

Global Partner Management Bulletin

Spring 2009

Dear First Data Integrator,

This year's "Spring Release" notice has an expanded format, designed to provide you with as much information as possible while you plan for your next release. It includes the required association changes (Spring Release) as well as upcoming compliance changes, past due notices, PCI Compliance reminders, and exciting new First Data products that your merchants are requesting.

As a reminder, you are required to use the most current First Data specification which includes the mandatory "TPP ID" field when recertifying. For a complete list of business/certification requirements, see the "Resources" section of this bulletin.

The items outlined in this bulletin may or may not have an impact to your current applications and is for informational purposes only.

Best Regards,
Global Partner Management
gpm@firstdata.com

Document Contents

Section 1: Spring Release Compliance Mandates.....	Page 2
Visa Changes	
Mastercard Changes	
Section 2: Additional Important Changes.....	Page 5
MasterCard	
American Express (CAPN Phase 3)	
Healthcare Spending Cards (IIAS)	
Discover® BIN Ranges	
Section 3: Past Due Compliance Notices.....	Page 10
American Express (CAPN Phases 1 and 2)	
Section 4: PCI Compliance Requirements.....	Page 12
Overview	
Transition from PABP to PA-DSS	
Vulnerable Payment Applications	
Section 5: New First Data Products.....	Page 13
American Express OnePoint® Program	
Loyalty Solutions	
Mobile Commerce GO-Tag™ Solution	
Resources	

Section 1: Spring Release Compliance Mandates

Please note that you are required to certify using the most [current specification version](#) located on www.fdms.com and send in a pre-assigned value in the “TPP ID” field. The TPP ID value will be assigned by Global Partner Management when you submit the certification request. Certification requests will be delayed until these two requirements are met.

VISA Changes

1) Changes to CPS/Small Ticket Fee Qualification

The CPS/Small Ticket program for consumer credit will be extended to MCC 5541 (Service Stations) for transactions that are \$15 or less. Visa Signature Preferred (VSP) transactions for MCC 5541 will not receive the CPS/Small Ticket interchange rate. They will continue to receive the VSP Fuel interchange rate.

The extension of Small Ticket will not apply to Visa Check Card or commercial card products. As a reminder, under the current No Signature Program and CPS/Small Ticket Payment Service, the merchant is not required to obtain a cardholder signature and is only required to provide a transaction receipt if one is requested by the cardholder. These requirements remain in effect.

First Data will make the appropriate updates to the qualification requirements for CPS/Small Ticket to include MCC 5541.

2) Changes to Visa Fleet Fuel Product Codes

Visa will change its fuel code structure to align with the October 2006 industry standard published by the Petroleum Convenience Alliance for Technology Standards (PCATS). This alignment will provide additional information for the types of Visa Fleet fuel codes that can be reported, including alternative fuels such as biodiesel, marine fuels, and aviation fuels.

Fleet and commercial card fuel transactions must contain the proper Visa Fleet Fuel Type code.

*Visa has provided mapping of existing values to the new Visa Fleet Fuel Type codes as a temporary solution. Effective **April 2010**, when fuel types are provided, merchants must submit the full range of new Fleet Fuel Type codes for Fleet and commercial card fuel transactions. Merchant specifications will be updated to align the new and revised Fuel Type codes. Merchants must update their terminal products to send the proper Fuel Type codes if they use the Visa defined codes. If a merchant uses PCATS or proprietary codes that provide the same level of detail, First Data will map to the Visa defined codes. The specifications and the authorization hosts to support the product codes were updated on **April 17, 2009**.*

3) Acquirer Mandate for Visa PayWave (Contactless) Transactions

Visa mandated, with the 08.2 Release, that Acquirers update their authorization hosts to support certain tags in authorization Field 55, Usage 1-VSDC Chip Data to:

- Support an Authentication Service to detect counterfeit cards
- Identify the form factor (card, fob, or phone) used at the point-of-sale
- Support of global inoperability for Visa PayWave transactions

The Visa PayWave (Contactless) Payment Specification 2.x contains the requirements for Field 55 and serves as an extension of the existing 1.4.2 specification. Visa will discontinue support of version 1.4.2 at a future date. All existing and new PayWave (Contactless) merchants must comply with the new 2.x specification by **2012**.

First Data implemented the necessary changes to accept transactions submitted with the 2.x PayWave specifications in preparation for merchant migration which will require terminal replacement or a contactless reader upgrade by January 1, 2012. Merchants performing contactless transactions conducted with products using the 1.4.2 specification will be unable to accept contactless transactions when migration to the new specification is complete.

4) Visa announced changes for an existing fee and the addition of new processing related fees

Zero Dollar Verification Messages

A Zero Dollar Verification message provides a means of validating a cardholder account number and other authenticating elements such as AVS and CVV2.

- Current fee is \$0.025/transaction and this amount will not change
- Effective **February 1, 2009**, additional authorizations such as declined messages and those containing AVS will be assessed the fee.

5) Misuse of Authorization – New Fee

This fee will be applied to authorizations that are not followed by a matching clearing transaction (or in the case of a cancelled or timed out authorization, not properly reversed). The new fee is \$0.045/authorization and is effective **July 1, 2009**. Criteria includes:

- Authorizations will be matched with corresponding clearing or authorization reversal transactions by means of the Tran ID
- For successful matching and to avoid the fee, clearing must occur within 10 days of authorization for all MCCs, with the exception of T&E which must clear within 20 days
- For cancelled or timed out authorizations the authorization reversal must be processed no later than 24 hours following the original authorization for card present authorizations or 72 hours for card-not-present authorizations

6) Zero Floor Limit – New fee

This fee will be applied for any clearing transaction submitted without proper authorization. The new fee is \$0.10/transaction and is effective **July 1, 2009**. Criteria includes:

- The Tran ID will be used to validate a 'proper' authorization
- Fee will be assessed on clearing transactions that cannot be matched to previously approved or partially-approved authorization transactions

For questions and additional information regarding Visa's data security requirements (CISP/PCI), please visit: http://usa.visa.com/business/accepting_visas_ops_risk_management/cisp.html

7) Extension of Product Identification

	North	South	Memphis	Atlanta	Omaha
Authorization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Settlement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Back-Office	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

Visa will implement changes for global product identification. In its first phase, product IDs will be assigned to all products issued in Canada. Product result (62.23) will be extended to all products in Canada. Additionally, existing product ID values will be reused for global products.

Visa mandates that acquirer processors receive the product results in Field 62.23 - Card-Level Results in all authorization responses and return these values in settlement transactions. The product result is included in the validation code calculation.

Card-level processing ensures that the product processing identified in the authorization is the same product used for settlement. In addition, card-level processing allows for the future expansion of card-level processing to other consumer and business products, as well as support unique product-based processing requirements.

The Card-Level Results field is required for proper interchange qualification; if the validation calculation fails the best rate a merchant can receive is EIRF. Derivation logic will be extended to Canadian issued cards for those merchants still not providing field 62.23.

Applicable FD specifications including field 62.23 were available in **April 2007**. Transactions that are matched with FD authorizations will not be required to contain the new field. Merchants not authorizing through an FD platform or who do not participate in the authorization matching process will be required to accept the field in the authorization response and include it in the settlement record.

Mastercard Changes

Partial Approval Amount Edit Changes

	North	South	Memphis	Atlanta	Omaha
Authorization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Settlement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Back-Office	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

MasterCard is modifying the edit that verifies approval amounts at automated fuel dispensers (AFDs) to allow a partial approval amount greater than the amount provided in the authorization request.

The Authorization System currently rejects partial approval amounts greater than the AFD pre-authorization transaction amount of USD 1 because the partial approval amount is greater than the requested pre-authorization amount.

This enhancement will allow the issuer to respond with a partial approval amount that is greater than the initial transaction amount (assuming the acquirer is using the market practice of USD 1 pre-authorizations), when the cardholder's available balance is less than the AFD transaction's chargeback protection amount.

MasterCard will no longer perform the partial approval amount edit for AFD transactions.

The Authorization System will allow the amount authorized by the issuer to be less than, greater than, or equal to the amount requested by the acquirer when the merchant category code is 5542.

The merchant's terminal must also support partial approvals. Only after support of the merchant's terminal for partial approval has been verified can the issuer indicate partial approval of a transaction.

*Reminder: MasterCard mandated merchant support of partial approvals, a reversal request to update the cardholder's open-to-buy balance, and account balance responses in three phases. Compliance Alert 0808507 provides the mandate schedule which begins **May 2010** and will end in **May 2011**. The phases are determined by the merchant type. Automated Fuel merchants must support these features in Phase 1, May 2010.*

Business owners must ensure merchants support partial approvals and that the fuel dispenser is capable of shutting off upon reaching the partial approval amount.

Section 2: Additional Important Changes

Please note that you are required to certify using the most current specification version located on www.fdms.com and send in a pre-assigned value in the "TPP ID" field. The TPP ID value will be assigned by Global Partner Management when you submit the certification request. Certification requests will be delayed until these two requirements are met.

MasterCard

MasterCard is announcing a mandate for acquirers in the U.S. region to support partial approvals, support sending a reversal request or advice to update the cardholder's open-to-buy balance, and support sending account balance responses within the Banknet® telecommunications network and the MasterCard® Debit Switch (MDS) for debit and prepaid transactions.

The mandate will apply to acquirers supporting merchants within select card acceptor business codes/merchant category codes (MCCs) and will be effective in five phases as announced in the article.

As indicated by MCC and implemented in the following phases:

Phase 1: 1 May 2010

Phase 2: 1 November 2010

Phase 3: 1 May 2011

Subsequent to the U.S. region issuer mandate for partial approvals, real-time reversals, and account balance responses announced in *Global Operations Bulletin* No. 9, 4 September 2007, MasterCard is mandating that all acquirers and merchants that acquire Debit MasterCard and Maestro transactions must support the partial approval of authorization transactions and real-time transaction reversals (full and partial) and account balance responses from the point-of-sale (POS).

U.S. region acquirers and merchants that acquire Debit MasterCard and Maestro transactions must implement changes to support these transactions at their internal host systems and also update message formats to and including the POS devices when a merchant requests an authorization.

The mandate will apply for acquirers and merchants within select MCCs. The mandate schedule begins in May 2010 and ends in May 2011. The complete list of MCCs for which this mandate applies and their associated dates is included in this article.

Changes to Authorization Messages and Selected Transaction Types

Effective with Banknet Releases 05.2, 06.1, and 06.2 and MDS Release 06.2, MasterCard implemented changes to the authorization messages that allowed debit and prepaid issuers the option to respond to an authorization request with a partial approval, which is used to approve a portion of the originally requested transaction amount or to reverse an authorization in full or in part. The account balance response enabled issuers to provide the current available balance on the cardholder's prepaid card account within authorization responses.

Historically, the decline rates for MasterCard and Maestro debit and prepaid products have caused concern for both cardholders and merchants. A primary concern is that these issuer programs and merchant terminals do not support partial approvals. As such, if a cardholder does not have sufficient funds in the debit or prepaid card account to cover the full amount of the transaction, the transaction is declined.

To further exacerbate the problem, prepaid cardholders frequently do not know the current available balance in their accounts while at the point of sale. The partial approval enables the issuer to approve a portion of the transaction amount in the authorization request when the transaction amount exceeds the amount of funds available on the card. The merchant can then initiate split-tender processing to obtain the remainder of the purchase amount in another form of payment from the cardholder. Prepaid issuers can transmit account balance information in an authorization response, which must be printed or displayed by POS terminals programmed to accept this type of data.

The applicable MCCs and effective dates for mandated support are listed below.

Effective Date	MCC	Description
1 May 2010	5310	Discount Stores
	5311	Department Stores
	5411	Grocery Stores, Supermarkets
	5499	Miscellaneous Food Stores---Convenience Stores, Markets, Specialty Stores and Vending Machines
	5541	Service Stations (with or without Ancillary Services)
	5542	Fuel Dispenser, Automated
	5812	Eating Places, Restaurants
	5814	Fast Food Restaurants
	5912	Drug Stores, Pharmacies
	5942	Book Stores
	5943	Office, School Supply and Stationery Stores
	7829	Motion Picture-Video Tape Production-Distribution
	7832	Motion Picture Theaters
	7841	Video Entertainment Rental Stores
	8011	Doctors---not elsewhere classified
	8021	Dentists, Orthodontists
	8099	Health Practitioners, Medical Services---not elsewhere classified
	5111	Stationery, Office Supplies
	5200	Home Supply Warehouse Stores
	5331	Variety Stores
	5399	Miscellaneous General Merchandise Stores
	5732	Electronic Sales
	5734	Computer Software Stores
	5735	Record Shops
	5921	Package Stores, Beer, Wine, and Liquor
	5941	Sporting Goods Stores
	5999	Miscellaneous and Specialty Retail Stores
	8041	Chiropractors
	8042	Optometrists, Ophthalmologists
	8043	Opticians, Optical Goods, and Eyeglasses
	4812	Telecommunication Equipment including Telephone Sales
	4814	Telecommunication Services
	5300	Wholesale Clubs
	5964	Direct Marketing---Catalog Merchants
	5965	Direct Marketing---Combination Catalog---Retail Merchants
	5966	Direct Marketing---Outbound Telemarketing Merchants
	5967	Direct Marketing---Inbound Telemarketing Merchants
	5969	Direct Marketing---Other Direct Marketers---not elsewhere classified

	8062	Hospitals
1 November 2010	4111	Transportation---Suburban and Local Commuter Passenger, including Ferries
	4816	Computer Network/Information Services
	4899	Cable, Satellite, and Other Pay Television and Radio Services
	7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers
	7997	Clubs---Country Membership
	7999	Recreation services---not elsewhere classified
1 May 2011	8999	Professional Services---not elsewhere classified
	9399	Government Services ---not elsewhere classified

Debit (including prepaid) acquirers and merchants in the U.S. region must ensure that their internal host systems and message formats to and including the POS device can process partial approvals, real-time reversals, and account balance responses according to the effective dates listed for each MCC applicable for the mandate.

MasterCard will transmit the account balance information on Maestro and Debit MasterCard prepaid card accounts to acquirers, except for prepaid card accounts in the payroll, government, and flex benefits business segments.

Merchants must display or print any account balance response received for the cardholder's benefit.

MasterCard has also communicated an exception for standalone POS Terminals. A "standalone" terminal is defined as a device that is not integrated into a merchant's POS system, such that the sale has to be manually keyed into the terminal. The phase in period for standalone terminals is as follows -

- All terminals deployed after May 1, 2010 must support the requirements
- All terminals downloads performed for any reason after May 1, 2010 must support the requirements
- If a merchant's MCC has a May 1, 2011 requirement date, then that later date shall prevail to support the requirements

*For questions referring to MasterCard's related security documents please visit:
<https://sdp.mastercardintl.com/documentation/index.shtml>.*

American Express – CAPN Phase 3

American Express has granted First Data an extension for support of the below Aggregator requirements until October 31, 2009.

The third phase of the American Express Card Acceptance Processing Network (CAPN) continues to update authorization and settlement. Phase 3 changes were originally mandated by April 30, 2009, but First Data received an extension date of October 31, 2009.

As part of CAPN Phase 3, American Express is strongly recommending Aggregator type merchants to send additional data in existing fields in the Authorization and Settlement messages. Below you will find an overview of the additional data being mandated by Amex.

Authorizations (In the 1100 message type):

- **Field 26: Card Acceptor Business Code** - The MCC code that reflects the classification for the specific entity rendering goods or services (seller MCC code)

- **Field 43: Card Acceptor Name/Location** - contains 2 subfields. Subfield 1 should be unique, merchant-assigned, 20-byte max, seller/vendor code (seller ID), followed by seller location (city & street), Subfield 2 is the postal code for the seller

Submissions (in the Location Detail Addenda Record):

- **Field 6: Location Name** - spec states that Amex "strongly recommends" that aggregators include both their *aggregator business name* and the *name of the actual seller* (separated by an asterisk)
- **Field 12: Merchant Category Code** - should reflect MCC for the specific entity actually rendering the goods or services (seller), and may vary for each transaction, depending on the category applicable to the aggregator's specific sellers or vendors.
- **Field 13: Seller ID** - the unique, merchant-assigned, 20-byte max, seller/vendor code (seller ID)

Healthcare Spending Cards(IIAS)

Per the IRS notice 2008-104 below, Drug Stores and Pharmacies now have an effective date of **June 30, 2009** to implement an IIAS solution or register for the 90% rule exception as appropriate for continued acceptance of FSA/HRA cards.

Drug Stores and Pharmacies that intend to implement an IIAS solution should do so as soon as possible to begin auto-substantiation of FSA/HRA transaction and to ensure continued acceptance after June 30, 2009. The SIGIS 90% rule registration process is now available and should be completed by applicable merchants prior to June 30, 2009.

IRS Notice 2008-104
PURPOSE

This notice provides additional transition relief with respect to the use of debit cards for medical expense reimbursements at stores with the Drug Stores and Pharmacies merchant category code.
BACKGROUND

Notice 2007-2, 2007-1 C.B. 254, provides that after December 31, 2008, health FSA and HRA debit cards may not be used at stores with the Drug Stores and Pharmacies merchant category code unless: (1) the store participates in the inventory information approval system as described in Notice 2006-69, 2006-2 C.B. 107, or (2) on a store location by store location basis, 90 percent of the store's gross receipts during the prior taxable year consisted of items which qualify as expenses for medical care under § 213(d) (including nonprescription medications as described in Rev. Rul. 2003-102, 2003-2 C.B. 559).

For transactions using debit cards at stores that meet the 90 percent rule described in (2) above, employers must treat all charges to the debit card as conditional (other than copayment matches, recurring expenses, and real-time substantiation as described in Rev. Rul. 2003-43, 2003-1 C.B. 935) pending substantiation of the charges through additional independent third-party information describing the goods or services, the date of the service or sale, and the amount of the charge.

TRANSITION RELIEF

The deadline in Notice 2007-2 is extended by six months so that, after June 30, 2009, health FSA and HRA debit cards may not be used at stores with the Drug Stores and Pharmacies merchant category code unless the requirements of (1) or (2) above are satisfied.

For more information, please go to www.sigis.com.

Discover® BIN Ranges – First Data’s Discover Full Acceptance

In response to merchant demand, Discover has been working with First Data to accelerate full Discover Acceptance (First Data authorizes and settles Discover transactions). First Data has communicated to merchants utilizing internet-based, hosted systems that Discover's full set of IIN*(BIN) ranges are now available. In order for merchants to take advantage of this offer, you must update your payment application. *IIN=BIN (Issuer Identification Number = Bank Identification Number)

What are the risks of not updating?

If your application is not updated, and merchants attempt to process a Discover transaction, there will be transmission failures and merchants will be unable to complete Discover Network transactions. For example, if a card is swiped/keyed and the IIN/BIN range cannot be identified or recognized, the transaction would stop and would not be sent to Discover to determine if the card is approved or declined. This may lead to one of the following scenarios:

- Loss of sales
- More customer calls/complaints
- Greater help desk expenses
- Customer dissatisfaction
- Merchant attrition

What do you need to do?

Update your application to reflect the following IIN (BIN) ranges:

Discover Network required IIN Ranges for transaction routing

601100 – 601109	622126 – 622925 <i>China Unionpay</i>	644000 - 649999	650000 – 659999
601120 – 601149			
601174 – 601174			
601177 – 601179			
601186 – 601199			

Where can you go for the latest Discover Network news?

The VAR Connection has been set up by Discover Network to keep you informed about the latest news and updates from Discover Network. E-mails and bulletins from the VAR Connection will help ensure that your POS applications remain current and that your merchant transactions continue to grow as Discover® Network Cards become more prevalent in the marketplace. To register for free, go to DiscoverNetwork.com/VAR.

Section 3: Past Due Compliance Notices

Please note that you are required to certify using the most current specification version located on www.fdms.com and send in a pre-assigned value in the “TPP ID” field. The TPP ID value will be assigned by Global Partner Management when you submit the certification request. Certification requests will be delayed until these two requirements are met.

American Express CAPN (Phases 1 and 2) - 4th notice

Merchants are being assessed fines due to POS software application and payment gateway non-compliance with American Express CAPN requirements.
Application updates and recertification required.

If you have already complied with this requirement, please disregard this section.

Re: NOTICE American Express Card Acceptance and Processing Network (CAPN) Initiative.

CAPN is a global, multi-million dollar, multi-year technology effort that seeks to deliver a more flexible, adaptable and efficient card processing infrastructure for the American Express core processing systems – authorization, submission, clearing and settlement. Due to the size of this initiative, the requirements were rolled out in phases.

The first and second phases of the CAPN project had to be implemented by **August 31, 2007**. If you did not make application changes and recertified with First Data, your merchants are being assessed fines by Visa. The information that follows summarizes the Phase I and II requirements for your reference.

Phase I

Included authorization changes for all American Express merchants in the industries of Retail and Lodging. The retail category includes merchants such as mail/telephone order, Internet, recurring billing, parking, financial services, restaurant, Quick Service Restaurant (QSR) and entertainment.

- Support for transactions under \$1.00 authorization
- The addition of a Transaction Identifier for the purposes of tracking a transaction throughout its lifecycle.
 - If FDGS currently performs authorization matching on your behalf, then FDGS will match this data at settlement.
- Enhanced POS Data Codes - The POS Data code consists of 12 positions, and American Express will use the field to identify terminal capability, security data, and specific conditions present at the time of the transaction. For example, Position 1 indicates the Card Data Input Capability, which may be Mag Stripe read, Integrated Circuit Card (ICC), Key entered etc.
 - If FDGS currently performs authorization matching on your behalf, then FDGS will match this data at settlement.
 - If you support recurring/MOTO ECI feature, then you are required to pass the valid recurring indicator at authorization and at settlement.
 - FDGS cannot perform matching for this field.
- Support Amex Prepaid Cards for partial authorization and authorization with balance return.
 - Merchants interested in using this feature, may certify with FDGS.
- Enhanced Keyed CID validation responses.
 - Merchants must be registered with American Express to participate in this program.

Phase II

Included the following changes:

- Authorization changes for Split Dial merchants who authorize with American Express and settles with FDGS.
- Settlement changes
 - American Express is adding support for Auto Rental Addendum record.
 - **Required fields include:** Rental Agreement #, Pick-up City Name, Pick-up Region Code, Pick-up Country Code, Pick-up Date, Return City Name, Return Region Code, Return Country Code, Return Date and Renter Name

- American Express is adding support for Corporate Purchase Card Level 2 Addendum record.
 - **Required fields include:** Ship-To-Postal-Code and Total Tax Amount
- Gas/Oil merchants may continue to submit transactions using their petroleum specification, but FDCS will have to transmit the settlement for these transactions as retail transactions to American Express per American Express requirements.
- Transactions from the following US Territories must be sent to American Express under the CAPN format:

Need to pass valid data at authorization and settlement for POS Data Codes and Transaction Identifier fields.

- American Samoa
- Federated Status of Micronesia
- Guam
- Marshall Islands
- Northern Mariana Islands
- Palau
- Puerto Rico
- Virgin Islands (US)

If the above data is not received, or is incorrect, noncompliance fees are applicable.

Fine schedules

Noncompliance Transaction Fee			
Actual/Estimated Annual American Express Charge Volume	Average Transaction < \$50	Average Transaction \$50–\$250	Average Transaction > \$250
\$10MM – \$100MM+	\$0.10	\$0.25	\$0.50
\$10K – \$10MM	\$0.15	\$0.50	\$1.00

Previous notifications

This information was communicated on the following previous dates listed below and may be accessed by going to http://www.firstdata.com/support/global_partner_management .

- 1st notice – 9/12/2006
- 2nd notice – 5/14/2007
- 3rd notice – 6/8/2007

Section 4: PCI DSS Compliance Requirements

Overview

On November 7, 2007, the Payment Card Industry (PCI) Security Standards Council (SSC) adopted Visa's Payment Application Best Practices (PABP), and in April 2008 it released it as the Payment Application Data Security Standard (PA-DSS).

- The PA-DSS supports the PCI Data Security Standard (DSS) and reinforces that payment applications must not store sensitive cardholder data. The PCI SSC is an open standards body that similarly manages the PCI DSS and PCI PIN Entry Device (PED) Security Requirements.
- With the release of the PA-DSS, the PCI SSC now provides a global set of security requirements supported by all five global payment card brands.

Using validated payment applications does not alone guarantee or ensure compliance with PCI DSS. Acquirers have an obligation to perform their own evaluation and due diligence to ensure the overall PCI DSS compliance of their merchants and agents.

Merchants and agents must implement payment applications in a manner that will meet their requirements for performance and functionality, free from errors or malicious code, and will be compatible with any other systems or applications. It is critical that merchants and agents work with their payment application vendors to ensure secure deployment, implementation, configuration, troubleshooting and maintenance in compliance with the PCI DSS.

Transition from PABP to PA-DSS

As part of the transition from PABP to PA-DSS, the PCI SSC has established a transition process to "grandfather in" payment applications that have been validated or are currently being validated against PABP.

- These payment applications will be listed at the PCI SSC's Web site and will include an expiration date by which the application must be revalidated under PA-DSS.
- Payment applications that requested a review under PABP must have been submitted to Visa by September 30, 2008, to be transitioned to the PCI SSC list.
- **If PABP validation was not completed by September 30, 2008, the application would have to undergo the PCI SSC's PABP to PA-DSS Transition Procedures in order to be listed.**

Visa is committed to working with the PCI SSC to ensure a successful transition of PABP to PA-DSS. For more information on the PA-DSS requirements or the transition process, please refer to the Frequently Asked Questions section of the PCI SSC's Web site at www.pcisecuritystandards.org. For a list of qualified security assessors (QSA), please visit: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Vulnerable Payment Applications

On January 1, 2008, Visa implemented a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system in the U.S. These mandates require acquirers to ensure their merchants and agents do not use payment applications known to retain sensitive cardholder data elements and require the use of payment applications that adhere to PABP, now PA-DSS. Accordingly, **as of January 1, 2008**, newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications.

By July 1, 2010, acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant payment applications. To mitigate the risk of compromise, acquirers must take prompt action to ensure that merchants and agents discontinue use of vulnerable payment applications and begin moving merchants and agents toward using only PA-DSS compliant payment applications. Visa is currently working toward developing similar mandates in regions outside of the U.S. For more information on Visa's payment application security efforts and the series of compliance mandates, please visit the Payment Applications section at www.visa.com/cisp. First Data has been enforcing the PABP/PA-DSS requirements since 2007.

Section 5: New First Data Products

Please note that you are required to certify using the most current specification version located on www.fdms.com and send in a pre-assigned value in the “TPP ID” field. The TPP ID value will be assigned by Global Partner Management when you submit the certification request. Certification requests will be delayed until these two requirements are met.

American Express® OnePoint Program – Full Service through First Data

Platform Availability: North (Cardnet), Nashville (Envoy), Omaha (targeted for 7/2009)

Merchants can now authorize and settle American Express® transactions through the First Data network when they sign up for the OnePoint program!

First Data is now able to offer merchants the OnePoint (Full Service) program which includes end- to- end servicing for all card types including American Express®. Merchants can now authorize and settle American Express transactions through the First Data network when they have signed up for the OnePoint program. Payment applications must be updated and recertified in order for merchants to take advantage of this exciting new offering.

It's important for us to work together to ensure merchants are set up correctly and that all transactions flow through First Data. If a merchant is set up on the OnePoint program, authorization and settlement information for all card types needs to be sent to First Data. No transaction information is sent to American Express (no split dial).

Why is this important for merchants?

By allowing merchants to authorize and settle American Express transactions directly with First Data, merchants can take advantage of the following benefits:

- One source for all card types
- Merchant receives one ACH for all bankcards
- Faster speed of pay for American Express
- Single statement and consolidated online reporting tool
- One customer service number
- Authorization and settlement is done through First Data
- More payment choices to offer consumers

What do you need to do?

Merchants must be able to authorize and settle American Express transactions through First Data in order to take advantage of the OnePoint Program. Split dialing to American Express is not an option with this program. First Data has enabled the functionality within our network, but we need to make sure you do your part. Here's what you need to do going forward:

- Update your application:
 1. Go to www.fdms.com/specs and download the specifications for either North (Cardnet) or Nashville (Envoy) containing this functionality.
North specifications: EDC, EDC+, ISO Dial, ISO global and PTS
Nashville specifications: VP Term, DL Host
 2. Make application changes.
 3. Send a request to gpm@firstdata.com once you are ready to certify/test the application changes. You'll receive a certification request form for completion.
 4. Once the certification request is submitted, **you will need to perform testing and certification; when complete you will receive** a release letter from First Data's Global Partner Management team and the solution will be ready for production release!
- For American Express merchants, it's important for you to know whether they are Full Service/OnePoint (FDC authorization and settlement) or Passthrough/ESA (FDC authorization and Amex settlement) since this will impact the way the merchant's application is configured.
- All Full Service/one point merchants must be configured so they can authorize and settle American Express transactions with First Data.
- Split dial is not an option for Full Service/OnePoint merchants.

Loyalty Solutions

Functioning in real-time, First Data's Loyalty Solutions platform captures customers' purchasing behavior from the POS. This data helps merchants create customized loyalty campaigns that identify customer purchase patterns enabling merchants to offer appropriate, effective promotions and rewards. These targeted campaigns and promotions help build brand loyalty and promote customer retention as well as increase customer frequency and spend. Customer specific communications and promotions can result in more valuable customer relationships. First Data Loyalty Solutions helps merchants create, expand and manage loyalty programs so marketing campaigns are better-tailored to the most valuable customers, more effective in influencing customer behavior and make a merchant's marketing dollars work harder. First Data's Loyalty Solutions offering is currently available on the Buypass, North and Nashville platforms.

Benefits of Certification

Integrating and certifying to First Data's Loyalty Solutions platform has many benefits:

- Increase and Diversify Revenue – First Data offers revenue sharing opportunities as well as custom development revenue from clients and partners.
- Improve Your Value Proposition – Adding First Data's Loyalty Solutions capabilities to your POS increases the value you bring to your merchants, whether you're augmenting existing loyalty capabilities or offering loyalty for the first time.
- Customer Satisfaction – Merchants are demanding flexible, real-time loyalty solutions. The more options and flexibility you provide, the more compelling your POS solution.

For more information visit http://www.firstdata.com/product_solutions/loyalty_solutions/merchant_solution.htm.

Mobile Commerce GO-Tag™ Solution

First Data's Mobile commerce solutions help meet consumer demand for choice, convenience, security and rewards by facilitating financial activity via a mobile device over a wireless telecommunications network. The GO-Tag™ solution from First Data leverages contactless technology to help make transactions fast, secure and convenient. They allow consumers to use a specially designed form factor to facilitate a prepaid payment rather than using cash, credit cards or debit cards, and without carrying a wallet or purse.

How It Works

The GO-Tag sticker can be adhered to a customer's personal item - cell phone, employee badge or MP3 player. After purchasing the GO-Tag form factor, the consumer then pays for their purchase by simply waving or tapping the GO-Tag form factor in front of a contactless reader at the point-of-sale (POS). Beyond the terminal, the secure transaction uses the existing gift card processing infrastructure. Though the end result is the same as if a cashier had swiped a card, this technology makes the purchasing experience more convenient and rewarding for the consumer.

Help Your Customers:

- Check out quickly and conveniently
- Improve security since the payment device never leaves their hands
- Enjoy the convenience of not dealing with cash in a unique point-of-sale experience
- Expand their choice in payment options outside their traditional wallet

Merchant Benefits:

- Generate more brand awareness
- Drive customer loyalty
- Establish a competitive difference
- Increase number of transactions per day, prepaid card reloads, and usage of contactless readers
- Improve operational efficiency
- Create readiness for mobile commerce

For more information, visit

http://www.firstdata.com/product_solutions/mobile_commerce_solutions/index.htm

Resources

The following resources are available to support First Data's valued third party integrator community.

Global Partner Management Team

The Global Partner Management (GPM) team provides end-to-end business support to all third party POS payment application providers and third party processors/payment gateways. Please contact one of the following team members for assistance:

- **POS Payment Application Providers – Rodney Slone**
Rodney.slone@firstdata.com or 770-218-4066
- **Third Party Processors/Gateways – Cheryl Ellmore**
Cheryl.ellmore@firstdata.com or 240-313-1027
- **General GPM Operational Support – Debbie Kallage**
Debbie.kallage@firstdata.com or 303-967-5429
- **Escalations – Jana Franks**
jana.franks@firstdata.com or 303-967-8671

First Data Business Requirements

- **POS Payment Application Providers**
 - Provide proof of PABP/PA-DSS validation prior to certification completion
 - Pass TPP ID field to First Data in authorization message (unique identifier)
 - Certify to the most current specification version
 - Certification requests will be submitted by GPM to certification teams
 - GPM will provide release letters to POS Payment Application Providers
- **Third Party Processors/Gateways**
 - Must complete business "due diligence" requirements prior to beginning certification
 - TPP Agreement
 - Credit/Risk Approval
 - Association/Bank Registrations
 - Proof of PCI-DSS Compliance (Service Provider status)
 - Pass TPP ID field to First Data in authorization message (unique identifier)
 - Certify to the most current specification version
 - Certification requests will be submitted by GPM to certification teams
 - GPM will provide release letters to Third Party Processors

First Data Specification Website

For access to the most current First Data specifications, please visit www.fdms.com/specs. Please note that certifications to outdated specifications or certifications that do not include the TPP ID field will not be permitted.

Production/Platform Support

For production support, please contact the appropriate help desk below and open an incident report (IR).

North (Cardnet): 800-555-9966

Nashville: 800-555-9966

South: 800-555-9966

Omaha: 800-337-1222

Buypass: 800-827-4396

Qualified Security Assessors (QSAs)

For a list of qualified security assessors (QSA), please visit: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
Preferred pricing is available for all First Data integrators through IGX Global. Please contact Geoff Nicholas (201-618-9882) for more information or go to www.igxglobal.com.

© 2009 First Data Corporation. All Rights Reserved. All trademarks, service marks and trade names referenced in this material are the property of their respective owners. The information contained herein is provided as a courtesy and is for general informational purposes only. This information is not intended to be a complete description of all applicable policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. This information may include, among other things, a compilation of documents received from third parties. It should not be used as a substitute for reference to, as applicable, association releases, bulletins, regulations, rules and other official documents. First Data shall not be responsible for any inaccurate or incomplete information. This bulletin may not be copied, reproduced or distributed in any manner whatsoever without the express written consent of First Data Corporation.