EMV – A Chip Off the New Block

WACHA Taking Flight With Payments
March 18, 2014

Paul Tomasofsky
President, Two Sparrows Consulting
Paul@TwoSparrowsConsulting.com
(201) 930-9551

Christa Addy
Product Manager, Shazam Network
caddy@Shazam.net
800-537-5427, ext. 4147

Ann Davidson
CUNA Mutual Group
Senior Consultant-Risk Management
Ann.Davidson@CUNAMutual.com
800-356-2644, ext. 6657117
The opinions expressed by Mr. Tomasofsky, Ms. Addy and Ms. Davidson during this presentation are exclusively their own and subject to change.
Agenda

- Chip Card Refresher
- Regulation II and Chip
- Global Brands Roadmaps for EMV
- What Issuers Want
- What Merchants Want
- Current U.S. Landscape
- Open Standards
Chip Card Refresher

EMV History

- Europay International SA, MasterCard and VISA
- 1994 – Initial Specification Developed
- EMVCo-formed in 1999 to manage the specification
  - VISA, MasterCard - 1999 (Europay became part of MasterCard in 2002)
  - JCB - 2004
  - American Express - 2009
  - Discover, UnionPay - 2013
How EMV Works

- Integrated Circuit Card (ICC)
- Designed to be used as Contact or Contactless
- Not just a card but a system
  - Terminals
  - New Messaging Data
  - New Application Logic
  - New Configuration Settings
- All Stakeholders Affected
  - Issuers
  - Merchants
  - Processors
  - Networks
  - Cardholders
How EMV Works

- Card Stock Chip is Locked Before Issuance
- Keys Need to be Injected onto Cards
- Card Security
  - CVC1 and CVV1 from Magnetic Stripe
  - CVC2 and CVV 2 from Signature Panel
  - Chip CVV (new for EMV)
- Online and Offline Processing Options
- Multiple Cardholder Verification Methods
- Issuer can send updates to card via terminals for some functions
Online Transactions

- Chip uses 3DES Encryption
- Authorization and PIN CVM validation goes to host
- Terminal’s integrity is checked
- Additional expected data generated that Issuer can validate and mitigate card counterfeiting
- Not all data is encrypted; PAN and expiry are in the clear
Offline Transactions

- Chip and terminal interact for authorization (No message to host)
- PKI used to encrypt transaction between chip and terminal
- Validates card is valid; can use dynamic data that will mitigate card counterfeiting
- Not all data is encrypted; PAN and expiry are in the clear
- Issuer can set parameters to force online authorization
Cardholder Validation Methods

- Issuer has options as to CVMs:
  - Online PIN
  - Offline PIN
  - Signature
  - NO CVM

- Issuer chooses a CVM priority list order
- Merchant Terminal match needed
- ATMs can be different than POS
Applications and Application Identifier (AID)

- Application
  - Contains the parameters that are used during the interaction between the card and the terminal
- AID
  - Written onto chip during card production
  - Identifies owner of the application
  - Helps the terminal work to process the card options
  - Network operating rules are linked to the AID
  - Chip cards can have multiple AIDs present
  - Terminal must be able to support the AIDs on the card
EMV Benefits

- Mitigates counterfeit cards; reduces fraud associated with usage of counterfeit cards
  - Introduces dynamic data that bad actors can’t easily replicate
- Allows for offline processing
Chip and Data Breaches

- Chip cards still have PANs and Expiry in the clear
- These elements can be intercepted during processing
- Can then be used for Card Not Present transactions
- Much more difficult to create a counterfeit EMV card than a counterfeit magnetic stripe card
- During an EMV deployment transition, magnetic stripes will still be needed on cards because terminal deployment will take time
Regulation II and Chip

- Unaffiliated Debit Networks Requirement
  - Common Application/AID
  - Multi-Application/AIDs

- Merchant Routing Choice
  - EMV was developed as Issuer choice

- ATM Implications (not part of Regulation)
Key Milestones

- **October 1**
  - PCI Relief – Early Conversion
- **April 1**
  - Merchant Acquirer Requirement
- **October 15**
  - Liability Shift – Merchant Fraud
- **October 15**
  - Liability Shift – Gasoline Retailers
Debit Network Alliance

- Formed December 2013
- Delaware LLC
- Group dates back to April 2012
  - SRPc Chip and PIN WG
About Debit Network Alliance

- Collaborative effort to provide interoperable adoption of chip technology for debit payments, while supporting security, innovation, and optimal technology choice.
- Equal access to EMV chip technology under terms supporting competition, network choice, innovation, and delivery of value to network participants.
- Perpetual access to the technology deployed to accomplish EMV in the US, the ideal solution for all parties represented by shared governance of the common debit AIDs.
- Support for all transactions types (PIN, signature, no-CVM) supported by the debit networks both existing and future.
What Issuers Want

- Compliance to Reg II
- Flexibility to port solutions between debit networks
- Support for all CVMs
What Merchants Want

- Single AID for domestic debit
- Routing Choice
- Support for all CVM
  - Most prefer PIN
Judge Leon Ruling

- Judge Richard Leon vacates Fed interpretation
  - Fed did not follow will of Congress
  - Including other costs in setting debit interchange rate
  - Fed must re-visit and do so quickly
  - Two unaffiliated networks also mis-interpreted
    - Two per *authentication method* was meant
- Implications
What Makes Sense

- Solutions that meet the Issuer requirements of portability among Networks without re-issuing cards
- Solutions that technically meet the Merchant and ATM owner requirements of a single Common US Debit AID on each card, allowing for AID selection, and host routing decisioning
- Ownership or perpetual agreement
- Cost effective
- Support for all transaction types
- Ensure competitive landscape
Standards for Chip

- EMVCo control of standard causes difficulties
  - Standard development too closely tied to business models

- Open, Consensus Standards is Preferred
  - All stakeholders contribute
  - Access to technology
  - Robust innovation
  - Robust competitive landscape

- Tokenization is next battleground
Questions