EMV 101 for Issuers
Agenda

- Market Update
- What is EMV
- How EMV works
- Product Overviews
- Planning steps
Market Update
Industry Dates

April 2013
Processors must support EMV

April 2015
3rd party ATM must support EMV

October 2015
Liability shift of counterfeit transactions

October 2017
Liability shift for AFD

Less than 300 business days to Counterfeit Fraud Liability Shift
Liability Shift Details

Counterfeit fraud liability is assigned based on hierarchy of which party has most secure option enabled. Standard rules apply when both are equal.

**EMV > Mag stripe**

AFD merchants have extended timeframe in consideration of cost/complexity.
Current EMV State of the Union

- **Debit**
  - US Common AID meets current Reg II requirement
    - Pin Preferring
  - Largest debit networks announced support
    - Jeanie

- **Credit**
  - US Issuing & Retail Industry expected to deploy signature preferring
Current EMV State of the Union

Issuers:
- Vantiv pilot begins August, 2014 with issuers and merchants
- Largest Issuers have issued statements affirming EMV 2014/15 plans
- Anticipate aggressive number of 2014 pilots:
  ‣ Smart Card Alliance EMV Forum (EMF) pilot planned Q4
    • Includes FIs and Merchants
- Utilizing Common US AID for debit ONLY
What is EMV?

**EMV** is a set of international standards that defines *interoperability* of *secure* transactions across the international payments landscape.

- EMV transactions introduce dynamic data specific to the card and the transaction, with the goal of devaluing transaction data in flight and reducing the *risk of counterfeit fraud*.

The computer chip on the card uses *cryptography* to provide strong security. In the context of EMV, *encryption* is only used to protect the PIN.

- EMV is a *card present schema* only.
Market Drivers for EMV

Counterfeit, Lost and Stolen Fraud Losses

• Currently Issuers are liable for all counterfeit fraud-related losses
• When EMV cards are issued, liability for counterfeit fraud will shift to merchant if the merchant is not EMV enabled
• The card brands assign fraud liability based on the least secure party to the transaction

Global interoperability of chip cards and payment devices

• Worldwide standard used by all countries
• Support for international commerce
EMV Benefits

• Chargebacks
  › Have the ability to charge back fraudulent transactions if retailer is not EMV compliant (October 2015)

• Reputational risk mitigation
  › What will customers start to think of cards without chips on them

• Fraud mitigation
  › Limited ability for fraudsters to replicate an EMV card or an EMV transaction
How EMV works
How does EMV work?

- An EMV card is inserted into a terminal.

- The chip embedded in the card contains a unique issuer key; this is accessed by the reader in the terminal.

- Using key from the card and data from the transaction, the chip creates and sends a unique code, or "cryptogram" to the processor’s host with the approval transaction, allowing the issuer to validate the card is legitimate and not counterfeit.

- The card is removed when the transaction is completed.
1. Card is inserted into EMV Terminal
2. First Half of EMV Transaction Protocol
   A. Application Selection
   B. Read Application Data
   C. Offline Data Authentication
   D. Processing Restrictions
   E. Cardholder Verification
   F. Terminal Risk Management
   G. Terminal Action Analysis
   H. Card Action Analysis
3. Online Authorization Request from Card to Terminal
4. Authorization Request from Terminal to Vantiv
5. Authorization Request from Vantiv to Issuer
6. Authorization Response from Issuer to Vantiv
7. Authorization Response from Vantiv to Terminal
8. Completion and script processing. If Issuer approved but card denied transaction a reversal is produced
9. Card is removed from EMV Terminal
What Changes for my Customer?

ATM transactions
Cards will remain in the ATM for the duration of the transaction

POS transactions
Insert card (no more swiping)
Remind customers to not forget their cards

The look of the card
The card looks and act differently

A good customer education program will be needed in order to transition customer smoothly to EMV cards
Understanding the Financial Impact

Fraud Losses

Interchange
Debit Product Overview
# Vantiv EMV Debit Solutions

## Card Procurement and Personalization
- CHIP Selection
- Chip Lifecycle Mgmt
- Profile selection & certification
- Chip procurement & personalization

## ATMs
- Hardware & Software Solutions
- Network Certification assistance
- EMV Enabled Authorizations

## Authorization
- Manage new data elements
- Manage cryptogram validation/response
- Manage EMV risk parameters
- Key Management

## Core Systems
- Manage new data elements in core platforms
- Manage chip and card Procurement

## Communications
- Cardholder communications
- Internal training and messaging
- Issuing strategy
EMV Debit Profiles

<table>
<thead>
<tr>
<th>Form Factor</th>
<th>Auth Mode</th>
<th>Profile(s) Summary</th>
<th>CVM List</th>
<th>Card Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact only</td>
<td>Online Only</td>
<td>Common Debit AID</td>
<td>Online PIN, No CVM</td>
<td>Debit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>International AID</td>
<td>Signature, Online PIN, No CVM</td>
<td></td>
</tr>
</tbody>
</table>

- To meet Durbin routing option compliance, the application selection process changes and two AIDs relate to one funding account.
- Online and Contact Only
- Contactless and Offline not immediately supported
## Certified Debit Profiles

<table>
<thead>
<tr>
<th>BRAND</th>
<th>PROFILE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterCard</td>
<td>MC 20/61 Offline CAM</td>
<td>Offline CAM; US Common; Int - Sig, Online PIN, No CVM</td>
</tr>
<tr>
<td>MasterCard</td>
<td>MC 20/61 Standard</td>
<td>US Common; Int - Sig, Online PIN, No CVM</td>
</tr>
<tr>
<td>MasterCard</td>
<td>MC 19/61 Offline CAM</td>
<td>Offline CAM; US Common; Int – Online PIN, Sig, No CVM</td>
</tr>
<tr>
<td>MasterCard</td>
<td>MC 19/61 Standard</td>
<td>US Common; Int – Online PIN, Sig, No CVM</td>
</tr>
<tr>
<td>Visa</td>
<td>Visa Standard</td>
<td>US Common; Int – Online PIN, Sig, No CVM</td>
</tr>
</tbody>
</table>
EMV Debit Card Product:
Fixed Product Offering, Limited Features

• Utilizes Visa & MC “common US AID” schemas
  › Expect 16 independent networks to sign with both V/MC to license US Common AID
  › Contact Only, No Contactless support initially
  › Online Authorization and Online PIN Only
  › No offline authorization or offline PIN support

• Utilize Oberthur for all card production & personalization
Fraud Monitoring/Parameters

• Standard services to include:
  › Validation of transaction cryptogram
  › Monitoring for duplicate Application Transaction Counters (ATCs)
  › Generation of response cryptogram

• Additional parameters scoped within SAS tool migration
  › Patterns develop over time with increased penetration of cards and terminals in market
Direct Changes

- Some updates are being made to the screens you use in Issuer Direct in order to support the ordering and ongoing management of EMV cards. New fields in the following functions:
  - Open Card
  - Card Inquiry Screen
  - Card Reorder
  - Card Replace
  - Transaction Research
  - Cardholder Research
  - ATM Research
EMV Configuration on Existing Card

**EMV Card Profile Information**

- **Form Factor**: Contact
- **Card configuration**: Contact, Oni-Only, PIN preferring
- **PAN Sequence #**: 000

**Offline Limits**

- **Upper**: N/A
EMV Profile Selection for New Card

EMV Card Profile Information

Form Factor: Contact

Card Configuration: Contact, Onli-Only, PIN preferring
Reports Direct Changes

- The Reports Direct data universes have been updated to include the following EMV related fields for Financial Institutions to create user defined reports. (Vantiv will be adding some Canned EMV related Reports to this tool)
  - EMV Capable Card - Indicates whether or not the card used is an EMV capable card based on the Service Code Indicator.
  - EMV Capable Terminal - Indicates whether or not the terminal acquiring the transaction was EMV capable based on terminal capability flag.
  - EMV Transaction - Indicates whether or not a transaction was an EMV transaction.
  - AID - Application Identifier describes which application generated the transaction.
  - EMV Application Name - The Application Name is the product name that corresponds with the AID field.
  - Issuer Country - The country of the Issuer based on BIN indicators.
Denial Code Changes

- Additional denial codes that would only be seen for EMV related transactions have been added to existing denial list. (Can appear in Transaction/Card Research or on the canned Vantiv Reports.)
  - 254 CRYPTOGRAM ERROR
    - Authentication process of the EMV encryption key between the ATM/POS terminal and Vantiv failed
  - 300 APPLICATION TRANSACTION COUNTER ERROR
    - During EMV authorization, Vantiv either identified an application transaction counter that was a duplicate of a previous counter or is outside the range agreed upon with the financial institution.
  - 301 CARDHOLDER VERIFICATION FAILURE
    - Special conditions within the Terminal Verification Results (TVR) prompted Vantiv to decline the transaction
  - 302 ERROR IDENTIFYING CHIP APPLICATION
    - Vantiv is unable to recognize the chip application associated with the Issuer tag data provided
Card Conversion Basics

- Vantiv has converted all BINS to Multi-Plastic Setup under “single BIN”
- Generic and White Plastic Gallery art will be pre-converted
- Issuer Custom Art will be managed as today
Chip Placement

- Real-estate on front of card is changed
- Activation sticker placement and size limitations
- Signature panel changes
Card Production Process

- Plastic
- Chip
  - Perso
- Plate
EMV FI Debit Pilot Overview

- SOW Finalization
- EMV Implementation Definition
- Card Production - Phase 1 Design
- Card Production - Phase 2 Collateral
- Mass Issue - Phase 1 - Small Production Pilot
- Mass Issue - Phase 2 - Large Production Pilot
- Go Live
- On-going

- Card Configuration
  Card Profile Selection
  Network Participation

- 15 wks
- 6 wks
- 4 wks
- TBD
- TBD
- TBD
- TBD
Instant Issuance

Current offering
- Standard Instant Issuance
- Card Extract Instant Issuance
- Integrated Instant Issuance

EMV Future offering
- Standard Instant Issuance
- Card Extract Instant Issuance
- Integrated Instant Issuance

Under Development
How does Debit Issuer “get started”

• Meet with Vantiv (RM / Product) to review product features needed/available
• Initiate project within Vantiv Conversions team
• Develop card “profile” requirements
• Open project with brand (drives certifications (Profile, Card))
• Develop/Forecast card quantity, timing, network and artwork requirements
• Choose implementation strategy
  › Natural or Mass Re-Issue
• Expect significant lead times (+12 weeks), begin in ‘Q3 for early Q1, 2015 roll-out
Vantiv EMV Credit Solutions
Full Service Supported by FDR

Card Procurement and Personalization
- CHIP Selection
- Profile selection & certification
- CHIP Lifecycle Management

Authorization
- Manage new data elements
- Cryptogram validation/response
- Manage EMV risk parameters
- Key Management

Core Systems
- New data elements in core platforms (3270/ CardStation)
- Pin Now DefenseEdge

Communications
- Cardholder communications
- Internal training and messaging
- Issuing strategy
### EMV Credit Profiles

<table>
<thead>
<tr>
<th>Form Factor</th>
<th>Auth Mode</th>
<th>Profile(s) Summary</th>
<th>CVM List</th>
<th>Card Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Offline Support</td>
<td>Online Pin Preferring, Signature</td>
<td>Signature, Online Pin, No CVM</td>
<td>MasterCard</td>
</tr>
<tr>
<td>Contact</td>
<td>Online Only</td>
<td>Online Authorization Only</td>
<td>Signature, Online Pin, No CVM</td>
<td>Visa</td>
</tr>
</tbody>
</table>

- Each credit card’s characteristics are managed within a certified application “profile”
- Vantiv is utilizing Visa & MasterCard certified application profiles Contact Only, Chip & Signature Preferring
- Contactless not immediately supported
- MasterCard Offline PIN support will be available when market becomes ready
- Profiles/chips are certified at FDR for easy BIN enablement
EMV Credit Card Product:
A Standard Product Offering that Accommodates the Majority of Community

- Contact Only, Chip and Signature Preferring
- Profiles certified at FDR for easy BIN enablement
- Contactless and Chip and Pin can be supported at later date
- Can use several card manufacturers for card production & personalization
- Currently 8 – 12 week lead time from date art work is received
- Utilizing New “PIN Now” IVR with new PIN Mailers for EMV cards
Credit EMV Beta Progress Report

- Released Visa Beta EMV Cards May 19th
- Currently working with MasterCard Beta targeting Mid-September 2014 roll-out
- Custom Clients – 1Q 2015
- Shared BINS – 1Q 2015
EMV FI Credit Pilot Overview

Once plastic procured, approximately 90 -120 days to implementation
How does Credit Issuer “get started”

- Meet with Vantiv (product and/or SE teams) to review product features needed/available
- Initiate project within Vantiv Conversions team. Open E-request
  - Determine card programs/BIN’s
  - Develop card “profile” requirements
  - Project opened at FDR in order to obtain project resource
- Project opened with Platform team – PCF & Rules set-up
- Project opened with Plastics Procurement
  - Develop/Forecast card quantity, timing, network and artwork requirements
- Choose implementation strategy
  - Natural or Mass Re-Issue

Expect significant lead times (+16 weeks)
Getting Ready
EMV Questionnaire

Contact Information
FI ACRO: 
Contact Name: 
Email: 
Phone: 
Core Processor Name: 
Core Processor Contact Name: 
Core Email: 
Core Phone:

Overall Project Information
List all debit and Gateway Credit BINs (ATM currently not supported) that will become EMV capable:

Are any of these BINs new to the Vantiv system? Yes No
If using existing BINs, will a BIN extension be necessary Yes No
Will the EMV plastic type be the default plastic type when ordering New Opens/Replace/Reissue Yes No
Does the Vantiv Contact Center Reorder/Replace any cards on behalf of the FI? Yes No

EMV Roll Out Strategy
Mass Issue
1. Does the FI want to Mass Issue all cardholders EMV plastics as part of this project? The FI will be responsible for reviewing and cleaning up the database as part of the EMV implementation project. Yes No

OR
2. Do you intend to utilize the Card Extracts/Maintenance File to initially open/reorder all of the cards as EMV plastics? Yes No

Natural Reissue
3. Does the FI want to Naturally Reissue cards upon expiration to an EMV plastic? Yes No

EMV Testing Requirements
4. Will the FI receive No EMV data, Partial EMV data, or Full EMV data in the authorization message? No EMV Data Partial EMV Data Full EMV Data

5. Will you be expecting EMV data in the Activity File? Yes No

6. Will the Card Extract/Maintenance File be used to order EMV chip cards? Yes No

7. Does the FI currently support MCIF/Web Service for Instant Issue or other maintenance in which will now need to support ordering EMV chip cards? Yes No

Card Production Changes
8. Will you need to change your card design due to the EMV chip placement? Yes No
Customer education

Documents
- Statement messaging – let your cardholders know when the new cards are coming
- Inserts – educate your cardholders on what will change
- Targeted letters – a personal touch with more education

Additional channels
- Mini web site – central area for information
- Sample videos – how POS and ATM will change
- In branch messaging – an additional great touch point

Cardholder facing staff / call centers
- Build an internal team “specialists” to answer questions
- Be prepared to have additional staff to handle more calls and longer call times as you launch
Start Planning **NOW!**

- Recognize that implementing **EMV** will take time and **can be complex**.
- **Assist your issuer in beginning their education process**, this drives the product profile and certification process.
- **Remember that there is a significant lead time**, even once the product is in its general release phase, for those issuers who want a Q1, 2015 rollout or pilot, they should begin by Q3, 2014 to ensure their timeline.

*Under 300 business days remain until the Counterfeit Fraud Liability Shift.*
Questions