EMV: What it is, why it's important, and what do I need to know?

EMV Basics for Merchants

vantiv™

Agenda

- What EMV is
- How EMV works
- Card brand roadmaps
- Debit routing
- Planning steps

vantiv

What is EMV?

vantiv™

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**.

EMV has become the world-wide standard and both **U.S.** neighbors, **Canada** and **Mexico**, have EMV mandates effecting U.S. multi-national retailers.

EMV is the stepping stone to the future of payments due to its dynamic data authentication (Contactless, Mobile).

What is EMV?

The computer chip on the card uses **cryptography** to provide strong security. EMV can utilize two forms of cryptography to secure a transaction:

- Digital signatures – ensures data is **authentic**
- Encryption – ensures data is kept **confidential**

The **digital signature** devalues the card and transaction data because even if the data is intercepted, the digital signature cannot be replicated.

In the context of EMV, **encryption** is only used to protect the PIN.

- Does ***not*** encrypt all of the transaction data

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
- When used with a PIN, also protects against lost and stolen fraud. 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

Contactless and Mobile payment schemes

vantiv

EMV around the world

World wide EMV deployment and adoption[1]

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America and the Caribbean	401M	49.2%	5.6M	78.5%
Asia Pacific	372M	26.7%	5.0M	50.5%
Africa & the Middle East	50M	28.6%	0.6M	76.7%
Europe Zone 1	755M	80.7%	11.7M	94.5%
Europe Zone 2	46M	15.5%	0.9M	73.2%
United States2	1.5M			
Totals3	1.62M	44.9%	23.8M	75.7%

[1]Figures reported in Q4 2012 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally
[2]US Figures are estimates based on reports from Visa and MasterCard as of Q4 2011
[3]Totals does not included data from the US

97% of European ATMs and **97%+** of Canadian ATMs are **EMV** compliant

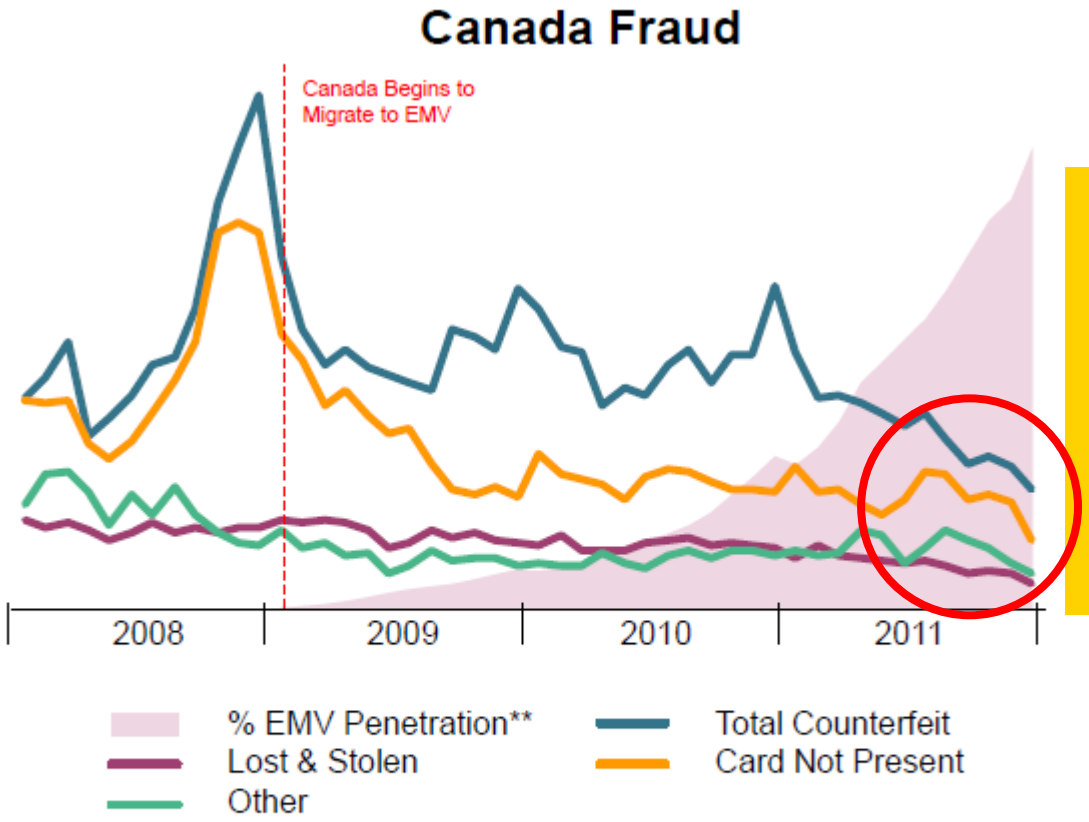
EMVCo

vantiv

Why EMV – Fraud trends Canada

2008-2010

HOLIDAY FRAUD PEAKS



BY 2011

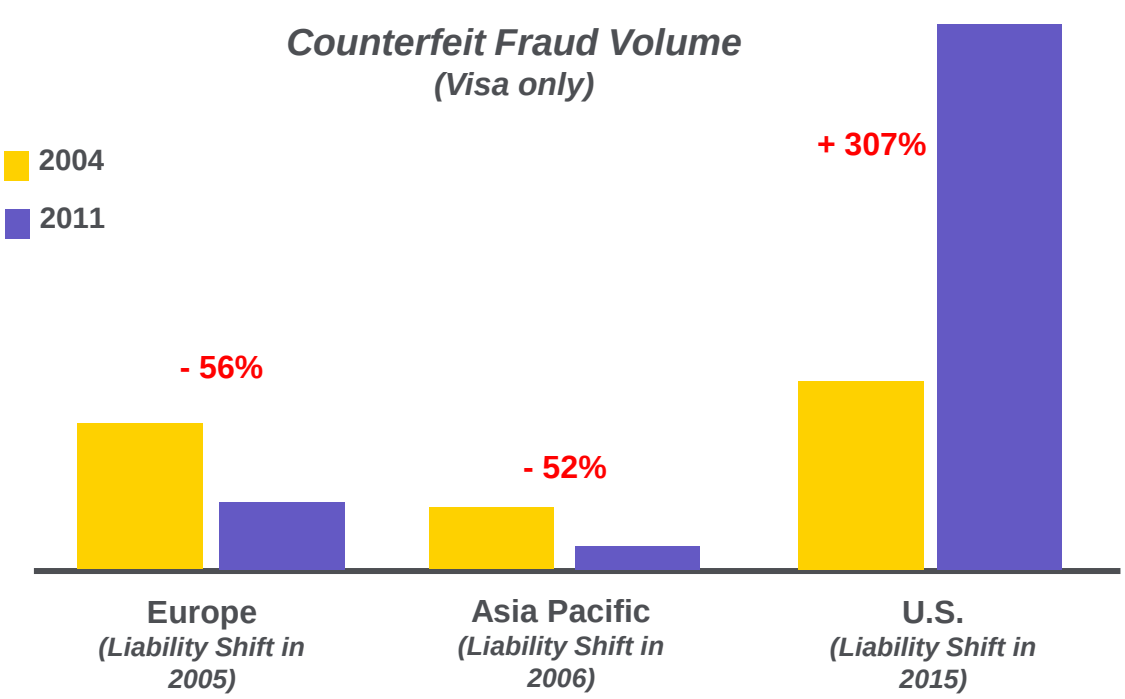
HOLIDAY FRAUD

SIGNIFICANTLY REDUCED

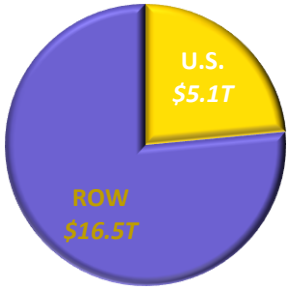
Source: MasterCard Analysis 2012
*Cross Border Counterfeit Fraud = Total Counterfeit Fraud – Domestic Fraud
** % face-to-face EMV penetration

vantiv

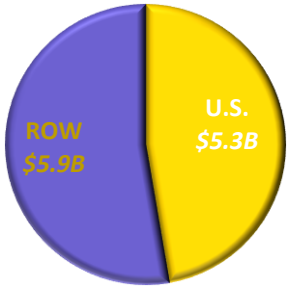
Why EMV – Global Fraud Trends



U.S. and Rest of World Sales Volume
2012



U.S. and Rest of World Fraud Volume
2012



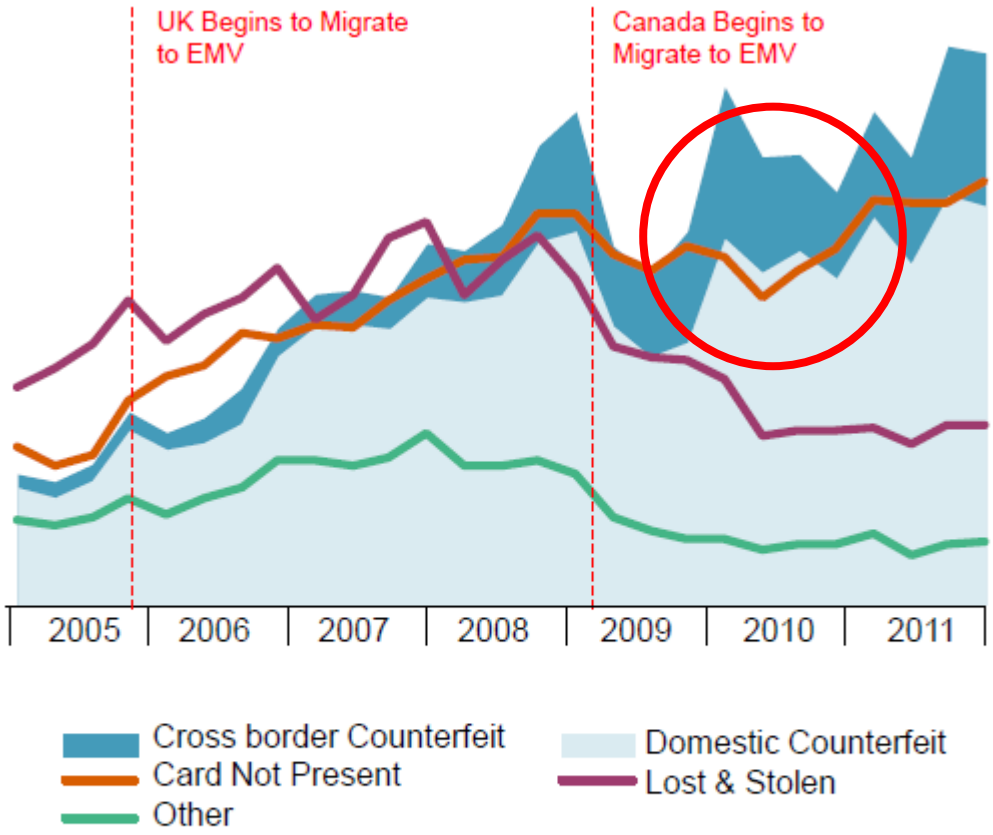
vantiv

Why EMV- Fraud trends in U.S.

As EMV migration nears completion in Canada, Europe and parts of Asia

U.S. Cross Border Counterfeit Fraud

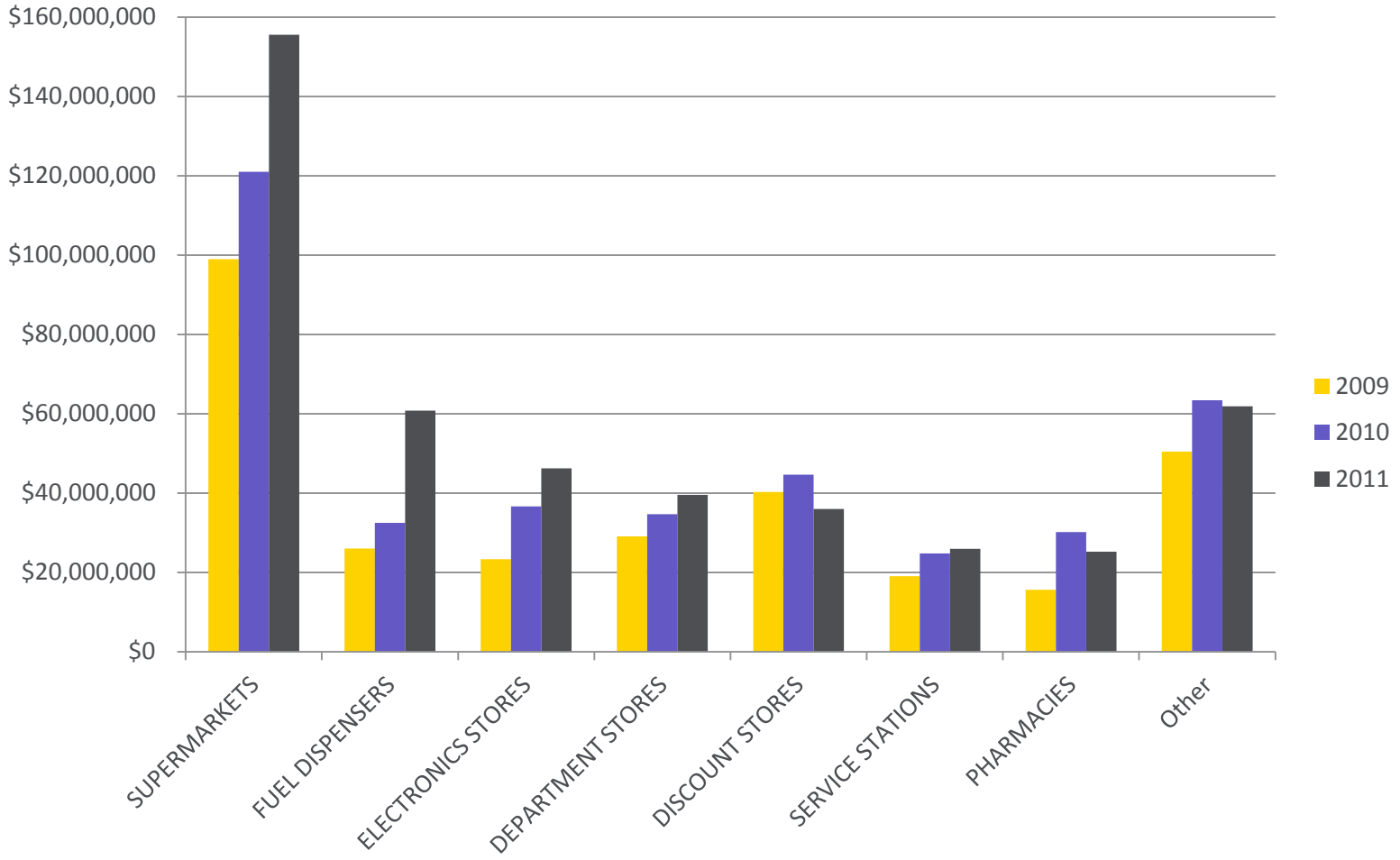
SIGNIFICANT
GROWTH SINCE 2005



Source: MasterCard Analysis 2012
*Cross Border Counterfeit Fraud = Total Counterfeit Fraud – Domestic Fraud
** % face-to-face EMV penetration

vantiv

What is the **risk**?

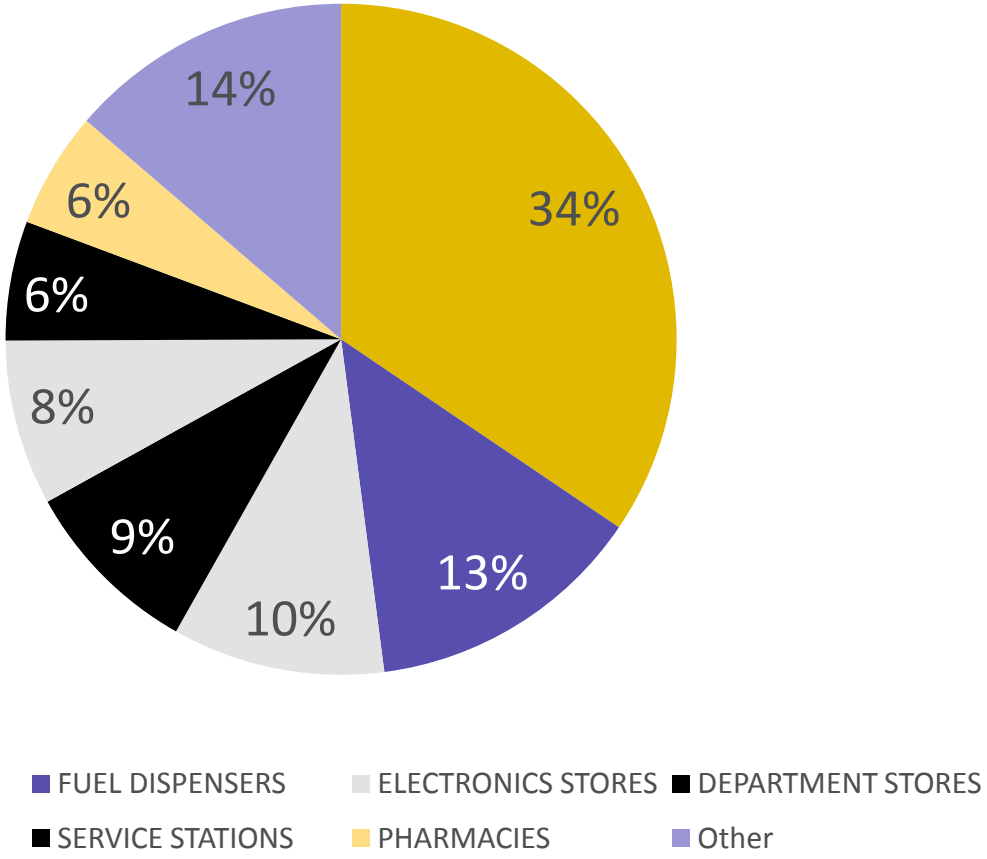


Source: Visa

Visa US Domestic Counterfeit Fraud

vantiv™

What is the **risk**?

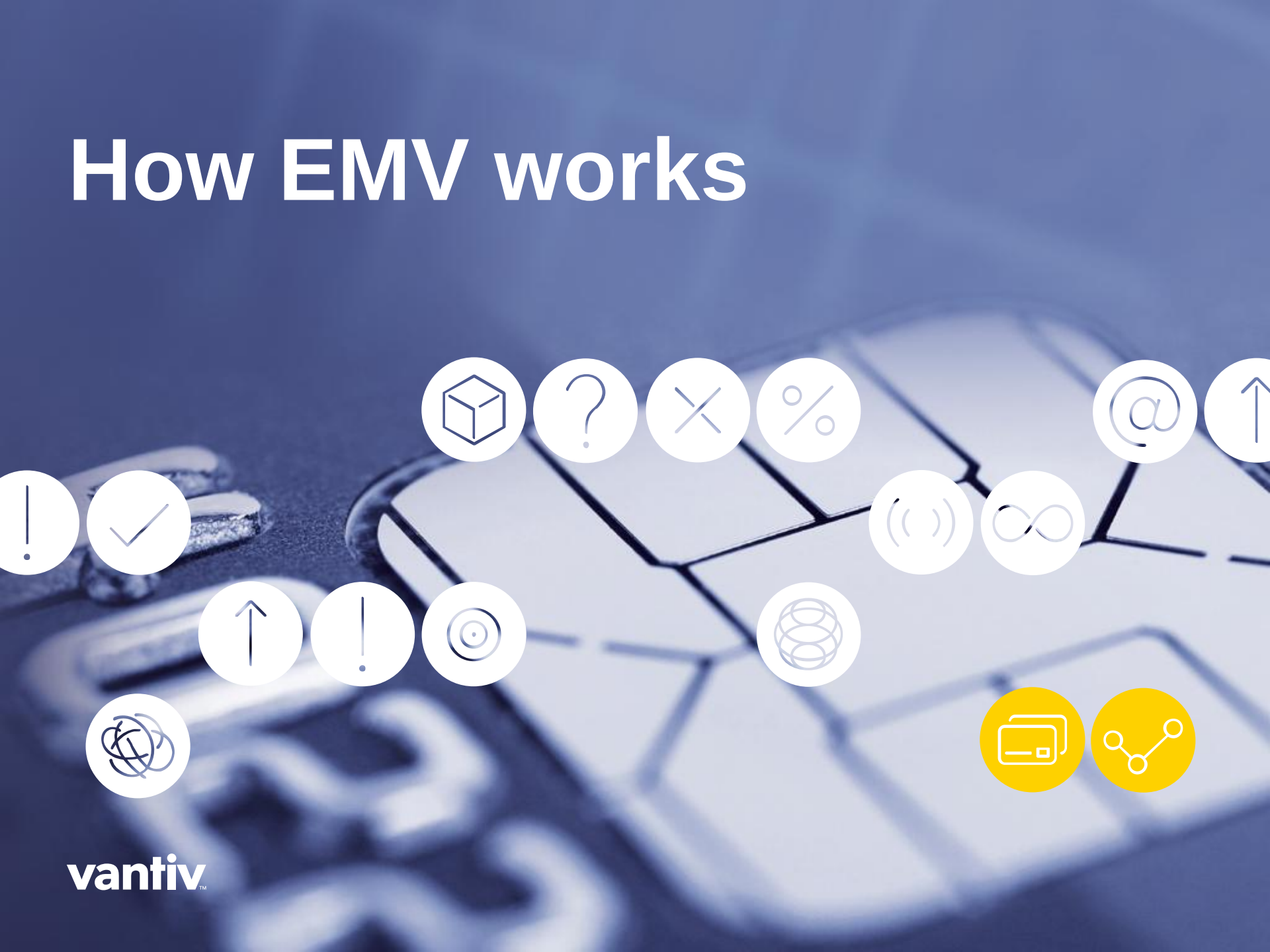


Visa US Domestic Counterfeit Fraud

Source: Visa

vantiv

How EMV works



vantiv™

How does EMV work?

- An **EMV** card is **inserted** into a terminal
- The chip embedded in the card contains the **account data**; this is accessed by the reader in the terminal
- Using data from the card and the transaction, the chip creates and sends a unique code, or "**cryptogram**", to the processor's host during the transaction, validating the card

- The card is removed when the **transaction is completed**

Contactless and Mobile

- An **EMV** chip can be on a **contactless card** where the chip is tapped or held near the terminal

- OR -

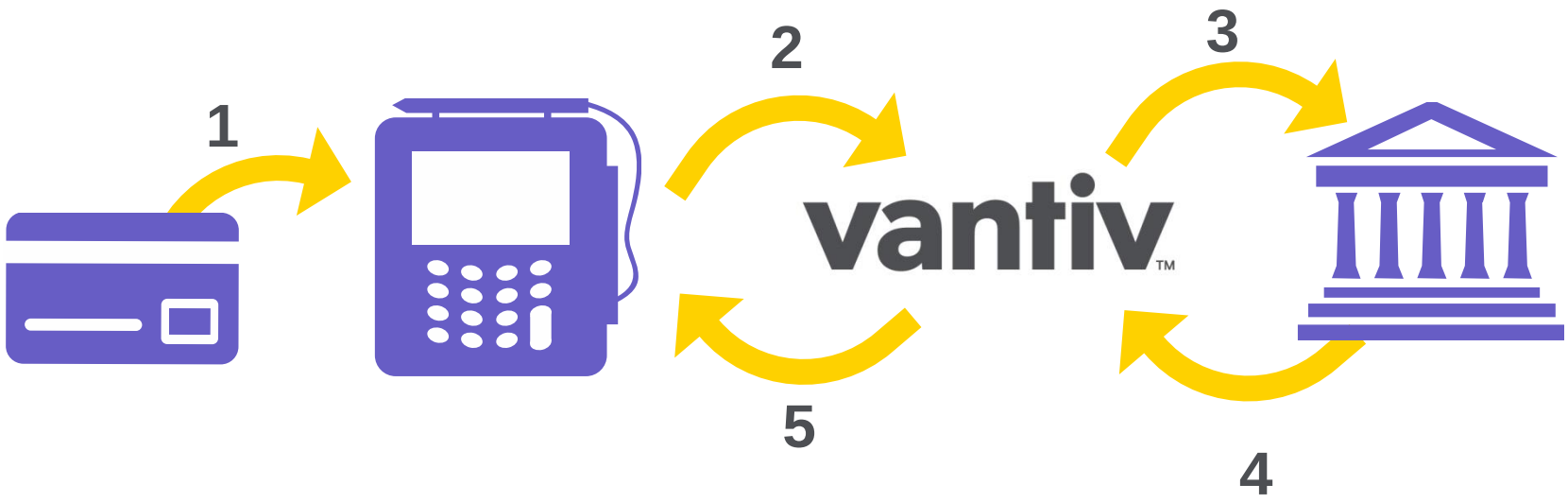
- A chip can be inside your **smart phone** and the phone is waived near the terminal

Difference between **Magnetic Stripe Terminal** and EMV Terminal

There is a fundamental difference between a **magnetic stripe** and an **EMV chip transaction**

- Magnetic Stripe Terminal
  - Card is simply a **static storage** device that is read by the terminal
  - The terminal performs **card swipe**, **PIN encryption** and **signature capture** (integrated environments) functions

Terminal Mag Stripe Transaction Flow



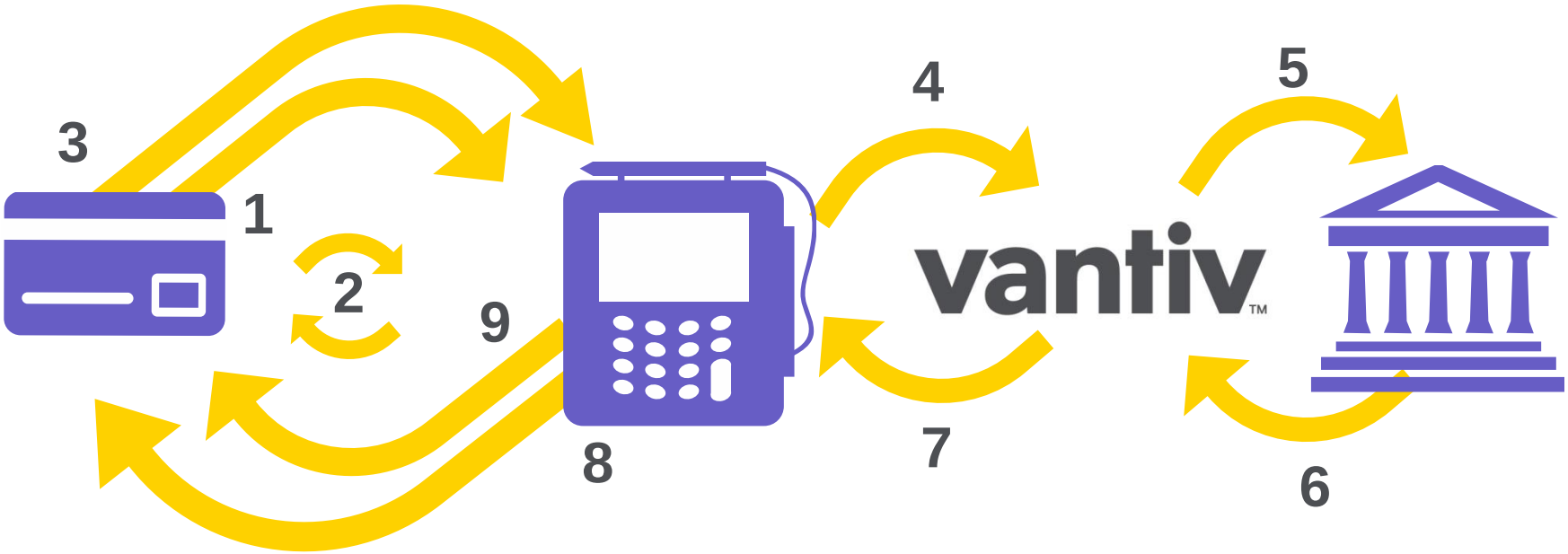
1. Card is swiped through Terminal
2. Authorization Request from Terminal to Acquirer
3. Authorization Request from Acquirer to Issuer
4. Authorization Response from Issuer to Acquirer
5. Authorization Response from Acquirer to Terminal

Difference between Magnetic Stripe Terminal and **EMV Terminal**

- The issuing bank defines the processing rules via parameters on the chip
- The chip on the card processes transactions information and determines how to apply the rules for processing
- The terminal helps enforce the rules on the chip
- If terminal is unable to provide the services requested by the chip, the issuer may set rules that will result in the chip declining the transaction.

vantiv

EMV Terminal and Transaction Flow



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

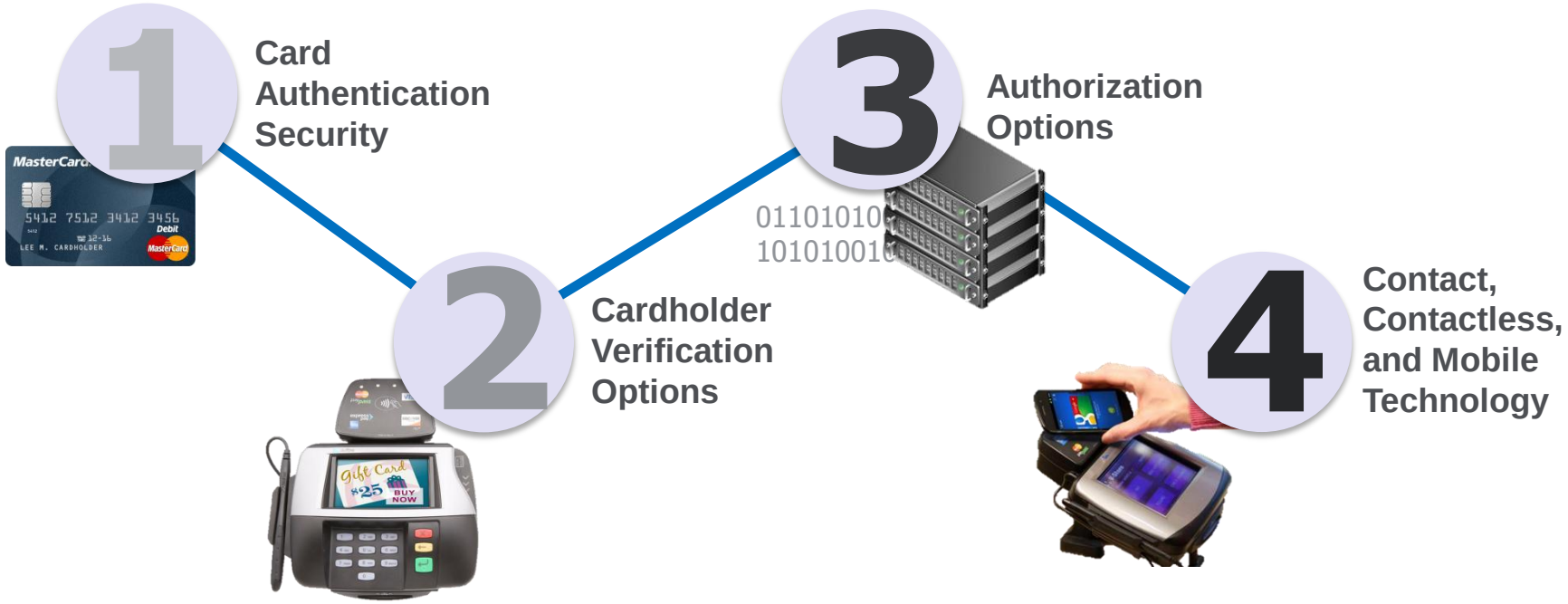
7. Authorization Response from Vantiv to Terminal

8. Completion and script processing. If Issuer approved but card denied transaction a reversal is produced

9. Card is removed from EMV Terminal

vantiv™

EMV Introduces New Security Functions



vantiv

EMV Card Authentication

Online Card Authentication

CARD

ISSUER HOST

1 **Generates an EMV Dynamic Cryptogram**

2 **Host Validates the EMV Dynamic Cryptogram**

Offline Card Authentication (optional)

CARD

TERMINAL

1 **Card provides the terminal a dynamic security certificate**

2 **Terminal validates the dynamic security certificate**

3 **Online Authorization**

vantiv

Cardholder Verification (CVM)

Is the cardholder the right person?

- More than one CVM is supported on a card
- Issuers choose what CVMs to support
- Issuer chooses the priority order of the CVMs

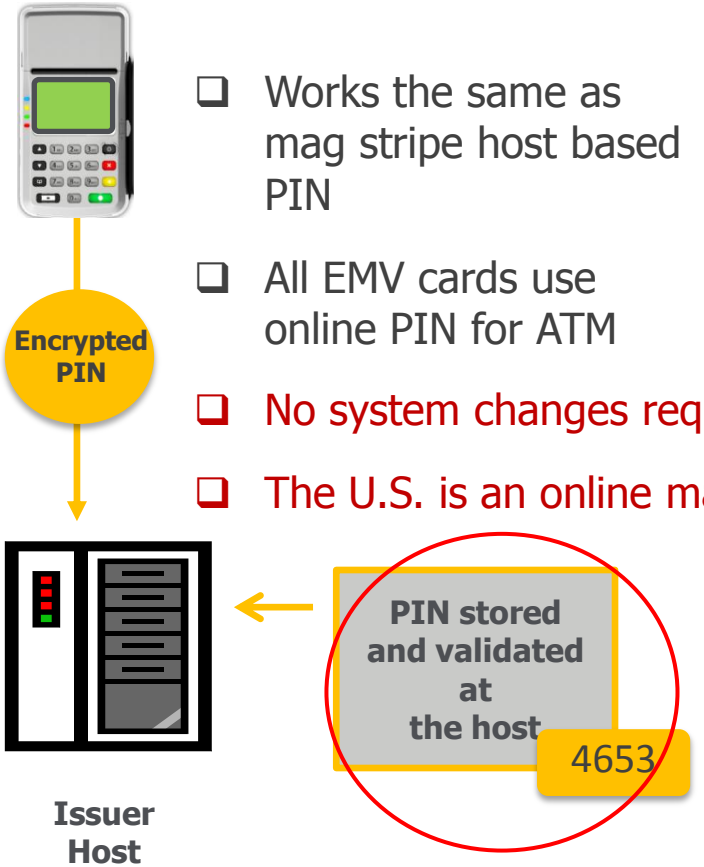
EMV CVM List

- Signature
- Online PIN
- Offline PIN
- No CVM

Online vs. Offline PIN

2

EMV Online PIN



- Works the same as mag stripe host based PIN
- All EMV cards use online PIN for ATM
- No system changes required
- The U.S. is an online market

EMV Offline PIN

- Most Offline PIN transactions go online for authorization
- Changes required:
  - ✓ PIN selection/activation process
  - ✓ Customer PIN Communications
  - ✓ Offline PIN change process
  - ✓ Synchronization with the online PIN
  - ✓ Add ability to send PIN and PIN counter updates to the card

vantiv

EMV Authorization/Approval

3

Issuers can make better authorization decisions with richer risk data provided in an EMV transaction

Transaction approval process

(1) Online Authorization

Works much like a magnetic stripe card transaction

- New EMV data is sent to the host
- Dynamic authentication technology is used
- New risk assessment rules are followed

(2) Offline Authorization (Optional)

The card authorizes the transaction

- No communication with a host system for authorization
- Card contains offline authorization criteria and counters

vantiv

EMV requires certification and validation

Terminal

- EMVCo terminal type approval – hardware and logic testing
- Payment network brand testing for each brand supported

Acquirer

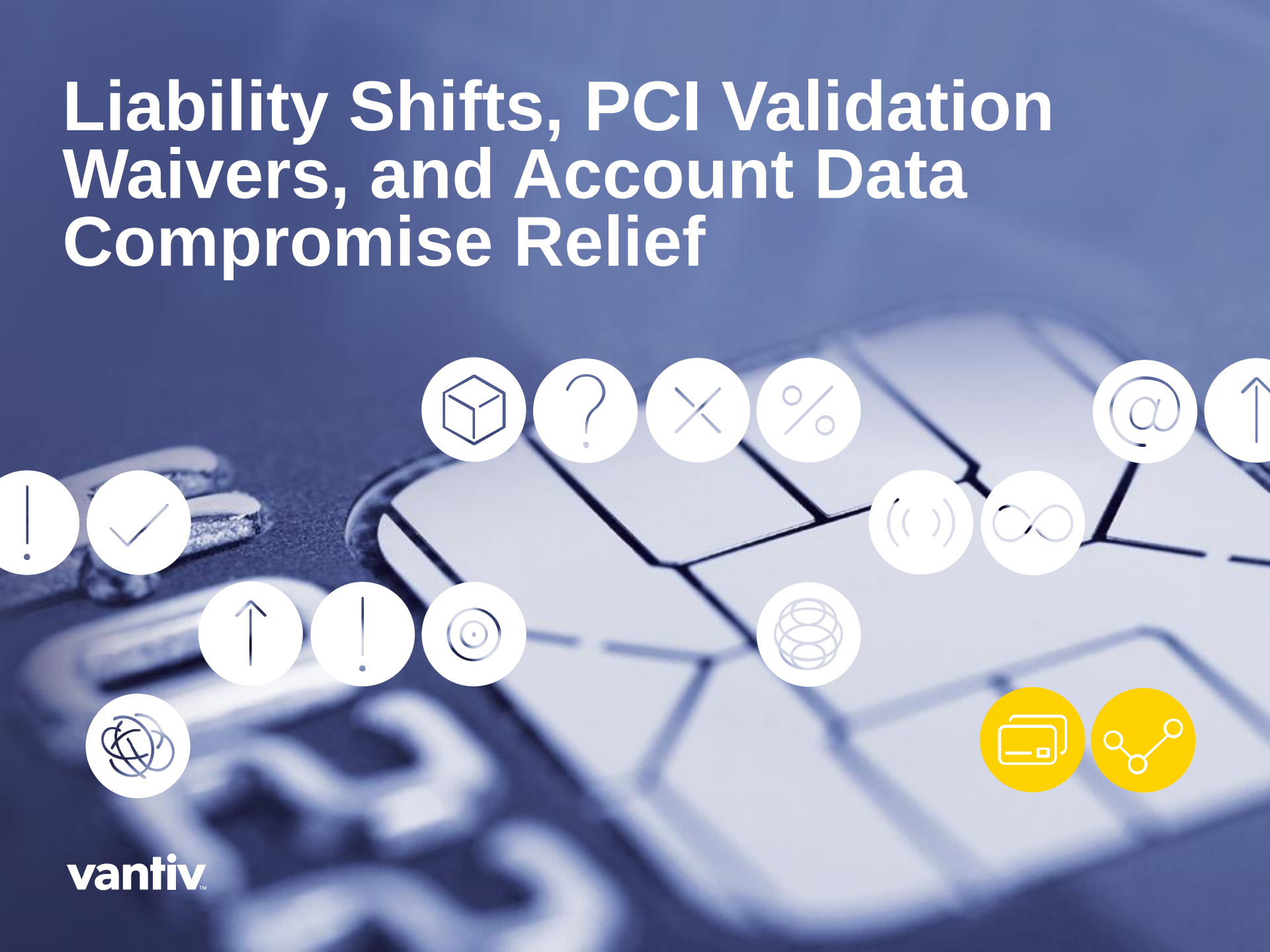
- Processor Network Host Certification
- Host certification already completed by Vantiv

Chip

- EMV Chip application certification (Before they can be sold)
- Card Personalization validation (For each product issued)

vantiv

Liability Shifts, PCI Validation Waivers, and Account Data Compromise Relief



vantiv™

What are the New Rules?

VISA	MasterCard	DISCOVER	AMERICAN EXPRESS
April 2013 Processors must support EMV	**April 2013** Processors must support EMV International ATM liability shift	**April 2013** Processors must support EMV	**April 2013** Processors must support EMV
April 2015 3rd party ATM must support EMV	**October 2015** Liability shift of counterfeit transactions	**October 2015** Liability shift of counterfeit transactions	**October 2015** Liability shift of counterfeit transactions
October 2015 Liability shift of counterfeit transactions	**October 2016** Liability shift for ATM	**October 2017** Liability shift for AFD	**October 2017** Fuel liability shift
October 2017 Liability shift for AFD Liability shift for ATM	**October 2017** Liability shift for AFD		

A Regional Debit Network solution proposal has been released by the EMV Migration Forum

vantiv

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 w/PIN > EMV w/Sig (contact or contactless) > Mag stripe

Visa, however, only states that the party that has not using EMV technology is liable.

AFD merchants have extended timeframe in consideration of cost/complexity.

PCI Validation **Waiver**

PCI Validation waiver (October 2012)

- **Visa, MasterCard**

PCI Validation waiver (October 2013)

- **Discover, American Express**
- **75% of merchant's transactions** must originate from EMV enabled terminals
- Must support both **contact and contactless transactions**
- Exempts eligible merchants from the annual **PCI DSS validation requirement**
  - For MasterCard, "eligible" merchants are Level 1/Level 2 merchants
- All merchants are required to maintain ongoing PCI DSS compliance

MasterCard Account Data **Compromise Relief**

October 2013

- MasterCard will allow for account data compromise relief if 75% of transactions initiated at compliant terminals
- This will be a 50% relief on fines and repayment to issuers for breached accounts

October 2015

- MasterCard will allow for account data compromise relief if 95% of transactions initiated at compliant terminals
- This will be a 100% relief on fines and repayment to issuers for breached accounts

This program only covers the operational recovery and fraud recovery portion of a breached merchant's liability. It does not apply to any investigation costs, remediation expenses, or non-compliance fines.

Start Planning **NOW!**

- Recognize that implementing **EMV** will take time and **can be complex**.
- Begin acquiring and deploying **EMV-capable hardware** that can accept an EMV application download later.
- Consider incorporating **contactless capabilities** now to avoid having to deploy new or additional hardware later on.
- Remember to include **associate training** and **cardholder education** in your plans.

*As of the beginning of **June 2014**, approximately **336 business days** remain until the **Counterfeit Fraud Liability Shift.***

Questions

vantiv™