Meeting Between Federal Reserve Board Staff and Representatives of Visa
July 1, 2014

Participants: Louise Roseman, Stephanie Martin, Jeffrey Marquardt, David Mills, Samantha Pelosi, Mark Manuszak, Krzysztof Wozniak, Clinton Chen, Andreas Westgaard, Slavea Assenova (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 recent market developments related to the deployment of EMV (i.e., chip-based) credit and debit cards in the United States. Representatives of Visa also provided an overview of payment tokenization.

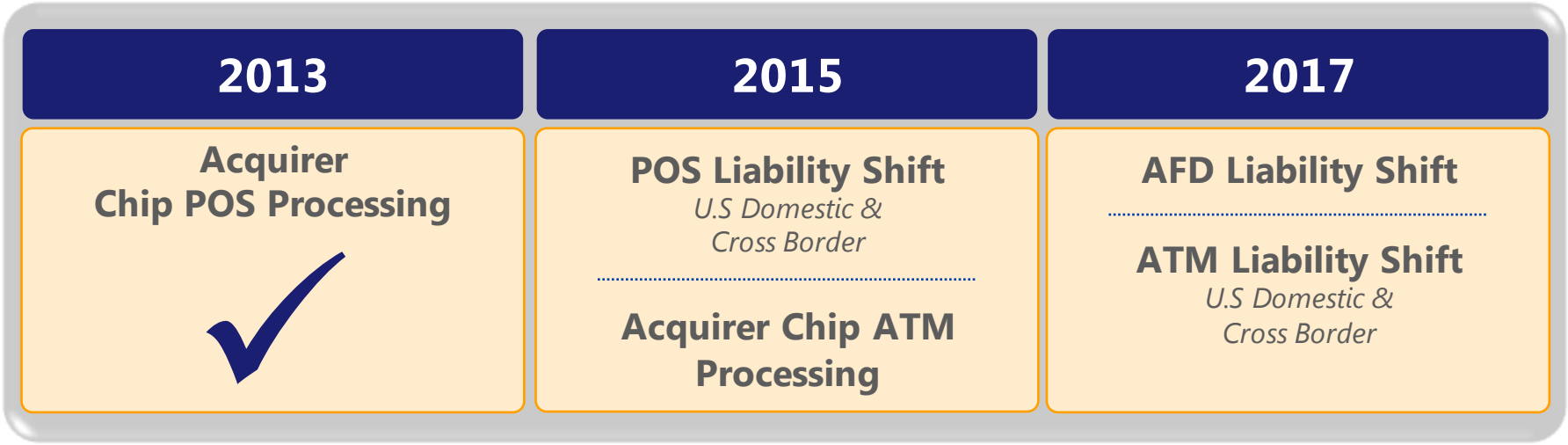
Attachment

EMV Update & Tokenization Overview

Discussion with the Federal Reserve

July 1, 2014

EMV Migration Momentum



Progress

- Industry groups continue to work towards issue resolution and stakeholder education
  - Payment Security Taskforce
  - EMV Migration Forum
- 13 unaffiliated networks adopted the Visa Common Debit Solution, representing all unaffiliated debit networks operating at POS
- An estimated 70% of US credit cards and 40% of US debit cards are expected to be EMV enabled by end of 2015,[1] along with 3.6M EMV-capable terminals[2]
  - Three quarters of issuers interviewed in an independent study plan to deploy "chip and signature" as preferred verification method for credit cards[1]

Ongoing Challenges

- Confusion surrounding "chip and PIN"
- Debit stakeholder readiness

1. Source: Aite Group: EMV Lessons Learned and the U.S. Outlook (June 10, 2014); 2. Source: Javelin Strategy & Research - EMV in the USA (April 2014)

VISA

Payments Security Taskforce

Overview

- Earlier this year, Visa and MasterCard formed a cross-industry group to enhance U.S. payments security, with a focus on encryption, EMV, and tokenization
- The goal of this effort includes advancing near-term opportunities for payment system security and communicating industry-wide commitment towards ensuring long-term payments system security
- The group fills a specific need that doesn't exist in the marketplace today - a group of senior executives who can effectuate actionable change in a short period of time and is intended to be complementary to other industry groups.

Participants

- This group includes a cross-section of industry participants with different viewpoints, including:
  - Top issuing and acquiring financial institutions and credit unions
  - Large online and brick-and-mortar retailers
  - Point-of-sale device manufacturers
  - Industry trade groups

VISA

Tokenization Overview

Existing Tokenization Services

- Tokenization has been used for many years by acquirers and merchants to:
  - Streamline user interface (e.g., username/password, email address or mobile phone number)
  - Remove financial primary account number (PAN) from a merchant database
- These token services typically:
  - Require de-tokenization prior to authorization and clearing
  - Are not shared with payment network or the issuer

New EMVCo Payment Tokens

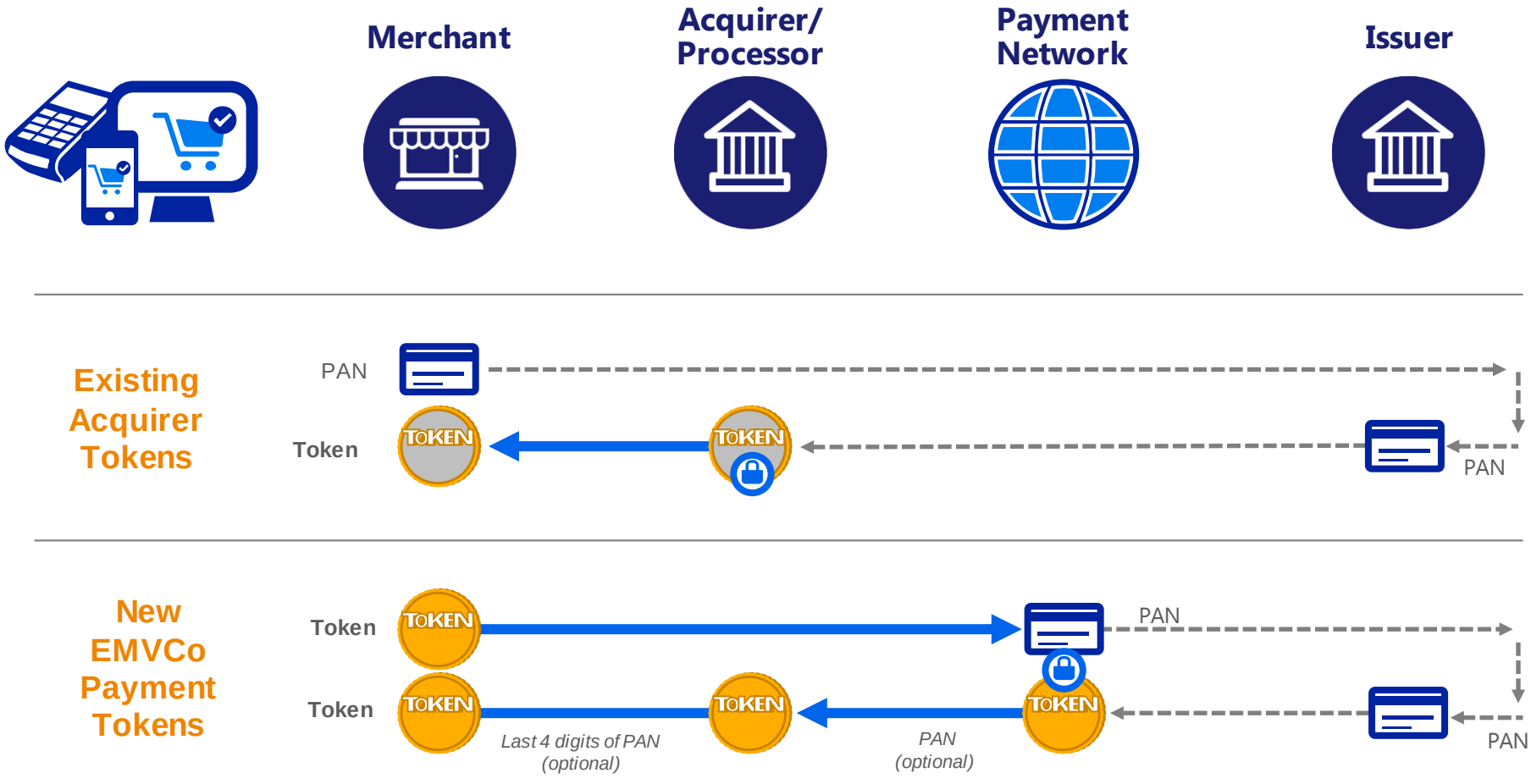
- A payment token is a "non-financial identifier" that can be used in place of an original payment credential to initiate a payment transaction
  - Tokens will be used to initiate payment transactions throughout the payment ecosystem
  - Domain restrictions may be applied to minimize fraud impacts if data is exposed
- Payment tokenization will:
  - Improve transaction security
  - Promote innovation
  - Provide a method for third party payment enablement

VISA

Tokenization Process

= Token service provider
= Auth. request
= Auth. response

ILLUSTRATIVE



VISA

Value Proposition

Value Proposition	Benefits	Existing Tokens	EMVCo Payment Tokens
Card reissuance	Card reissuance is not required if merchant database is compromised	✓	✓
	Card reissuance is not required if acquiring database is compromised		✓
Increased protection of sensitive data	Elimination of the PAN at the merchant level	✓	✓
	Elimination of the PAN at the merchant and acquirer level		✓
Risk reduction and risk detection	Reduced risk of subsequent fraud in the event of a merchant data breach	✓	✓
	Provides opportunity for merchants / networks / issuers to exchange relevant information for enhanced risk detection during token provisioning and authorization		✓

Key Tokenization Activities

Acquirer Token Solutions Introduced

- Card breaches increase in the U.S. with the rise of merchant databases
- Acquirer and gateway token solutions are introduced, allowing merchants to store tokens in place of the PAN to devalue the data

EMVCo Payment Token Standard

- Announced by Visa, MasterCard, and Amex in October 2013
- Cross industry standard for globally consistent approach to payment tokens
- Elements include new data fields, identification & verification, assurance and domain restrictions
- Adopted by EMVCo

Payment Security Taskforce

- Executive level, cross-industry group established, focused on advancing payment system security enhancements and building towards a long-term industry roadmap
- Tokenization selected as focus area along with EMV and Encryption

VisaNet Processing

Mandatory June 2014

- All U.S. VisaNet endpoints must be capable of recognizing and processing payment token-related data
- Critical step in migration to payment token processing

Visa Service *(In Development)*

Optional for all issuers

- Generate / issue payment tokens in lieu of original payment credential (PAN)
- Offered as an "on-behalf of" issuer service

VISA

Multi-layered protection devalues data and eliminates cross-channel fraud that cannot be addressed by EMV alone

EMV

- Benefit: Generates a dynamic card verification value and if stolen can not be used to create counterfeit cards
- Gap: Sensitive PAN data is sent in the clear and if stolen can be used for card not present fraud (i.e. cross-channel fraud)

Encryption

- Benefit: Protects sensitive PAN data by rendering it unusable if stolen, across all channels
- Gap: No single global security and implementation standard exists for encryption of data in-transit thereby limiting incentive for mass adoption

Tokenization

- Benefit: Removes the sensitive PAN data from the ecosystem and if data is stolen, provides domain controls that restrict the use of the data (e.g. card present mobile transaction token if stolen can not be used for a card present transaction)
- Gap: Implementation of new EMVCo payment tokens requires integration with existing payment infrastructure

VISA