 1 – Final amount not known at the time of Authorization Rules: The following field rules are defined: - This field may only be sent in an EMV Credit Authorization transaction. - This field must be sent in an EMV Credit Authorization transaction when the final amount is not known at the time of Authorization, except when the Terminal Category Code is 05 and the merchant does not want to support EMV Credit only transactions

First Data.

Rapid Connect (Buypass)

Specifications		Rapid Connect (Buypass)
PINless POS (Alternate Routing Indicator)	Field Descriptor	XML Tag Name: PLPOSDebitFlg
	Value Sets	Request Values: 1 – PINLess POS Debit is supported Response Values: C – Processed as Credit D – Processed as Debit
Signature Debit	Field Descriptor	
	Value Sets	Not available for Buypass RC - Target 17.04
Final Amount Indicator	Field Descriptor	XML Tag Name: FinAmtInd
	Value Sets	Request Values: The following values are defined for this field: 1 – Final amount not known at the time of Authorization Rules: The following field rules are defined: - This field may only be sent in an EMV Credit Authorization transaction. - This field must be sent in an EMV Credit Authorization transaction when the final amount is not known at the time of Authorization, except when the Terminal Category Code is 05 and the merchant does not want to support EMV Credit only transactions

First Data.