First Data’s Program on EMV™

Independent Software Vendors
November 2014

EMV™ is a trademark owned by EMVCo LLC.
Agenda

• EMV™
  • Overview & Background
  • Processing
  • Certification

• EMV Complementary Products
  • Rapid Connect®
  • TransArmor®
  • STAR® RapidFlash
  • GlobalChoice™ – International Currency Solutions
  • Apple Pay™

• Summary & Questions
What is EMV™?

- EMV – micro-chip payment standard created by Europay®, MasterCard®, Visa® over 10 years ago and has been implemented globally

- EMVCo – organization owned by the global brands that manages the standard for global inter-operability

- EMV payment cards improve security over magnetic stripe technology through an embedded computer chip
  - Card validation ensures the card is legitimate
  - Cardholder authentication reduces fraud from lost and stolen cards
How EMV™ works

Payment Card is...

1. Inserted into chip-enabled slot reader (contact)

   OR

2. Waved above the device (contactless)

• Data on the chip ensures the card is **authentic**
  • Blocks the ability to copy the contents of the chip to another card
  • Prevents the use of skimmed or counterfeit cards

• PIN or signature ensures that the person presenting the card is the **rightful cardholder**
  • PIN applies to Credit & Debit cards
EMV™ card and terminal adoption

The U.S. is the last member of top 20 world economies to commit to a domestic or cross-border liability shift associated with chip payments.

Contact EMV Global Adoption*

*Figures reported as of Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States. Figures are reported by region and do not imply country-by-country statistics.
EMV™: Recent U.S. history

- **2011**: global payments brands introduced roadmaps for EMV technology and encouraged its adoption
- **April 2013**: first domestic milestone required processors like First Data to accept EMV–based payments from merchants
- **4Q 2013**: Retailer data breaches occur
- **1Q 2014**: First Data reaches agreement with Visa & MasterCard to utilize U.S. Common Debit AID
- **October 2015**: next milestone - fraud liability shift to all point-of-sale devices (except Automated Fuel Dispensers Oct. 2017) will take effect
  - Liability for counterfeit fraud transactions shifts from financial institution to merchant if the merchant does not accept EMV transactions

---

43.7%
Of total worldwide payment card fraud losses were from the US, however only generated 23.5% of total volume.¹

$580.5 million
Total debit card fraud losses incurred by retailers. Spend $6.47 billion annually on credit and debit card fraud prevention annually.¹

59%
Of the more than 37 billion debit card transactions that were made were verified by signature, 85% of all fraudulent debit card transactions involved signature verification and $1.15 billion of the total $1.35 billion in debit card fraud losses (85%) stemmed from signature based debit card transactions.²

$8.6 billion
Estimated total cost of fraud per year in the United States (0.4% of the $2.1 trillion card payment industry)

32%
Lost/Stolen, Counterfeit & Non-receipt fraud account for 32% of 2008 US fraud losses, representing approximately $2.9 billion

95%
EMV deployment in the US is estimated to eliminate 95% of lost/stolen fraud

90%
An estimated 90% of counterfeit card fraud could be eliminated with EMV deployment in the US

¹Nilson Report, August 2013
²Payments Journal, February 2012

**Source:** Alte Group, "Card Fraud in the United States" – The Case for Encryption, January 13, 2010
The Marketplace at the end of 2015

- The U.S. is set to transition more than 1.2 billion payment cards and 8 million point-of-sale (POS) terminals to meet the requirements for EMV smart card payments to be ubiquitous.

- Physical EMV hardware (cards and POS terminals) will cost issuers and merchants more than $6.8 billion in the U.S.

- It is forecast that more than 575 million EMV chip-enabled payment cards will be in circulation in the U.S. (48% of the total 1.2B)

- More than 50% of U.S. retail locations are projected to be EMV-capable.

- The long tail of EMV migration will be small and micro businesses.

- The EMV transition will help fix an important loophole in card fraud: counterfeiting.
  - However, based on experiences in other markets, card fraud is expected to migrate to the point of least resistance: the card-not-present environment.
Liability implications of EMV™

• In U.S. today:
  • Fraud in card-present environments is absorbed by Bank/Issuer unless merchant fails to meet POS acceptance and dispute resolution requirements
  • Losses are offset when dispute resolution requirements allow liability to be shifted through “chargeback process” to Acquirer/Merchant
  • Merchant/Acquirer takes liability for merchant data breaches or skimming attacks

• In 2015 with EMV:

<table>
<thead>
<tr>
<th>Visa</th>
<th>MasterCard Liability Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit fraud losses “shift” to party who does not enable EMV if fraud would have been avoided if EMV had been used</td>
<td>Party that cannot support a lower-risk option holds the liability. Equal capabilities = issuer holds liability.</td>
</tr>
<tr>
<td>Issued Device/Card</td>
<td>Acceptance Terminal</td>
</tr>
<tr>
<td>Magnetic stripe and contactless magnetic stripe</td>
<td>Magnetic stripe and/or contactless magnetic stripe</td>
</tr>
<tr>
<td>EMV contact or EMV contactless (signature CVM)</td>
<td>EMV contact or EMV contactless (not PIN capable)</td>
</tr>
<tr>
<td>EMV contact or EMV contactless (online or offline PIN CVM)</td>
<td>EMV contact or EMV contactless (online or offline PIN capable)</td>
</tr>
</tbody>
</table>

Note: Above interpretation based on Visa and MasterCard requirements. Issuers should review this internally.
## Why implement EMV™?

### Financial Institutions

**Reduce fraud**
- Potential to reduce POS counterfeit fraud losses with use of chip
- Shift fraud liability to merchants that do not support EMV

**Improve market perception**
- Demonstrate to customers and market that cardholder security is important
- Poor brand perception by cardholder if their issuer is last to implement EMV

**Avoid increased exposure to cybercriminals**
- Late adopters will be the weakest link for cybercriminals – they will find the path of least resistance to identify weakness
- As the market of non-chip card dwindles, the criminals will target non-chip cards

### Merchants

**Increase security at the POS**
- A primary way cybercriminals use stolen credentials is to create a false card to impersonate the actual card
- Historically, as cybercriminals recognize EMV implementation is underway, they increase activity

**Reduce liability costs**
- The global card brands have announced a Liability shift for Oct 2015
- In 2015, if the merchant does not support EMV, that liability will shift to the merchant

**Avoid increased exposure to cybercriminals**
- Criminals will find the path of least resistance through late adopters to identify weakness
- As the population of non-EMV locations dwindles, the criminals will concentrate on non EMV-locations
The First Data Approach

Multi-layered Security & Compliance

**COMPLIANCE**
A step-by-step, self-guided approach to help small and mid-size merchants complete the SAQ

**FRAUD PREVENTION**
Fraud reduction technology that can help protect against losses from accepting counterfeit and lost or stolen payment cards at the point-of-sale

**DATA SECURITY**
Powerful payment card security that combines encryption with random number tokenization

**PROTECTION**
Value added services for Level 4 merchants to increase data security, protect against fraud, and provide coverage in the event of a data breach.

First Data can provide you with the tools to help protect your customer’s data from cyber criminals.

EMVTM is a trademark owned by EMVCo LLC.
EMV™ & Data Security – How do they relate?

Multi-layered security solution

- Advances in technology has increased cyber attacks
  - Data in motion (e.g., with memory-scrapers)
  - Data at rest (e.g., from a database)

- Stolen data used to produce
  - Counterfeit cards
  - Fraudulent online transactions

Focusing on only one or two points of entry can still leave vulnerabilities

<table>
<thead>
<tr>
<th>Security Needs</th>
<th>First Data Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV</td>
<td>Protecting Data Against Card Counterfeiting</td>
</tr>
<tr>
<td></td>
<td>EMV Chip-based technology reducing the risk of accepting counterfeit cards. PIN reducing the risk of misuse of lost or stolen cards.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Protecting Data in Transit</td>
</tr>
<tr>
<td></td>
<td>Encryption Protecting cardholder data in motion from the swipe of the card until it reaches our secured processors.</td>
</tr>
<tr>
<td>Tokenization</td>
<td>Protecting Data at Rest</td>
</tr>
<tr>
<td></td>
<td>Tokenization Making it impossible to steal data at rest from merchant servers or POS, while reducing the cost and complexity of compliance.</td>
</tr>
</tbody>
</table>
First Data’s EMV™ capabilities

Current EMV capabilities

• First Data is producing EMV-enabled credit cards and processing EMV credit transactions TODAY

• First Data has been processing real-time EMV transactions with the largest retailer for more than 3 years

• First Data processed more than 10 million U.S.-based merchant EMV transactions in 2013

• Currently, First Data’s issuing business processes more than one million EMV transactions a month

• First Data has issued more than 10 million EMV cards
First Data EMV™ Processing

A deeper dive into EMV
Magnetic Stripe Transaction Processing

- Terminal performs little or no risk assessment
- Magnetic stripe cards are easy to counterfeit
- Track Data is often in clear
- The Auth data is static
- Risk assessment is performed at the host
- Static data limits identification of counterfeit cards

• Magnetic stripe cards are easy to counterfeit
EMV™ Transaction Processing…the new Normal

- Dynamic Auth data
- Terminal and EMV Chip perform risk assessment
- Dynamic cryptogram validation
- May return an authentication cryptogram
- Post issuance updates

Start

End

Acquirer

Payment Network

EMV Data

ARPC

Bank

EMV Data

ARPC

Member Bank

The Card is King!
Cardholder Verification Methods (CVM)

- Cardholder Verification Methods indicate the priority order of how the cardholder may be validated in the field – not just one way
  - PIN (online and offline), Signature and No Cardholder Verification Required (No CVM) supported
    - Online PIN is encrypted by the PINpad and sent online to the Issuer host for validation
    - Offline PIN is sent to and validated by the chip; Offline is never sent to the host – only the result is passed
- Negotiation between the card and terminal determines which CVM to use
Application Identifiers (AID)

Global AID v. U.S. Common Debit AID

• EMV transactions utilize AIDs to determine how or where a transaction should be routed
  • If Global AID is used, transaction must be routed to the one corresponding network only
  • If U.S. Common Debit AID is used, transaction may be routed via unaffiliated networks

![Diagram showing 1 to 1 Relationship](image1)

![Diagram showing 1 to Many Relationship](image2)

• Visa and MasterCard introduced “U.S. Common Debit AIDs” to support Durbin regulations* to route debit/prepaid transactions to unaffiliated networks
  • Debit Network Alliance (DNA) and other individual debit networks may also offer U.S. Debit AIDs that will only reside on non-Visa and non-MasterCard branded debit cards

*Durbin amendment to the Dodd–Frank Wall Street Reform and Consumer Protection Act
U.S. Common Debit AID Best Practices

• Select U.S. Common Debit AIDs when present
  • Recommend that the Global AIDs be removed from the Candidate List when both U.S. Common Debit and Global AIDs present for the same funding account; this provides maximum flexibility in debit routing options

• Send all Debit transactions as dual message
  • Recommend that all transactions be sent as dual message, even for PIN Debit transactions, which enables maximum flexibility in routing options
Transaction Processing

• Total Transaction Amount Must be known before Card is Presented
  • EMV POS Solutions must complete tendering process before prompting for card entry
  • Cashback amount must be included in the total transaction amount

• Processing begins with 1st Generate AC process which has two steps
  • Terminal Action Analysis – performed by the device kernel to request the Generate AC
  • Card Action Analysis – performed by the card and results in the Generate AC response

• Processing of an Online authorization are finalized during 2nd Gen AC process
  • All Full EMV transactions (ex. Purchase) sent for online authorization must still have the card finalize the Issuer authorization decision whether approved or declined
    • Transaction may be approved or declined
    • If approved online and declined during 2nd Gen AC, a reversal must be sent to Issuer host
Terminal Action Analysis – Step 1 (1st Gen AC)

• Kernel analyzes the IAC, TAC and TVR values and sends “Generate AC” command requesting card to return its offline authorization decision

• This 1st Generate AC command must:
  1. Specify whether a CDA signature is requested
  2. Indicate type of Application Cryptogram being requested based on the kernel’s preliminary authorization decision:
     • **AAC** – Decline transaction – generally used to terminate chip interaction for Partial EMV transactions (ex. credit Refund where only the card number is needed)
     • **ARQC** – Process transaction online *(recommended by First Data)*
     • **TC** – Approve the transaction offline
  3. Provide transaction data required by card to perform Card Risk Management
  4. Provide transaction data required to calculate Application Cryptogram

Could you please approve this transaction online? Here’s my ARQC.
Card Action Analysis – Step 2 (1st Gen AC)

• EMV card performs Card Action Analysis including evaluating Card Risk Management results and responds with the appropriate cryptogram based on the 1st Generate AC request
  • AAC (Decline) Requested – card must respond with:
    • AAC – Declined
  • ARQC (Online authorization) Requested – card may respond with either:
    • ARQC – Go Online (online issuer authorization required)
    • AAC – Declined
  • TC (Offline approval) Requested – card may respond with any of the following:
    • TC – Approved
    • ARQC – Online Authorization Required
    • AAC – Declined

Could you please approve this transaction online? Here’s my ARQC.

Absolutely! Here’s your ARQC.
Online v. Offline Approval

- Authorizations may be obtained from the Issuer either Online or Offline
  - Online authorizations are recommended, however Offline authorizations are supported
- Transactions must always go to card first for authorization decision (1st Gen AC)
  - Approve the transaction (Offline approval)
  - Decline the transaction (Offline decline)
  - Request the transaction be sent to the Issuer host for authorization (Online authorization required)
- EMV Offline Authorizations are Issuer approvals and as binding as Online approvals
  - Merchant stand-in may still be utilized and Merchant accepts ALL risk
Key Requirements

- **EMV Test Tool is Required for Card Brand Certification**
  - First Data requires use of an approved EMV Test Tool to perform Card Brand Certification; **First Data requires use of the Collis Brand Test tool**

- **Total Transaction Amount Must be known before Card is Presented**
  - All EMV POS Solutions must complete tendering process before prompting for card entry
  - Cashback amount must be included in the total transaction amount

- **Service Code ‘2xx’ and ‘6xx’ Must force Chip Usage**
  - If Service Code ‘2xx’ or ‘6xx’ is read in mag stripe (indicating that a chip is present), EMV POS Solution must prompt to insert card into chip reader

- **AID List Must be Loaded into Kernel at Kernel Initialization**
  - All AIDs supported by the EMV POS Solution must be loaded into the kernel at kernel initialization for use during Application Selection

- **CVM selected Must be Printed on Receipt**
  - Cardholder Verification Method must be printed on receipt; “Verified by PIN” must be printed for PIN transactions and a signature line must be printed for signature transactions
Key Best Practices

• Select U.S. Common Debit AIDs when Present
  • Recommended that the Global AIDs be removed from the Candidate List when both U.S. Common Debit and Global AIDs are present for same funding account; Common Debit AIDs provide maximum flexibility in debit routing options

• Use “No PIN” / “PIN” rather than “Credit” / “Debit” when Prompting
  • Recommended when using Cardholder Selection method that cardholder prompts displayed are “No PIN” / “PIN” rather than traditional “Credit” / “Debit” prompts

• All CVMs should be Supported
  • Recommended that all CVMs (Online PIN, Offline Plaintext PIN, Offline Enciphered PIN, Signature and NO CVM) be supported for attended solutions

• Do Not Print Receipt until the Card has been Removed
  • Recommended that EMV POS Solution does not print receipt until cardholder has removed the card, which will decrease instances of cards being left behind

• Sound Audible Beep while Waiting for Card to be Removed
  • Recommended that EMV POS Solution sound an audible beep until card is removed to decrease instances of cards being left behind
Frequently Used Acronyms

Complete listing of acronyms and terms with full definitions can be found in the Implementation Guide on the First Data Specifications website: https://specs.firstdata.com/kb/371/

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC</td>
<td>Application Authentication Cryptogram</td>
</tr>
<tr>
<td>AID</td>
<td>Application Identifier</td>
</tr>
<tr>
<td>ARC</td>
<td>Authorization Response Code</td>
</tr>
<tr>
<td>ARPC</td>
<td>Authorization Response Cryptogram</td>
</tr>
<tr>
<td>ARQC</td>
<td>Authorization Request Cryptogram</td>
</tr>
<tr>
<td>ATC</td>
<td>Application Transaction Counter</td>
</tr>
<tr>
<td>CAM</td>
<td>Card Authentication Method</td>
</tr>
<tr>
<td>CDA</td>
<td>Combined Dynamic Data Authentication</td>
</tr>
<tr>
<td>CVM</td>
<td>Cardholder Verification Method</td>
</tr>
<tr>
<td>DDA</td>
<td>Dynamic Data Authentication</td>
</tr>
<tr>
<td>IAC</td>
<td>Issuer Action Codes</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Chip Card</td>
</tr>
<tr>
<td>SDA</td>
<td>Static Data Authentication</td>
</tr>
<tr>
<td>SVC</td>
<td>Service Code</td>
</tr>
<tr>
<td>TAC</td>
<td>Terminal Action Code</td>
</tr>
<tr>
<td>TC</td>
<td>Transaction Certificate</td>
</tr>
<tr>
<td>TVR</td>
<td>Terminal Verification Result</td>
</tr>
</tbody>
</table>
EMV™ Certification

Planning for a smooth implementation
EMV Certification – 3 Levels

Each combination of Hardware, Kernel and Payment Application is one certification

- **Level 1 (L1) – Hardware Certification** – Completed by the terminal vendor (Ingenico, Verifone, etc)
  - Approved devices listed on EMVCO.com
  - EMV Level 1 terminal type approval verifies that the terminal chip reader demonstrates sufficient conformance to Level 1 of the EMV mechanical and electrical protocol specifications covering the transfer of data between the terminal and the card

- **Level 2 (L2) – Kernel Certification** – Completed by the terminal vendor
  - Approved devices listed on EMVCO.com.
  - EMV Level 2 terminal type approval verifies that the software residing in the acceptance terminal performing the EMV processing demonstrates sufficient conformance to the EMV specifications
  - EMV defines the EMV Level 2 kernel as the terminal application software that supports the EMV payment application functions as defined in the EMV specifications
  - The non-EMV application functionality that supports functions like the printer and display, and building messages to send to the acquirer is not considered part of the kernel

- **Level 3 (L3) – Payment Application Certification** – Completed by First Data and ISV
  - Approved applications listed on FirstData.com
  - Certifies entire application stream with the Card Brands
Requirements for Certification

- **EMV Enabled Device**
  - Level 1 and Level 2 certification required from EMVCo.
  - Certified devices are listed on [www.emvco.com](http://www.emvco.com)

- **EMV Test Tool**
  - EMV card simulator must be purchased from an Association-approved provider
  - First Data requires use of the Collis Brand Test Tool

- **Association Certifications**
  - Certifications to Visa, MasterCard, American Express and Discover are required

- **Certification Slotting**
  - First Data Certification Analysts must be assigned to each certification
  - [Work with your assigned Product Manager to schedule an available time slot to complete your certification](http://www.emvco.com/approvals.aspx?id=83)
Support of Online PIN for Credit and Common Debit AID

• Coding can Begin Now!
  • Updated specifications available in November 2014 will define a new response value and support regional debit networks (STAR, NYCE, etc.) for U.S. Common Debit AID
  • Register on the First Data specifications website (https://specs.firstdata.com) to be notified when the new specifications are released
  • Regional debit networks will be available for testing in late February 2015 and available in production in early March 2015

• First Data recommendation:
  • Complete coding for complementary products then proceed with EMV coding and testing
  • Wait until late Q1 or early Q2 to finalize certification and move into production
  • Enables implementation of all EMV functionality with only one certification event
  • Final decision is up to you on how you wish to proceed with your unique project requirements
Development and Certification Process

- Estimated 4-5 month Duration for EMV Certification
  - Complete description of phases and tasks can be found in the Implementation Guide on the First Data Specifications website: https://specs.firstdata.com/kb/371/
EMV™ and First Data Products

Helping make the transition easier and more secure
Rapid Connect®

Certification portal for EMV™
How can First Data Help you with Your EMV™ Planning?

- Businesses in card present environments that need to accept EMV cards need greater support now from their service providers.

- First Data has significantly invested in the development of Rapid Connect® to simplify the way developers can certify for EMV and our TransArmor® encryption and tokenization solution.

- Rapid Connect greatly eliminates multiple integrations developers have with our various authorization and settlement platforms.

  Consolidating multiple integrations equals time and money savings, and reduces EMV complexity!
Introducing the Rapid Connect® Solution

• Radically simplified integration and certification: Single ‘spec’ that works across multiple First Data platforms; opportunity to consolidate First Data interfaces which reduces EMV Certifications and costs

• Developer portal, SDK/toolkits & sandbox: Quickly and easily integrate a wide variety of payments services into any software application

• Intelligent online test environment: Automated diagnostic tools recognize and remedy failure points, speeds up code review and significantly decrease certification time

• Dedicated, readily-available support: Easy-to-access tools, guidelines, requirements and specialized consultation resources

• Easy access to innovative payment technologies: Rapid delivery of new First Data products, features, and programs; save time and resources to enable the latest in payment innovations
Rapid Connect® drives commerce…
The single point of integration for multiple payments, industries, platforms, everywhere.

Developer Benefits
• Smart developer portal that offers quick and easy integration to a wide variety of payments and services
• Single XML spec provides easy access to the latest payment technologies
• Dedicated support to expedite the development and integration process
• Faster certification with self-testing and automated diagnostic tools
• ‘Hands on’ guidance from a global payments leader with EMV expertise

Merchant Benefits
• Faster access to new technologies
• Create new loyal customers - TransArmor, Value Added Services
• Single payment Provider with Global reach
• Specialized Support

** some features may only be available via certain platforms/configurations

EMV™ is a trademark owned by EMVCo LLC.

© 2014 First Data Corporation. All Rights Reserved.
TransArmor® Data Protection

E2EE + Tokenization
TransArmor Data Protection – What is it?
E2EE + Tokenization – A brief overview

TransArmor: A dual-layered payment card security solution combining encryption + tokenization technology that removes sensitive payment card data from the merchant environment, to reduce the threat and liability associated with a data breach.

EMV with TransArmor Data Protection – Why do I need it?
EMV+E2EE+Tokenization – Multi-layered Security

• EMV along with the added security layers of TransArmor end-to-end encryption and tokenization provide the multi-layered security that is necessary in today’s card environment.

• Many of our mutual clients have shown, and continue to show interest in having TransArmor as part of their security solution – specifically within their ISV POS solutions.

• Save heavily on development costs and time, while providing bleeding edge security to your customers. Adding TransArmor at a later date would require recertification of EMV adding unwanted costs and time.
TransArmor Data Protection

E2EE + Tokenization

**Encryption Types** - *Protecting Data in Motion*

**RSA/Public Key Infrastructure (PKI):** The RSA algorithm uses asymmetric encryption with two keys - a Public key & Private key
  - Uses the RSA 2048-bit algorithm, and Encrypted data does not resemble original data

**TransArmor Verifone Edition (TAVE):** A symmetric encryption installed at the hardware level to perform format-preserving encryption using the VAES algorithm
  - Encrypts sensitive cardholder data so that the output is in the same length and character set as the input

**Token Types** – *Protecting Data at Rest*

**TransArmor Tokens (Single-Use)**
  - Generated at the RSA SafeProxy within FD’s PCI secure environment and returned with the transaction’s authorization to the merchant. Cannot be used to initiate a financial transaction without the card being present

**TransArmor Multi-Pay Token (Multi-Use)**
  - Same characteristics as a TransArmor Token with additional features, making Multi-Pay Tokens valuable for both POS and eCommerce/Card Not Present environments. Unlike traditional tokens, Multi-Pay Tokens can be used to initiate a financial transaction without the card being present
  - A TransArmor Multi-Pay Token can be safely stored in the merchant environment in lieu of the customer’s account data
STAR® “RapidFlash”
STAR® “RapidFlash”

What is STAR “RapidFlash” (PINless) Debit?

• First Data is enabling support for PINless POS transactions on STAR and other PIN Debit Networks
• A convenient new, no PIN required payment solution targeted at certain merchant categories
  • POS PINless is a new offering from the Debit Networks as an alternative to transactions that are accepted currently without a signature
• Merchants understand the benefits of No CVM payments and desire routing choice
  • Cardholder convenience – no confusion as to selecting “debit”, “credit”, “PIN” or “signature” – just a swipe!
• Regulations allow merchants greater control over their debit transaction routing, PIN and PINless
  • Durbin Amendment removed network routing rules, promoting competition among networks and choice for merchants
  • PINless Debit is integrated into First Data’s Smart Routing Product to enable routing choice/priority
GlobalChoice™

Dynamic Currency Conversion

Dynamic Pricing
Dynamic Currency Conversion & Dynamic Pricing

Solutions that allow merchants to provide their international customers with an “in-country” online shopping experience

• **Dynamic Currency Conversion (DCC):** an innovative credit card processing solution that enables merchants to offer their international customers the choice to pay in their own currency or in U.S. dollars (USD)

• **Dynamic Pricing:** A solution that combines the revenue benefits of Dynamic Currency Conversion with an “in country” shopping experience.
DCC Overview

• Dynamic Currency Conversion offers merchants the ability to offer a choice to international customers to pay in the currency of their credit card. Our solution fully protects the merchant and cardholder from currency fluctuation. Over 80 currencies supported.

• Redirects the current revenue stream enjoyed by Visa®, MasterCard® and issuing banks to the merchant, acquirer and our treasury provider FEXCO.

<table>
<thead>
<tr>
<th>Value Shifts to the Merchant</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Without</strong>: Currency Conversion Fees Flow to:</td>
</tr>
<tr>
<td><strong>With</strong>: Currency Conversion Fees Flow to:</td>
</tr>
</tbody>
</table>

Card Association & Issuer

Merchant & Partners
Benefits for The Market

**Merchant Benefits:**

- Earn additional income on credit card transactions from foreign customers.
- Offsets existing association fees directly associated with accepting International credit cards.
- Eliminates exposure to foreign exchange rate risk.
- Increases customer service by giving consumers a custom purchase experience.
- Allows merchants to attract new customers and win business over competitors.

**Consumer Benefits:**

- Allows foreign customers to pay for or shop and pay for goods and services in their local currency
- Elimination (in most cases) of International Transaction Fee imposed by issuer.
- Full customer disclosure of exchange rates and fees
- Informs customers of the exact purchase price in a familiar currency.
- No hidden fees or charges.
- Ability to make an educated and informed decision – CHOICE
- Better shopping and payment experience

**ISV Benefits:**

- Major competitive differentiator
- Compete effectively on RFP’s and RFI’s
- Provide clients the ability to offset cost of EMV, Security and other needs.
- Client “Stickiness” - customization
- Retain and secure merchants for long term.
- Provide clients with a service they all want.
- Help clients expand their business.
- Increase volumes.
Product Highlights

- Leadership and Experts in DCC acknowledged by Visa, MasterCard and MAG.
- DCC solutions are fully certified by card associations.
- Our DCC is integrated and live at more than 18,000 merchant locations in the U.S.
- Deep understanding of Property Management Systems and well poised to provide more DCC support to the Hospitality market more than any other provider.
- Deep understanding of Point of Sale Systems and well poised to provide more DCC support to the Retail market more than any other provider.
- Support the largest number of DCC currencies for the U.S.
- We are the leading experts in implementing DCC at merchants using complex and integrated systems.
- We are the largest provider of DCC in the United States processing over $1.4 Billion in DCC transaction volume in 2013.
- Our portfolio has the largest and most recognizable DCC portfolio in the United States.
- Our DCC team has experience in implementing DCC across multiple locations with multiple POS lanes.
- DCC team physically located in the United States providing full operational, production, compliance, project management, product management and integration support.
Apple Pay™
Apple Pay™

• Highlights of the First Data – Apple Pay™ solution for iPhone® 6 and Apple Watch™:
  • First Data brings safety and security to these mobile, online and point-of-sale transactions.
  • First Data’s STAR® Network is one of the first PIN debit networks to provide a Token Exchange Service that accepts Apple Pay transactions. It supports Durbin Compliance.
  • First Data supports merchants with secure, contactless acceptance at the point of sale via Near Field Communication (NFC) technology. Merchants can use contactless-enabled devices from First Data or from their current device reader provider.
  • To enable your solution to accept payments within the apps on the iPhone® 6, simply certify with First Data for In App payment support.
  • To enable your solution to take Apple Pay card present transactions via NFC, simply certify for contactless payments. First Data’s contactless payment infrastructure supports Apple Pay card present tokenized transactions.

Apple®, iPhone®, Apple Watch™ and Apple Pay™ software are registered trademarks of Apple, Inc.
Summary & Questions
Next Steps…

• If you have not already, contact your Global Partner Management Product Manager or gpm@firstdata.com to discuss your EMV certification timeline and any of First Data’s solutions presented today
• Plan at least 4-5 months in your timeline for EMV certification
• Reserve a certification start time in advance…the schedule is filling fast
• If you have not already, visit www.RapidConnect.com to sign up for our certification portal
• For additional EMV resource information, you can visit www.FirstData.com/emv/