Meeting Between Federal Reserve Board Staff and Representatives of Visa
March 5, 2014

Participants: Louise Roseman, Stephanie Martin, David Mills, Mark Manuszak, Geoff Gerdes, Clinton Chen, Samantha Pelosi, Anjana Ravi, Aaron Rosenbaum, and Linda Healey (Federal Reserve Board)

William Sheedy, Alex Miller, Kimberly Lawrence, Ky Tran-Trong, (Visa); Oliver Ireland (Morrison & Foerster, LLP)

Summary: Representatives of Visa met with Federal Reserve Board staff to discuss their observations of market developments related to the deployment of EMV (i.e., chip-based) cards in the United States. The Visa representatives also provided an overview of the technical migration to EMV and of the use of PIN as a consumer authentication method.

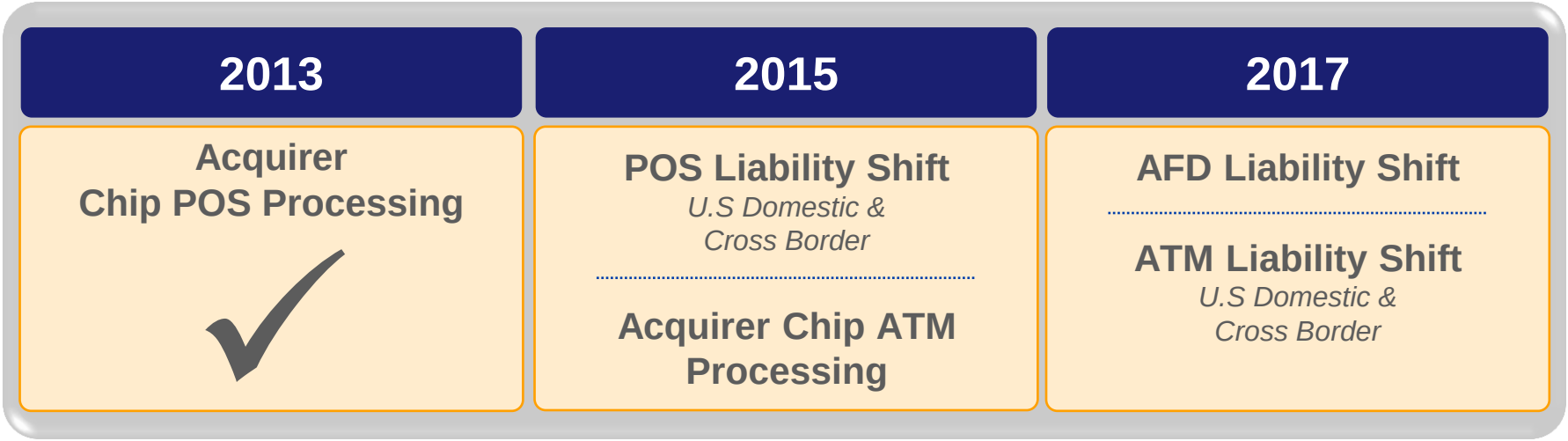
A copy of Visa's presentation is attached.

EMV Update

Discussion with the Federal Reserve

March 5, 2014

EMV Migration Momentum



Progress

- Visa and MasterCard separately reaffirmed roadmaps as initially announced
- Industry groups continue to work towards issue resolution and stakeholder education
  - Payment Security Task Force led by Visa and MasterCard
  - Merchant/Financial Trade Association Cyber Security Partnership
  - EMV Migration Forum
- 11 out of 14 unaffiliated U.S. debit networks, including Interlink, have adopted the Visa Common Debit Solution
- 6.5M+ US issued Visa EMV cards, mostly credit, mostly chip and signature

Ongoing Challenges

- Critical mass adoption of the Visa and MasterCard Common Debit Solutions
- Confusion surrounding "chip and PIN"

Chip CVM Considerations for the U.S.

- Chip and PIN do not have to be deployed together; markets that deployed without PIN focused on minimizing stakeholder and cardholder impact.
- Credit in the U.S. is not currently configured to work with PIN, and not all cardholders know or want to use a PIN at the point of sale.
  - Most merchant, acquirer and issuer payment environments would require a re-architecture to accept a PIN credit transaction
  - On debit, where many cardholders know/use their PINs at the POS, 63% of transactions are without a PIN
  - As only an estimated 2% of U.S. credit cardholders know their PINs, adding PIN to credit would likely create cardholder confusion at the POS and result in lost sales for merchants
- Given recent data breaches, the industry is rightly focused on accelerating the migration to EMV, which would significantly reduce the incentive for large data compromises; adding PIN for credit would greatly increase the time and investment required to migrate to EMV.
- Chip by itself eliminates counterfeit fraud; PIN doesn't stop counterfeiters, it merely slows them down. Once chip is deployed, PIN is only good for stopping fraudsters who have stolen the physical card – assuming the PIN has not also been stolen.
- PIN is "static data" – easily skimmed and phished, typically resulting in ATM fraud.
  - Adding PIN to credit would double the number of PINs in the ecosystem
  - ATM fraud is dramatically higher in Chip & PIN markets
- PIN is not an appropriate solution for all environments or all stakeholders.
  - PIN is not well suited to all environments (i.e., restaurants, small ticket, e-Commerce)
  - Nearly 2/3 of U.S. acceptance locations do not handle PIN today, requiring investment
  - Innovations such as contactless, "no signature required," and mobile wallets are not well suited for PIN
- PIN is not globally interoperable; nearly all PIN networks (like in the US) are domestic networks and do not work internationally. Signature is the only common cardholder verification method globally.

VISA

EMV and CVM in Other Large Markets

Chip and …	Key Countries		Rationale
Signature	Argentina Colombia Hong Kong Indonesia (credit) Mexico[1] Peru (credit)	Singapore South Korea[1] Taiwan Thailand (credit) Venezuela	• Cultural norms / mimicked CVM usage on prior magnetic stripe only products • Lack of infrastructure support / business case to build out PIN acceptance
Offline PIN	Brazil (credit) Canada France	Japan S. Africa UK	• High legacy telecom/online authorization costs
Online PIN	Australia Brazil (debit) Chile Germany Italy India[2] Indonesia (debit)	Kuwait New Zealand Peru (debit) Saudi Arabia Spain Thailand (debit) UAE	• Cultural norms / mimicked CVM usage on prior magnetic stripe only products

[1]Considering/beginning migration to PIN
[2]Migrated to PIN after initial EMV migration

VISA

Fraud Management by Payment Channel

Illustrative


Channel	Card/Device	Merchant	Acquirer	Network	Issuer
Authentication Type	*Consumer*	*Device*	*Payment*		
Card Present	• PIN • Signature • AVS	• Magstripe • EMV • NFC	• Fraud Scoring • Alerts		
Card Not Present	• Username/PW • V.me	• Device ID • CVV2 • CVV	• Tokenization • VCAS / VbV • Fraud Scoring • Alerts		
Mobile	• Biometrics • V.me	• NFC • Device AID • Geo-location • Dynamic QR			

Multi-Layered Protection