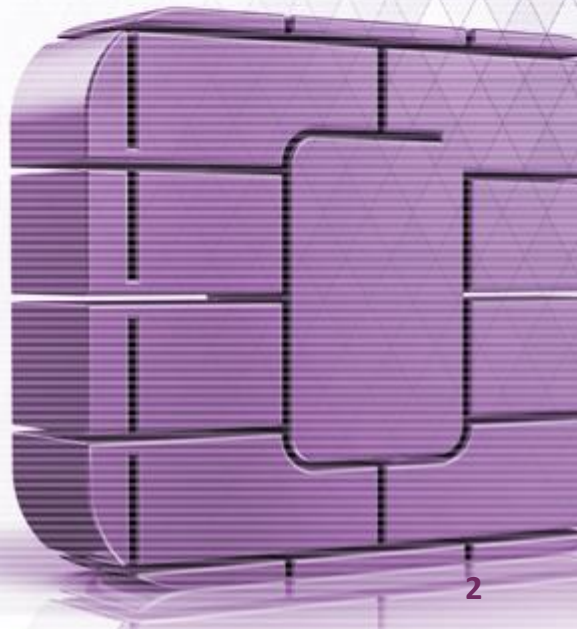
EMV® Migration Forum

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud

Randy Vanderhoof
Director, EMV Migration Forum

- Welcome
- Overview of the EMV Migration Forum
- The focus of today's webinar



EMV® Migration Forum

Today's Presenters

Ms. Francine DuBois
VP Global Sales & Partnerships
NagraID Security

Mr. Rodman K. Reef
Founder and Managing Principal
Reef Karson Consulting, LLC

Mr. Neeraj Gupta
Senior Product Manager

Vantiv, eCommerce

EMV® Migration Forum

Agenda

- Objective
- CNP Fraud in an EMV World
- Methodology
- Authentication Methods
- Fraud Prevention Tools
- Tokenization
- 3-D Secure
- Conclusion

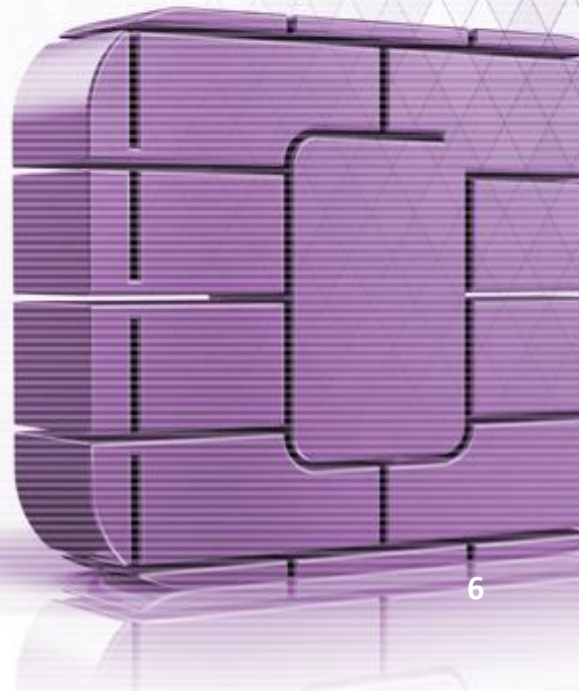
Webinar Objective

EMV® Migration Forum

Webinar Objective

Provide Information to Industry stakeholders on current tools and best practices for securing the Card-Not-Present (CNP) channel which can be implemented in parallel with the U.S. EMV Conversion

Focus on techniques which are currently available. Additional techniques which are in development and scheduled to be available in late 2016 and beyond are “out-of-scope”



EMV® Migration Forum

Card Not Present Fraud…

In an EMV World

EMV® Migration Forum

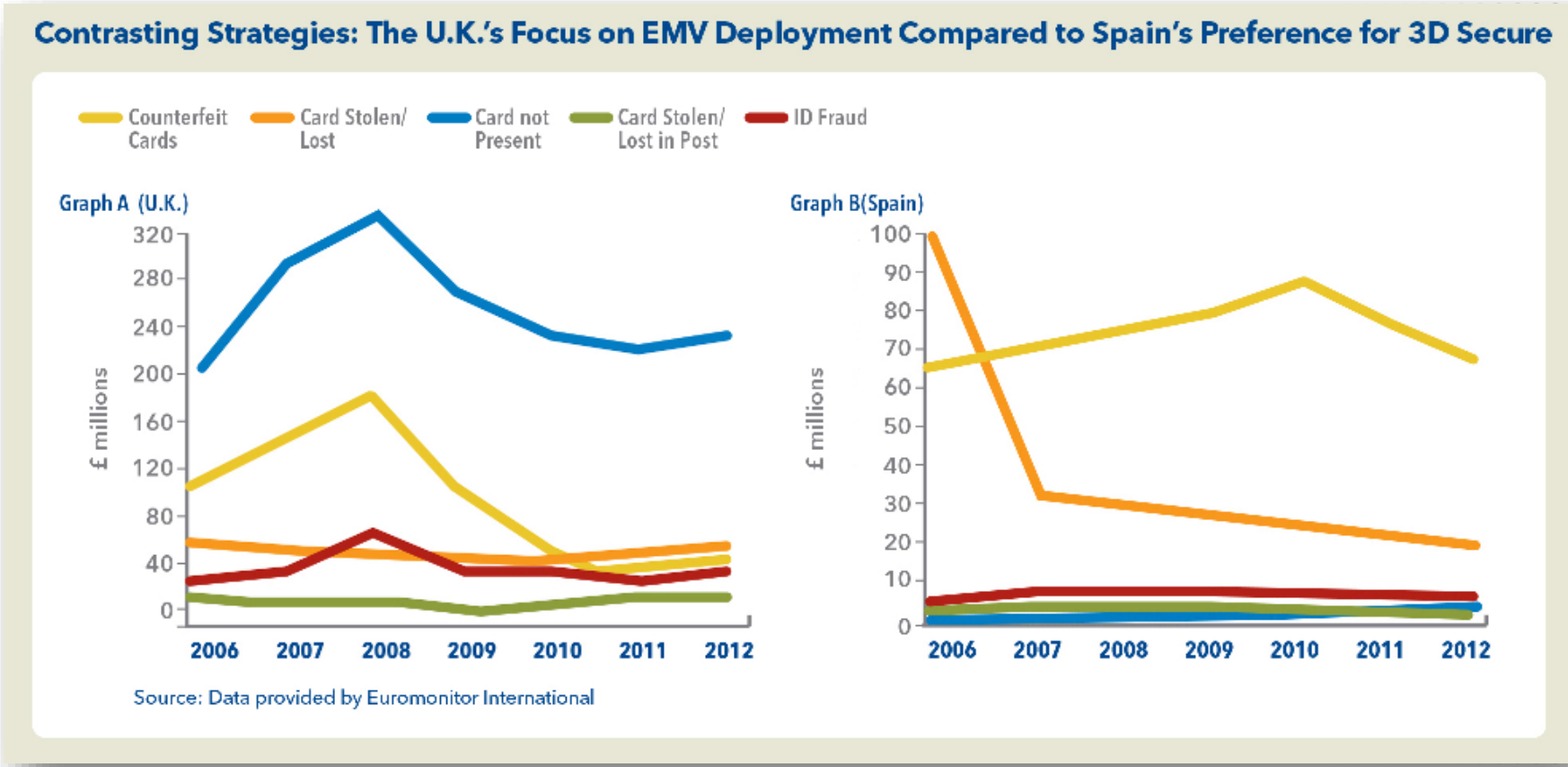
CNP Fraud in an EMV World

"The experiences of other countries may illustrate the short-term impact that EMV payment cards could have on…the United States. [EMV] will likely [cut off] some methods of card payment fraud but fraud will also shift to other types of card payment with relatively weak authentication protocols. Counteracting those shifts may require additional steps."

– Richard J. Sullivan, FRB of Kansas City

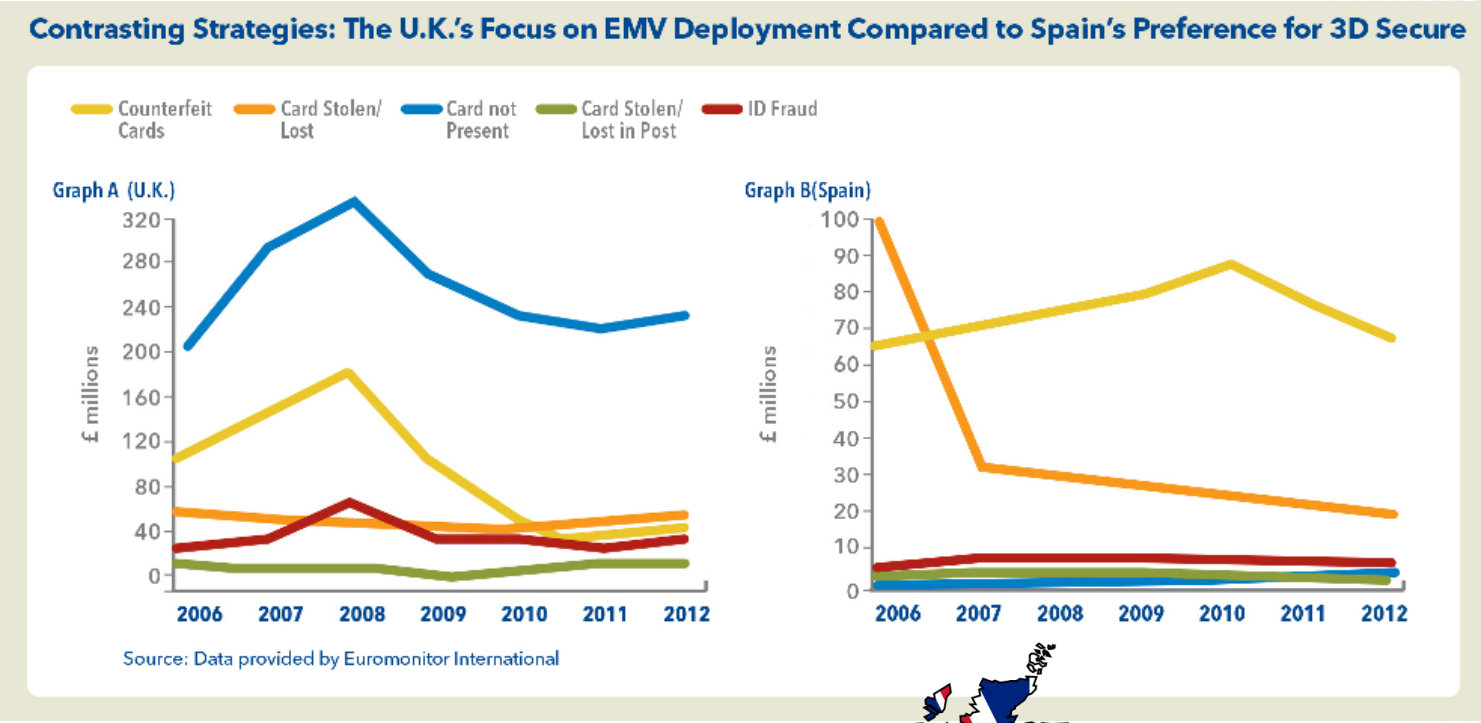
EMV® Migration Forum

CNP Fraud in an EMV World



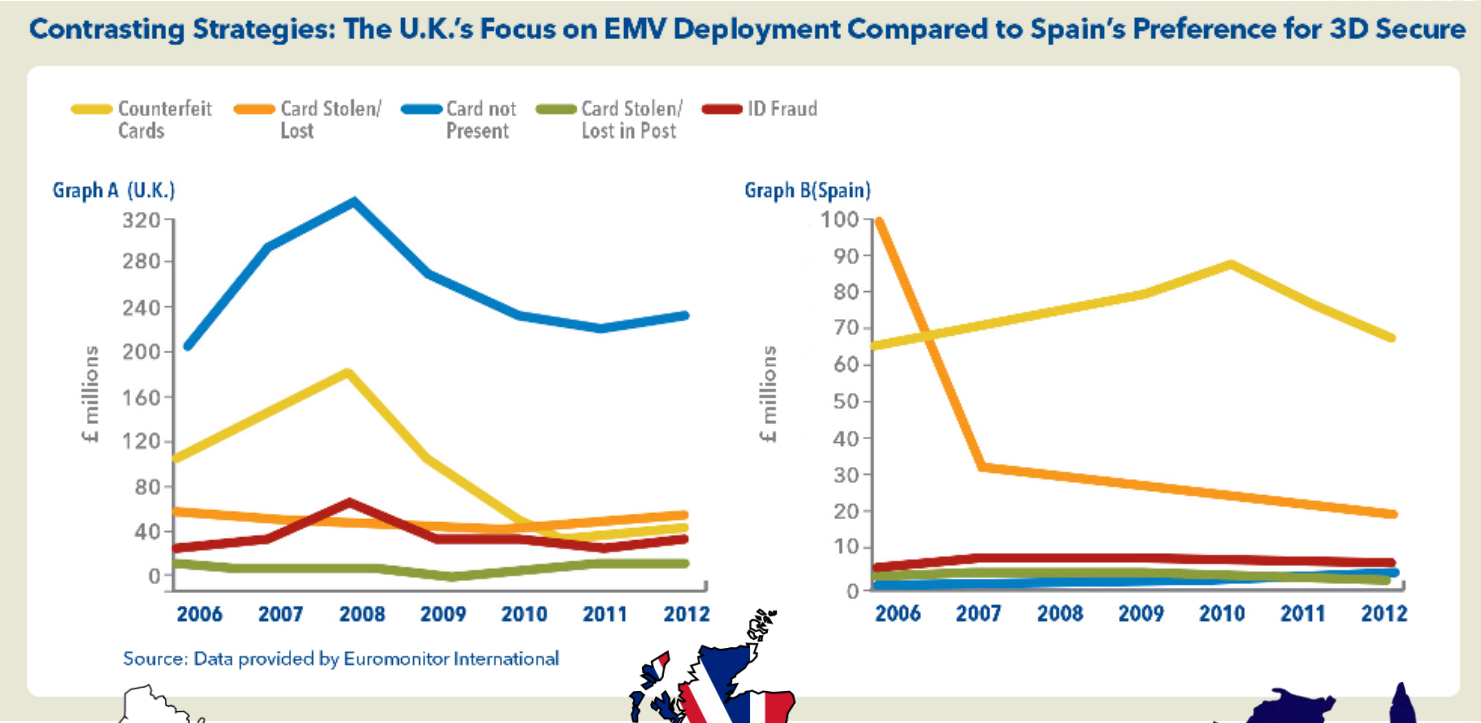
EMV® Migration Forum

CNP Fraud in an EMV World



EMV® Migration Forum

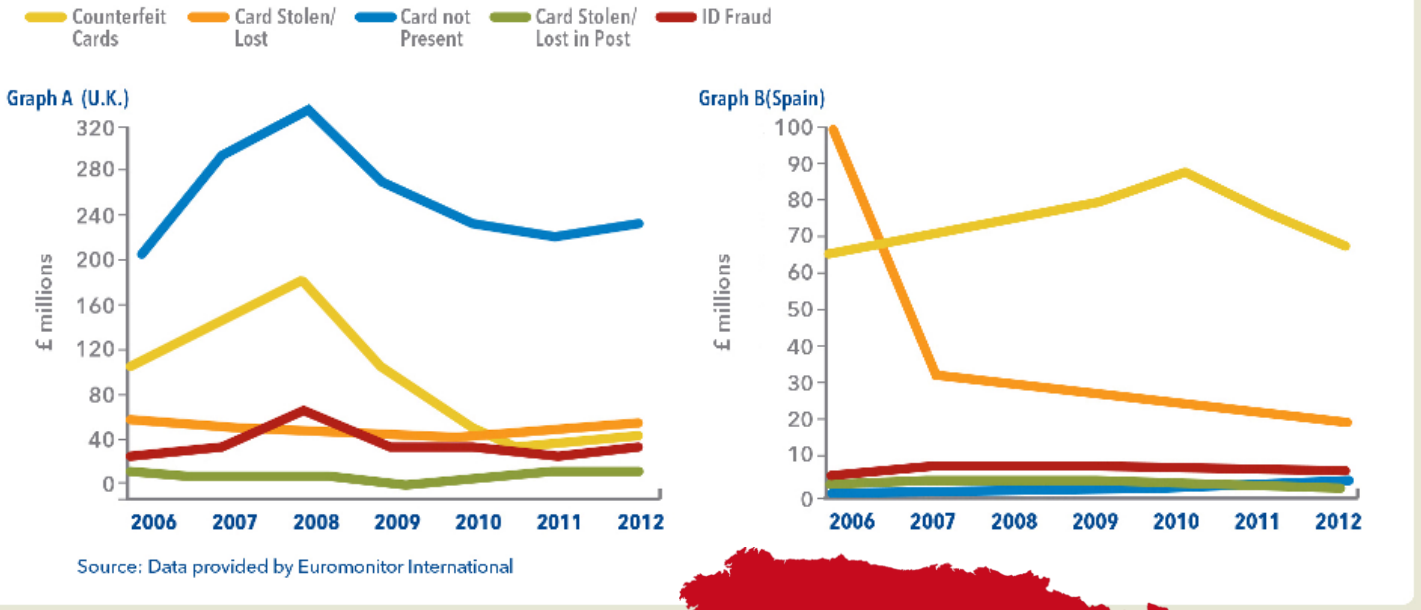
CNP Fraud in an EMV World



EMV® Migration Forum

CNP Fraud in an EMV World

Contrasting Strategies: The U.K.'s Focus on EMV Deployment Compared to Spain's Preference for 3D Secure

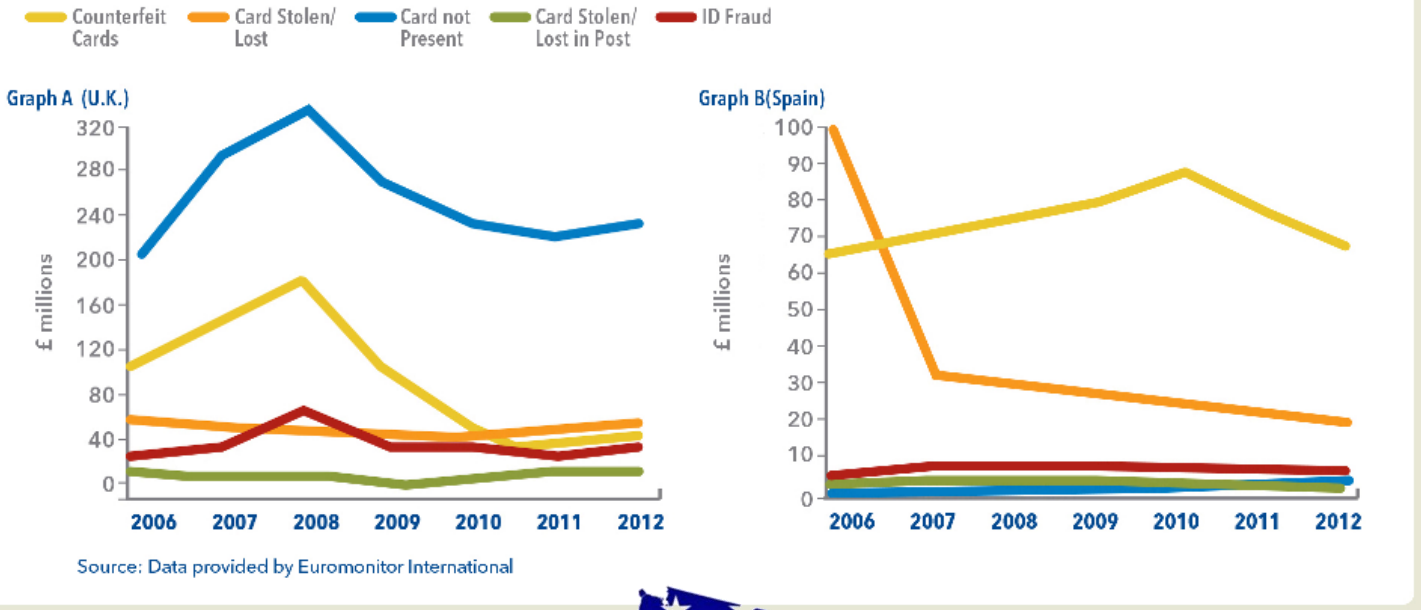


Source: Data provided by Euromonitor International

EMV® Migration Forum

CNP Fraud in an EMV World

Contrasting Strategies: The U.K.'s Focus on EMV Deployment Compared to Spain's Preference for 3D Secure



Source: Data provided by Euromonitor International

EMV® Migration Forum

Methodology

EMV Migration Forum

Methodology

Evaluation & Authentication Methods and Fraud Tools

Stakeholder Groups (merchants/acquirers, issuers, networks/brands) independently scored each method/tool against the key factors.

Authentication Methods

EMV Migration Forum

Authentication Methods

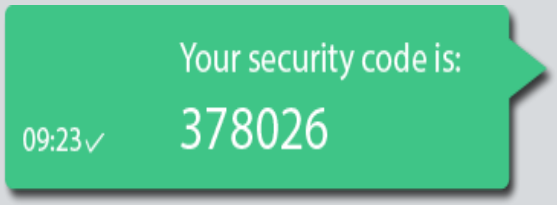
Device Authentication

- Authenticates the device used to access an e-commerce site
- Based on multiple data points acquired either before or during a transaction
- Consumer is not aware of the process unless the device is not recognized
- Usually performed by the merchant or the merchant's vendor

Authentication Methods

One Time Password

- One-Time Password (OTP) - A unique string of numbers and/or letters which is valid for only one transaction
- OTPs prevent replay attacks and other fraudulent transactions
- OTPs are generated by algorithms and can be delivered through a hardware device, paper, text messages, email and/or web-based channels
- When the delivery uses a different channel than the transaction, an OTP can be an effective component of two factor authentication
- OTPs are usually generated and authenticated by the card issuer



EMV Migration Forum

Authentication Methods

Randomized PIN Pad

- Provides a floating PIN pad on the merchant's checkout page for consumers who use PIN-enabled debit or credit cards for e-commerce transactions.
  - It can also be used with one-time PINs
- The consumer uses either a mouse, their finger or another pointing device to enter the PIN. The location of the numbers changes with each number entered.
- Only the x-y coordinates are transmitted and converted into an industry standard PIN in an HSM in a secure data center. The consumer's PIN is never in the clear

EMV® Migration Forum

Authentication Methods

Biometrics

- Uses unique features of a consumer's hand, voice, face, veins, or eye
- Biometrics data should be transmitted via secure channels
- Security of enrollment, data transmission and location of the biometric data file
- Use of biometric data could raise security and privacy concerns

*The white paper considered only facial and voice recognition and only the use of a smartphone for data capture.

Fraud Prevention Tools

EMV® Migration Forum

Fraud Prevention Tools

Best Practices

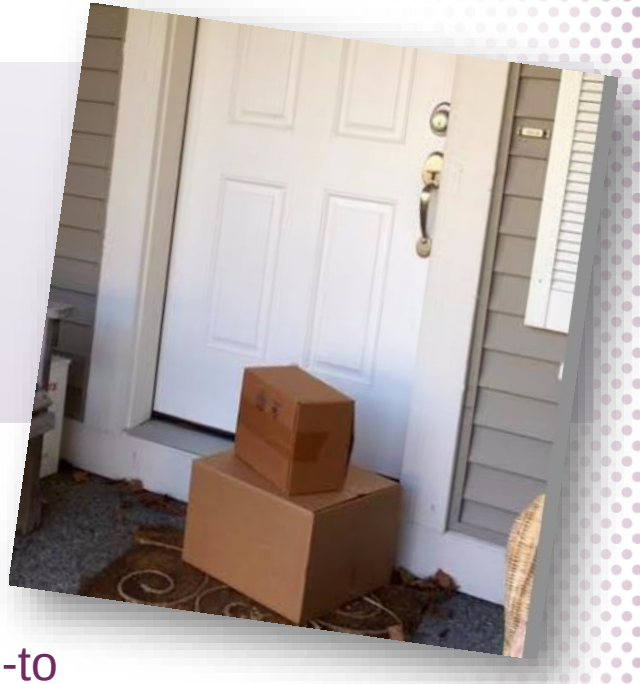
1. Proprietary Data/Transaction Data
2. Validation Services

EMV® Migration Forum

Fraud Prevention Tools

Proprietary Data/Transaction Data

- Collected by Merchants Acquirers and Issuers
- Accessed as Needed
- Used to enhance risk management

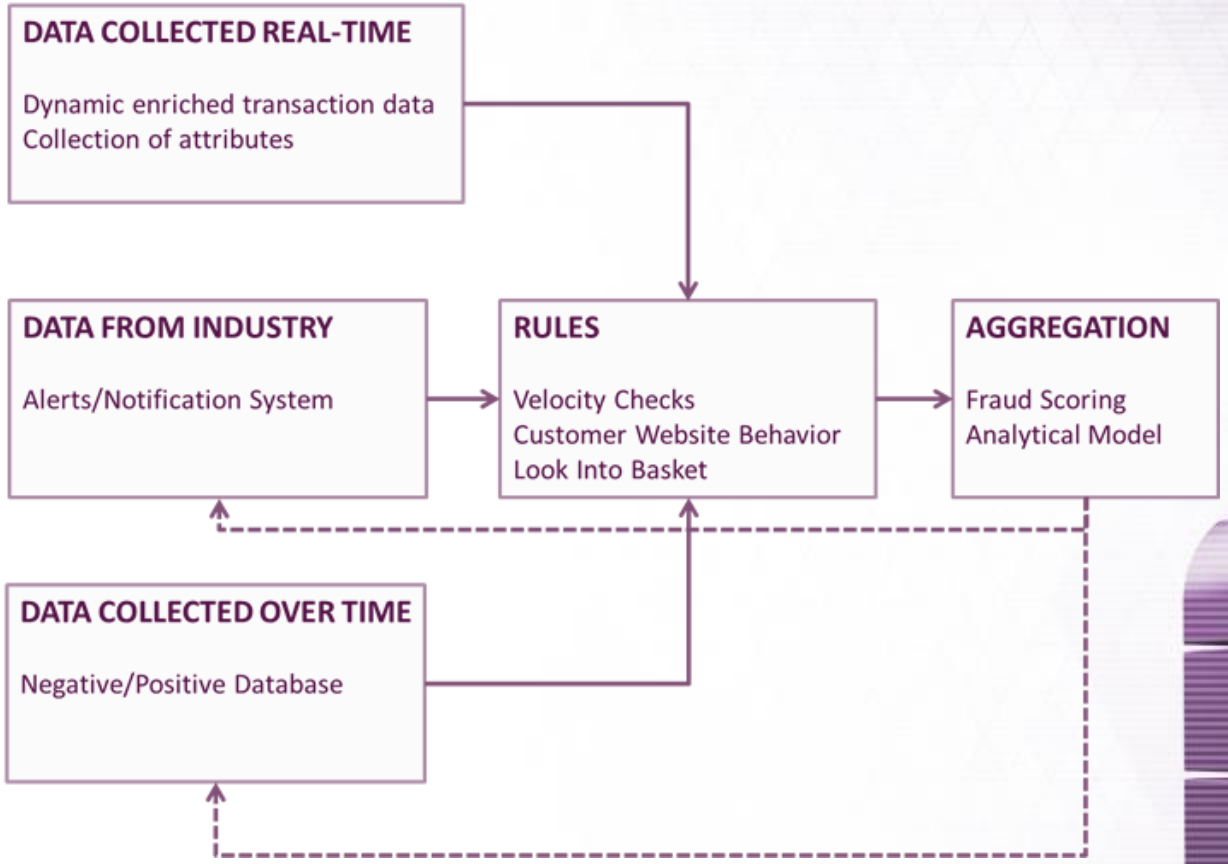


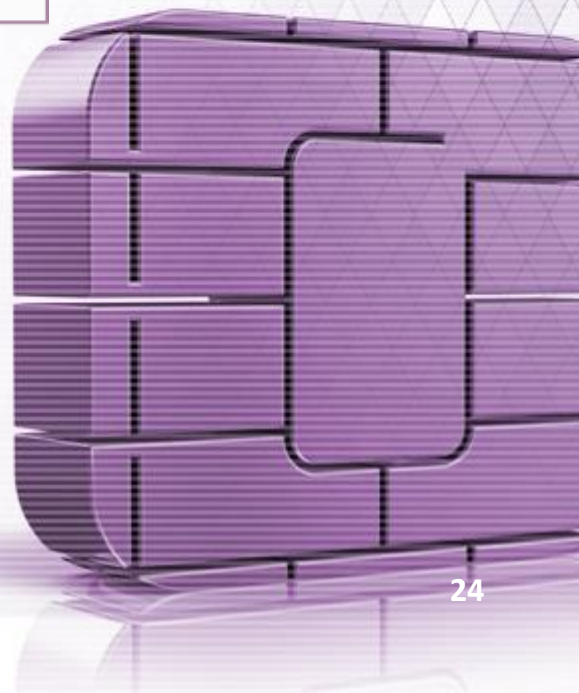
Examples:

- Lists of risky payment cards
- Order history
- email addresses, IP addresses and ship-to addresses of bad actors

Prior to delivery of product or service the data is scored

Proprietary/Transactional Data Fraud Tool





Fraud Prevention tools

Validation Services

Address Verification Service (AVS)

- Uses customer information other than a PAN to validate the card account holder is participating in the transaction
- The AVS validates the billing address of the cardholder's account
- Requires participation of the Issuers bank
- Card security code (CVV2, CVC2, etc.)

Security codes are present on the card.

- It is an encrypted value determined by card attributes including the PAN and the expiration date

Using AVS and/or the card security code can impact card brand fees and chargeback rights

Tokenization

EMV Migration Forum

Tokenization

End User

9876 0123 4567 8901 + 123

PAN
(Personal Account Number)

Merchant

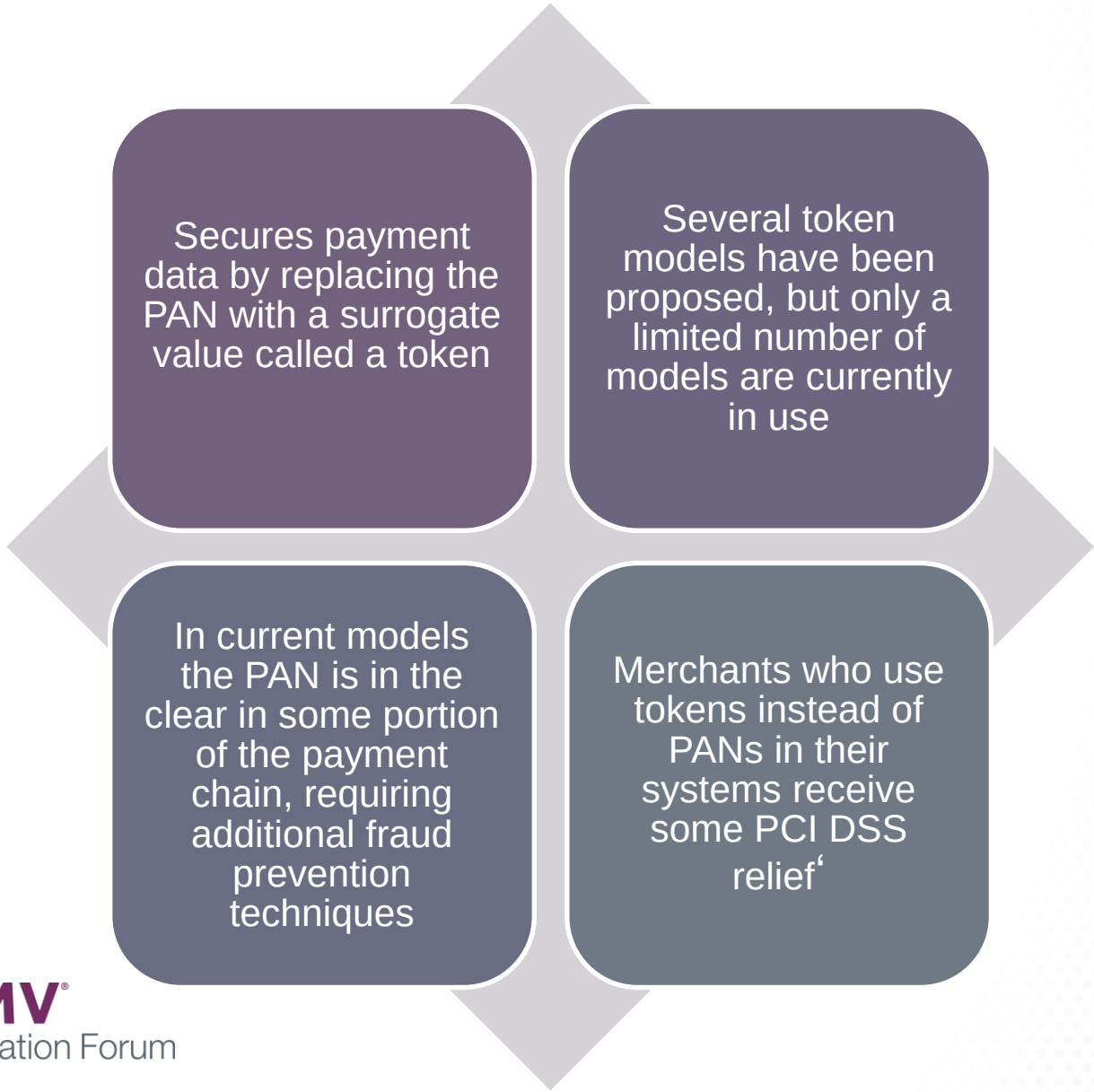
Processor

1000 6661 3334 8901+ 456

Surrogate PAN (tokenized data)

EMV® Migration Forum

Tokenization



3-D Secure™

EMV® Migration Forum

3-D Secure™

3–D Secure™ (3DS)

A secure communications protocol used to enable real-time cardholder authentication directly between the merchant and the issuer

The payment brands built proprietary products on top of this protocol: American Express SafeKey™, MasterCard's SecureCode®, etc.

EMV® Migration Forum

3-D Secure™

3–D Secure™ (3DS)

A secure communications protocol used to enable real-time cardholder authentication directly between the merchant and the issuer

The payment brands built proprietary products on top of this protocol: American Express' Safe Key, MasterCard's SecureCode, etc.

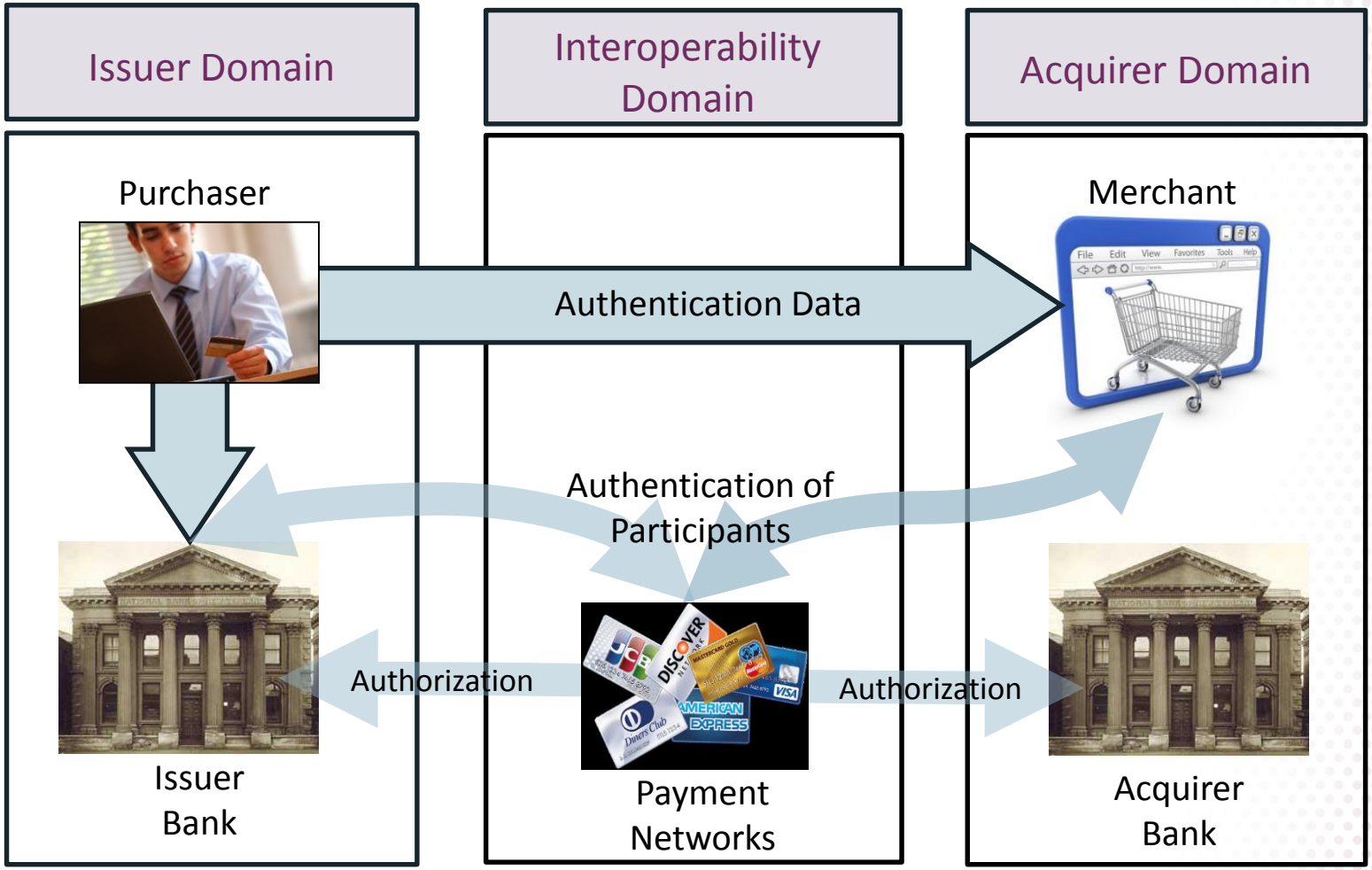
Authentication

Requires the cardholder to communicate a secret known to the issuing bank through the 3DS channel

3DS supports multiple authentication methods including static passwords, OTPs, biometrics, etc.

EMV® Migration Forum

3-D Secure™ Components & Flow



EMV Migration Forum

3-D Secure™ (3DS)

Older Model

Every transaction is authenticated and the cardholder is enrolled before performing a transaction

Newer Model

Risk based.
Given transactions are authenticated only when the risk exceeds a predetermined level

The issuing bank determines the model used and the authentication method (static password, OTP, etc.)

EMV® Migration Forum

Conclusion

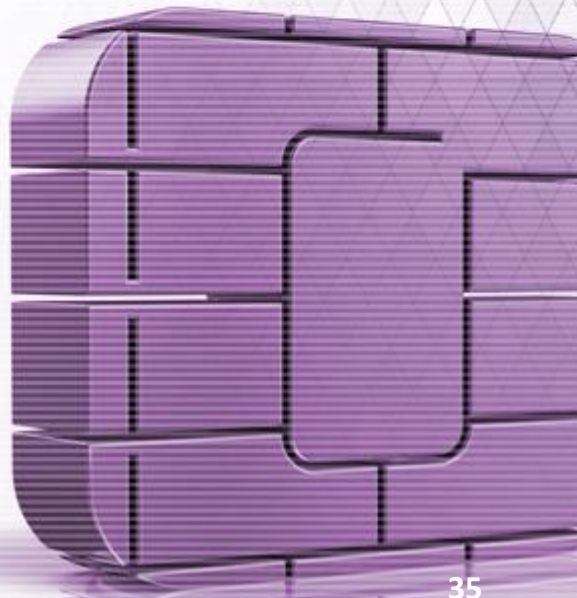
Mitigating the expected increase in CNP fraud should be considered in any EMV strategy

There is no one “silver bullet” to reduce or eliminate CNP fraud

A layered approach is recommended to reduce the risk of fraudulent actions

EMV® Migration Forum

Questions



EMV® Migration Forum

EMV®
Migration Forum

WWW.EMV-CONNECTION.COM