



# Fiscal Service EMV Education Series

## EMV Basics for Federal Agencies

Fiscal Service / Vantiv  
January 15, 2015

**Disclaimer:** This communication, including any content herein and/or attachments hereto, is provided as a convenience only, does not constitute legal advice and does not create an attorney client relationship. Because of the generality of this communication, the information provided herein may not be applicable in all situations and does not constitute a comprehensive list of issues that could impact your business or agency. As such and to understand how the information in this communication may impact your business or agency, you are encouraged to seek the advice from your legal counsel, compliance and/or other subject matter expert based on the facts and circumstances of your organization's particular situation.

# Agenda

---

- Executive Order 13681
- What is EMV?
- Global Impact of EMV
- How EMV Works
- Card Brand Rules
- EMVCo
- Next Steps
  - › Fiscal Service Deployment Plan



# Executive Order 13681



# Executive Order and Card Acceptance

- Applies to Executive Departments and Agencies
- Point of sale (POS) card acceptance provisions apply to covered agencies directly and to the Treasury through the Fiscal Service's Card Acquiring Service (CAS)
  - › “Standalone terminals” acquired through CAS
  - › Third-party, integrated agency POS systems
- All new terminals acquired by agencies through Treasury *or through alternative means authorized by Treasury* after December 31, 2014 must include hardware necessary to support EMV chip and pin
  - › For existing card terminals acquired through Treasury, a plan must be developed by January 1, 2015 for agencies to install EMV-enabling software



# What is EMV?



# Brief History of Chip Cards

- Chip-based payment cards introduced in the 1980's
  - › High communications costs and unreliable service
  - › Offline processing susceptible to fraud
- Specifications developed country by country
  - › Interoperability issues
- Europay, MasterCard and Visa
  - › Joint effort to develop common specification
  - › EMVCo formed in 1999
    - Now includes Amex, Discover, JCB and China UnionPay



# What is EMV?

- International standard defining interoperability of secure transactions
  - › Introduces **dynamic data** specific to the transaction
  - › **Devalues** transaction data; reducing risk of counterfeit fraud
- World-wide adoption including U.S. neighbors, Canada and Mexico
  - › Effecting U.S. multi-national retailers
- Enabler of future payments types
  - › Contactless, Mobile
- Chip & PIN ≠ EMV



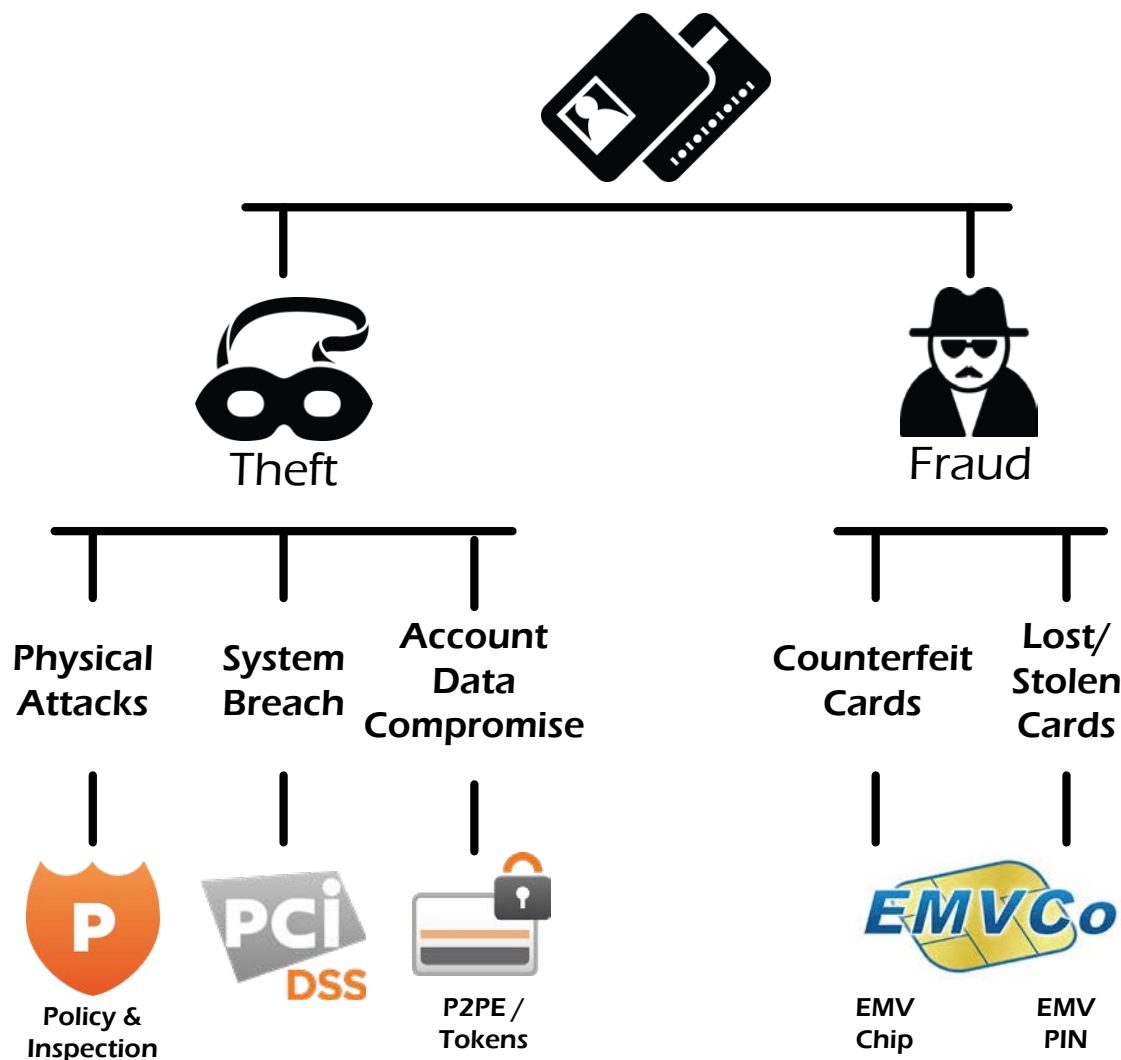


# What is EMV?



- Chip on card uses cryptography to provide security
- Utilizes 2 forms of cryptography
  - › Digital signatures – ensures data is **authentic**
  - › Encryption – ensures data is kept **confidential**
- Digital signature devalues the data
  - › Even if data is intercepted, signature cannot be replicated
- Encryption is only used to protect the PIN
  - › EMV does **not** encrypt all transaction data

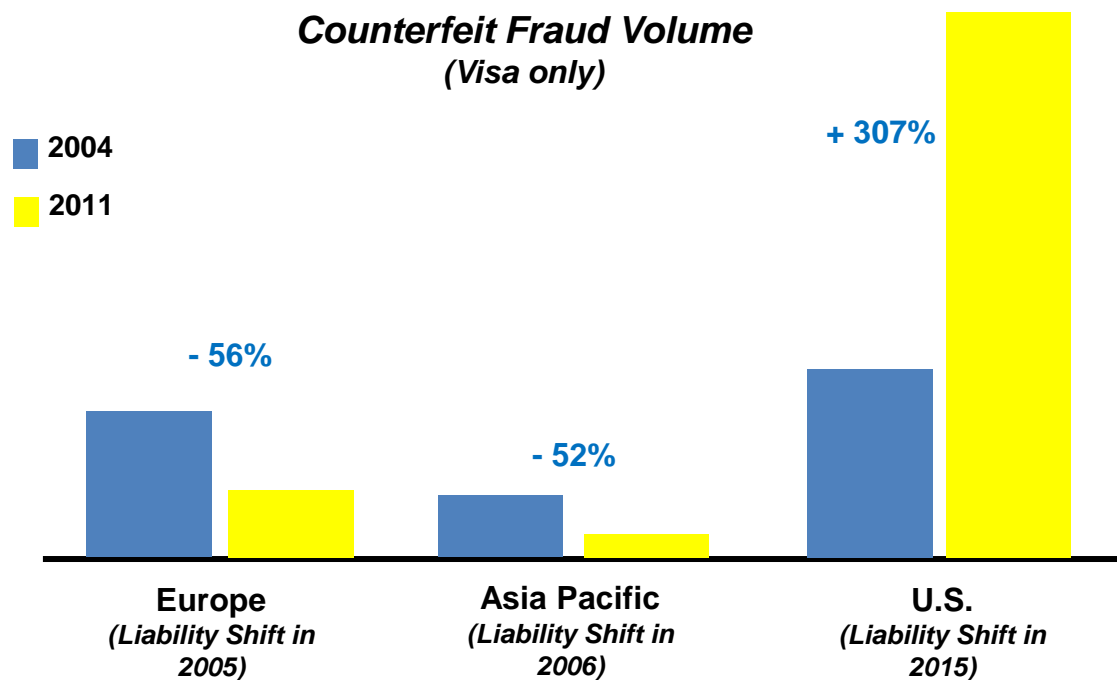
# EMV in the Security Equation



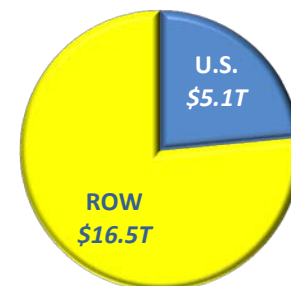
# Global Impact of EMV



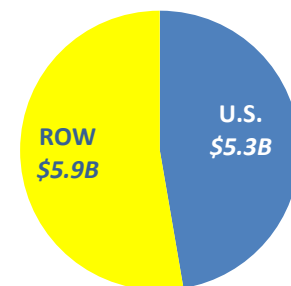
# Global Fraud Trends



**U.S. and Rest  
of World Sales  
Volume  
2012**



**U.S. and Rest  
of World Fraud  
Volume  
2012**



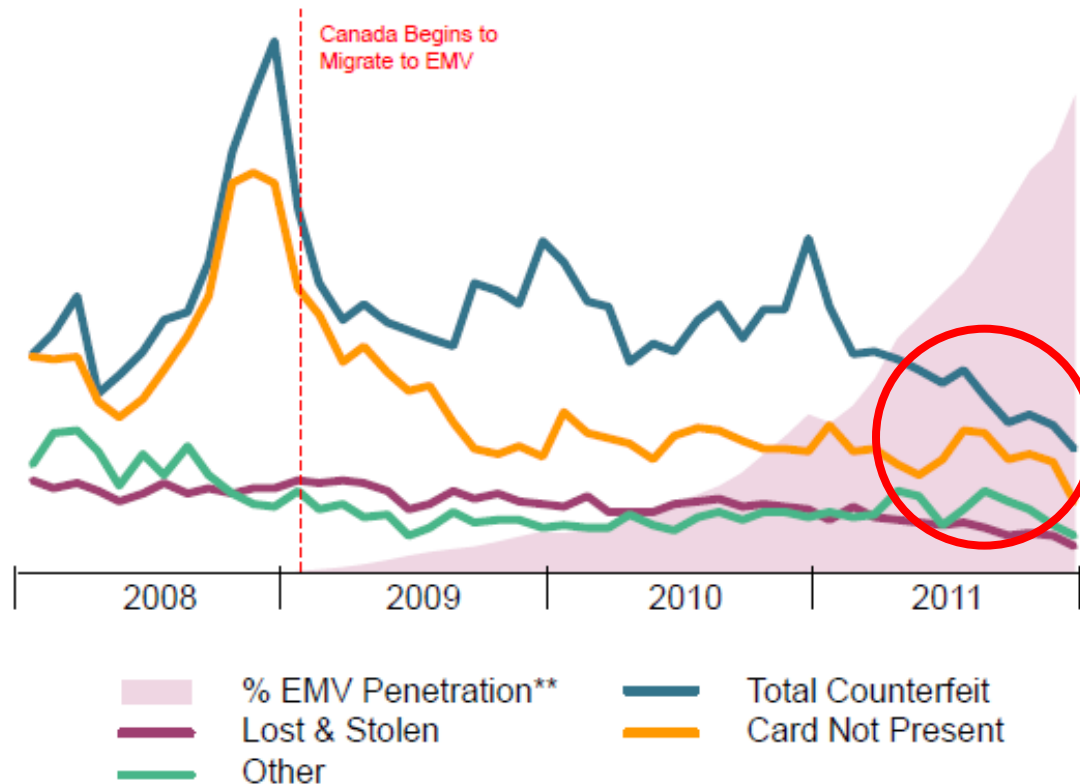
# Canadian Fraud Trends



## Canada Fraud

2008-2010

HOLIDAY  
FRAUD  
PEAKS



2011

HOLIDAY  
FRAUD  
SIGNIFICANTLY  
REDUCED

Source: MasterCard Analysis 2012

\*Cross Border Counterfeit Fraud = Total Counterfeit Fraud – Domestic Fraud

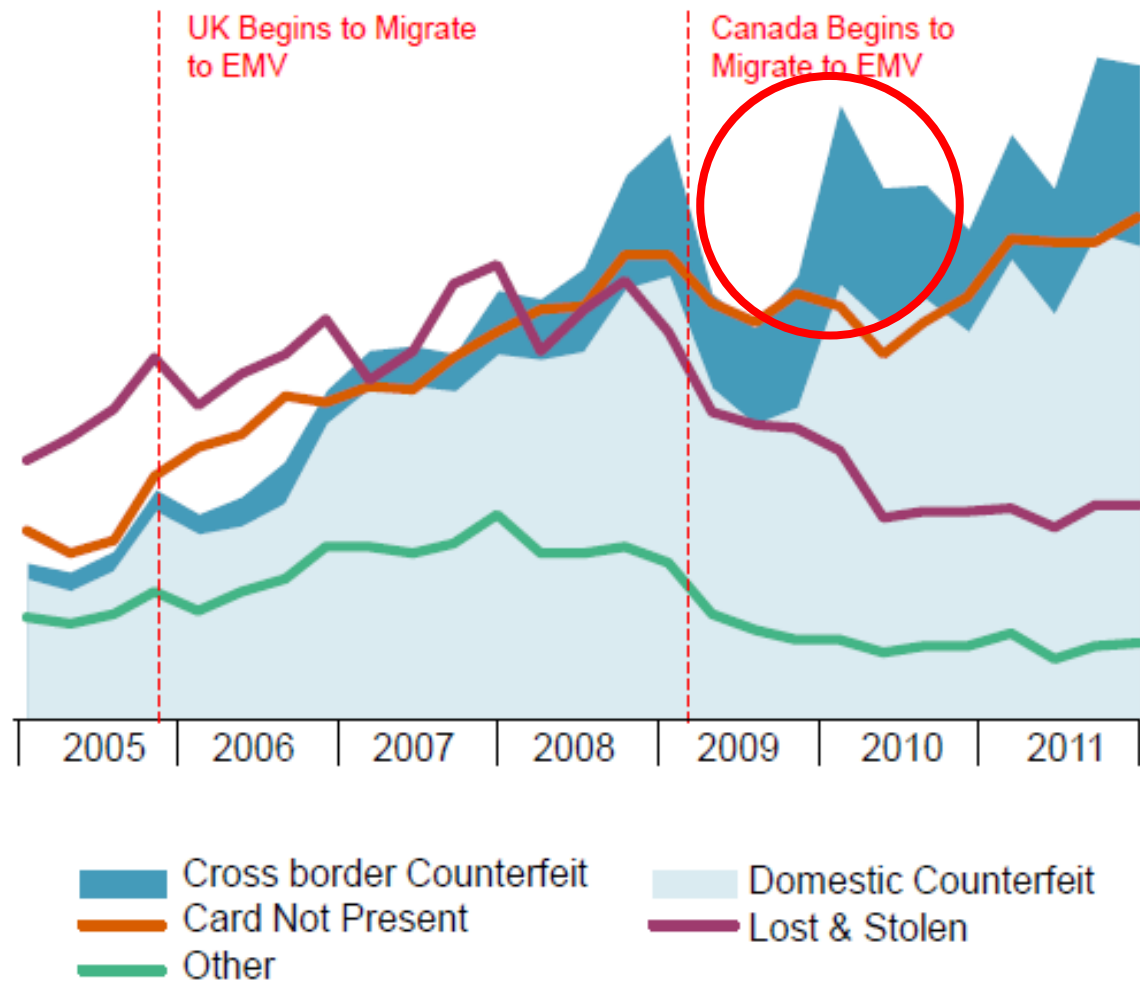
\*\* % face-to-face EMV penetration

# U.S. Fraud Trends



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

**U.S. cross-border counterfeit fraud shows significant growth**



Source: MasterCard Analysis 2012

\*Cross Border Counterfeit Fraud = Total Counterfeit Fraud – Domestic Fraud

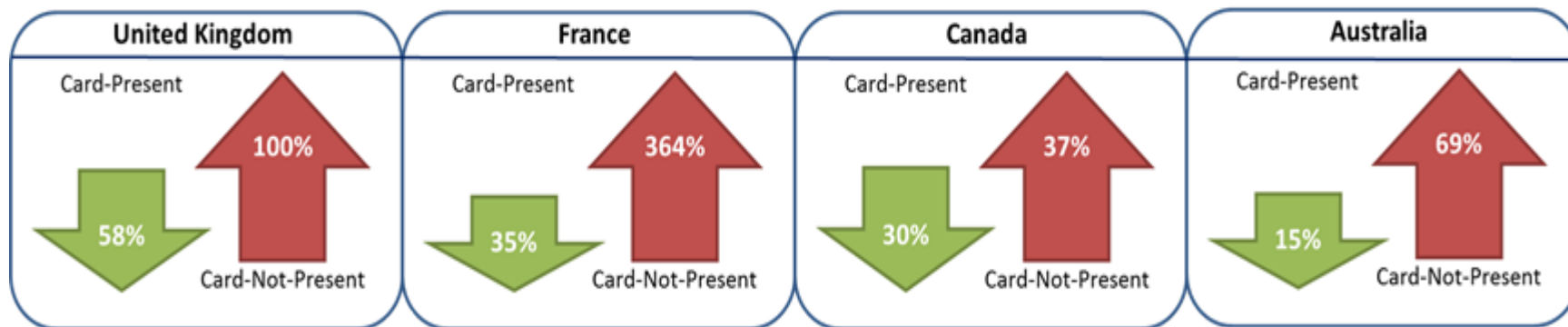
\*\* % face-to-face EMV penetration



# Impact on Card Not Present



## Incidence of Fraud by Channel Following EMV Adoption\*



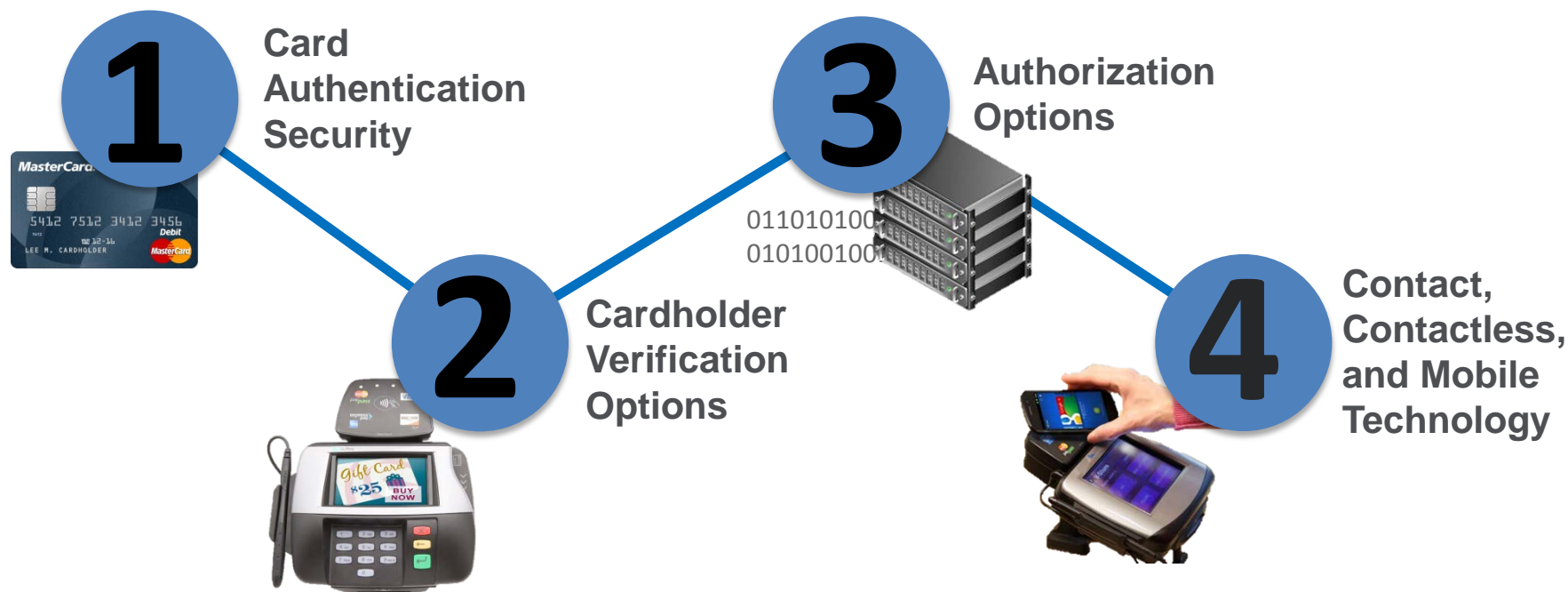
- Increase in Card-Not-Present fraud is driving other solutions
  - › 3-D Secure
  - › Tokenization
  - › Chip authentication devices

\* Retail Payments Risk Forum Working Paper  
Federal Reserve Bank of Atlanta  
January 2012

# How EMV works



# EMV Introduces New Security Functions



# EMV Card Authentication

1

## Online Card Authentication



## Offline Card Authentication (optional)



# Cardholder Verification Method (CVM)

2



Is the cardholder the right person?



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

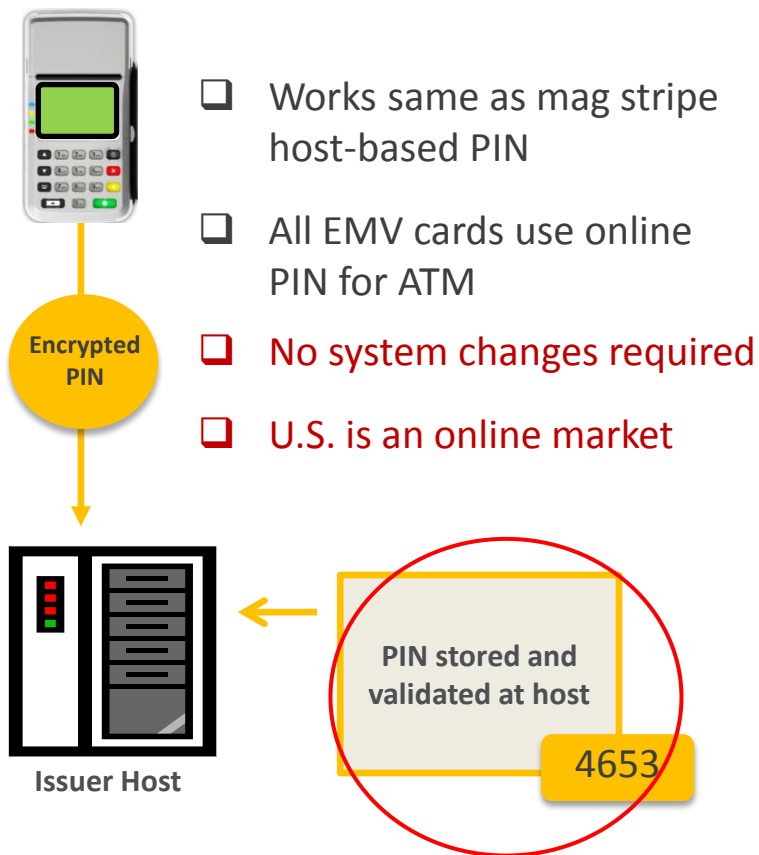
## EMV CVM List

- Signature
- Online PIN
- Offline PIN
- No CVM

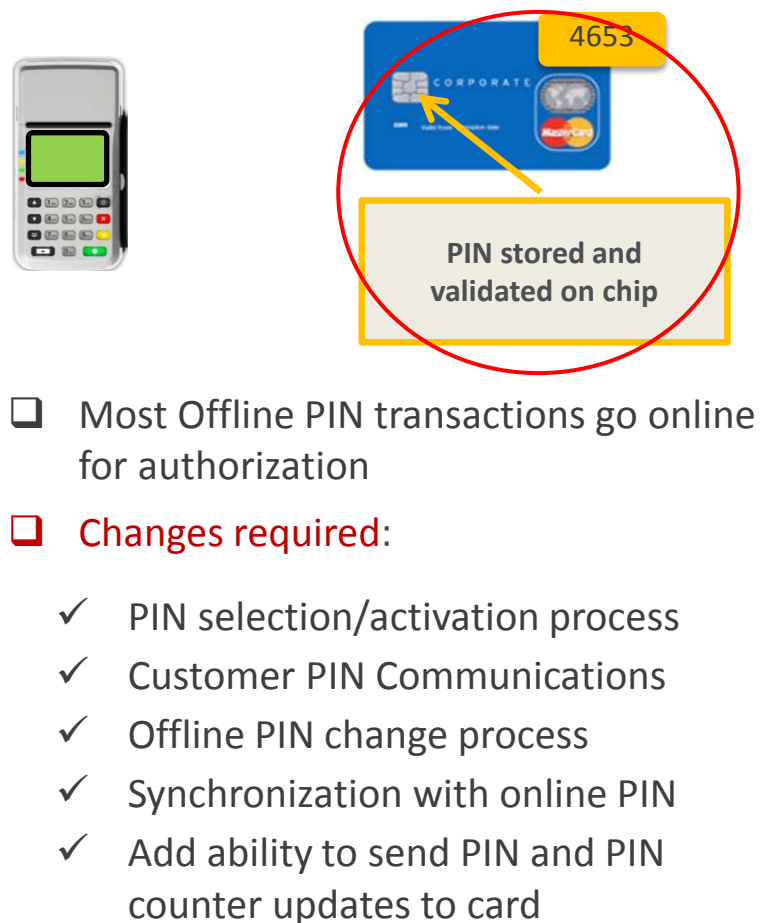
# Online vs. Offline PIN

# 2

## EMV Online PIN



## EMV Offline PIN





# EMV Authorization/Approval

3

Issuers can make better decisions with risk data provided in EMV transactions



Transaction approval process



## (1) Online Authorization

**Works much like magnetic stripe transaction**

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

## (2) Offline Authorization (Optional)

**The card authorizes transaction**

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

# Card Brand Rules



# Brand Roadmaps

**vantiv™**



**DISCOVER®**



**April 2013**

Processors must support EMV

**April 2015**

3rd party ATM must support EMV

**October 2015**

Liability shift of counterfeit transactions

**October 2017**

Liability shift for AFD  
Liability shift for ATM

**April 2013**

Processors must support EMV  
International ATM liability shift

**October 2015**

Liability shift of counterfeit transactions

**October 2016**

Liability shift for ATM

**October 2017**

Liability shift for AFD

**April 2013**

Processors must support EMV

**October 2015**

Liability shift of counterfeit transactions

**October 2017**

Liability shift for AFD

**April 2013**

Processors must support EMV

**October 2015**

Liability shift of counterfeit transactions

**October 2017**

Fuel liability shift

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

# Liability Shift

**vantiv**<sup>TM</sup>

- Counterfeit fraud liability is assigned to least secure party
- Standard rules apply when both are equal
- Inclusion of PIN adds Lost/Stolen shift



**EMV w/PIN > EMV w/Sig > Mag stripe**

**DISCOVER**<sup>®</sup>

- Visa only states that the party not using EMV technology is liable



# EMVCo



**vantiv**<sup>TM</sup>

# EMVCo Initiatives

- EMV Next Generation
  - › Contact/Contactless convergence
  - › Simplified terminal implementations
  - › Cryptography (Elliptical Curve Cryptography)
- Mobile & Mobile Point-of-Sale (mPOS)
  - › Guidance for mPOS development
- Tokenization
  - › Develop spec to support secure/interoperable transactions





# Next Steps






# Next Steps – High Level

- Executing Treasury’s “Plan” for standalone terminals:
  - › Identify and engage agencies/POCs with CAS standalone terminals
  - › Arrange Fiscal Service bulk purchase of replacement terminals
    - Obtain inter-agency agreements to confer agency ownership and reimbursement of the Fiscal Service
  - › Schedule replacement terminal and EMV-enabling software deployment with agencies
- For agencies with third party, integrated solutions:
  - › Contact your solution provider and ascertain when EMV-enabled upgrades will be available
  - › Contact Vantiv to ensure solution is supported

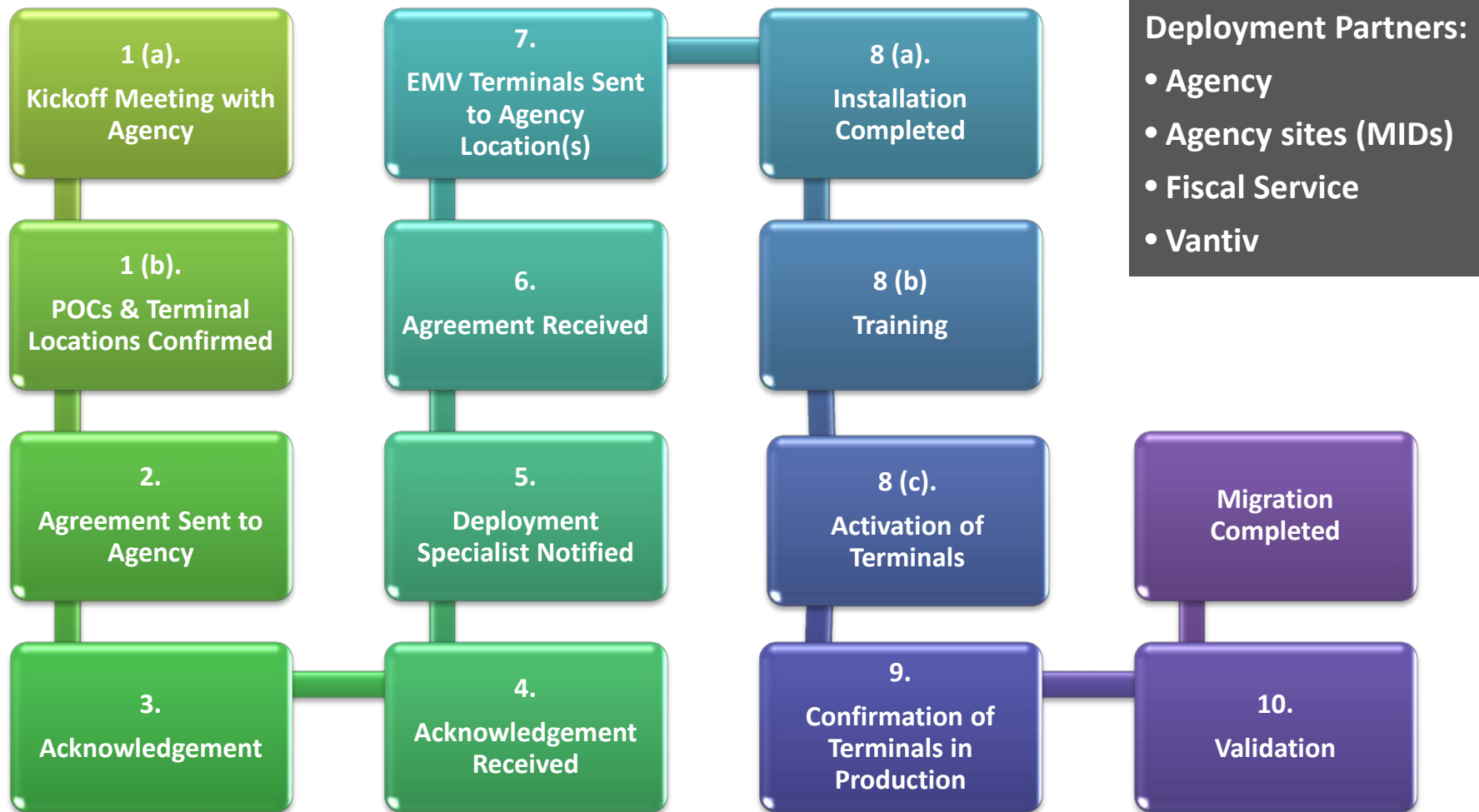
# Next Steps – CAS Rollout

1. Deploy up to 3,200 EMV-enabled replacement terminal packages to 52 CAS Program agencies:
  - › VeriFone Vx520 terminal with Vx820 customer-facing PIN pads
    - ~ 40 wireless terminals (Ingenico iWL255)
  - › Shipped to each agency site, with installation via scheduled teleconference call with Vantiv technical support
2. Deploy up to 400 EMV-enabling software and PIN pads to existing EMV-capable terminal sites:
  - › VeriFone Vx820 and Ingenico iPP220 customer-facing PIN pads
    - ~ 11 wireless terminals
  - › E-mail agency site POCs download instructions once software available

# Next Steps – Deployment Scheduling

TASK 1: Roadmap Development														
TASK	OCT 2014	NOV 2014	DEC 2014	JAN 2015	FEB 2015	MAR 2015	APR 2015	MAY 2015	JUN 2015	JUL 2015	AUG 2015	SEP 2015	OCT 2015	NOTES
Identify EMV-Enabled Terminal Requirements														1
Identify Existing EMV-Capable <u>And</u> Non-Compliant Terminal Sites/MIDs														2
Identify Third-Party System ISV/VAR Agency Sites/MIDs														2, 11
Confirm Site/MID POC Information, Terminal Needs														3
TASK 2: Standalone Terminal Upgrade and Replacement														
TASK	OCT 2014	NOV 2014	DEC 2014	JAN 2015	FEB 2015	MAR 2015	APR 2015	MAY 2015	JUNE 2015	JULY 2015	AUG 2015	SEPT 2015	OCT 2015	NOTES
Inform Agencies Of Executive Order / EMV Compliance Needs														4
Complete EMV-Enabling Software Testing, Training And Certification														5
Source And Acquire Replacement Terminals And PIN Pads														6
Deploy Enabling Software To EMV-Compliant Terminals/Sites														7
Deploy PIN pads To EMV-Compliant Terminals/Sites														7
Deploy Replacement Terminals To Non-EMV Compliant Sites														8
Validate EMV Terminals Installed And Functioning														9
Contact/Escalate Non-Responsive Agency Sites														10
NOTES														
<ol style="list-style-type: none"> <li>1. Standalone terminals will be EMV chip &amp; PIN –enabled, with Near Field Communications (NFC) capability.</li> <li>2. Sites/MIDs identified by FS and Vantiv through CAS program management.</li> <li>3. Will be identified by Fiscal Service outreach and CAS program agency contact.</li> <li>4. Initial communication with Executive Order and EMV information distributed to all CAS program agency contacts in 11/2014. Conference call with ISV/VAR agencies held 12/1/2014; Webinar for all agencies planned for 1/15/2015.</li> <li>5. Vantiv working with terminal manufacturers Ingenico and VeriFone to develop EMV–enabling software to integrate with Vantiv-supported CAS Program standalone terminals.</li> <li>6. Acquisition of replacement standalone terminals and PIN pads via bulk purchase planned. Hardware/software will be acquired by Fiscal Service with ownership transferred through inter-agency agreements to CAS program agencies upon deployment.</li> <li>7. Approximately 400 CAS standalone terminals (Ingenico and VeriFone) are EMV-capable but require an enabling software download and addition of a PIN pad to become Executive Order-compliant and meet CAS program needs.</li> <li>8. See Note 1. VeriFone Vx520 terminals with Vx820 customer facing PIN pads have been selected to meet CAS program agency needs. Total terminals ~3,200.</li> <li>9. CAS will contact agency sites that have not activated replacement terminals or software downloads.</li> <li>10. Agency sites that have not responded to validate POC information for deployment or activated EMV terminals will be contacted by Fiscal Service escalation if still non-responsive after repeated attempts.</li> <li>11. Vantiv will work with CAS program agencies and their ISV/VAR providers to understand EMV upgrade and certification requirements. Under the Executive Order, these card acceptance solutions are the responsibility of each agency and not the Fiscal Service.</li> </ol>														

# Deployment – 10-Step Engagement



# Contacts

- **Primary Contact**

Ian Macoy

Director, Settlement Services Division

(202) 874-6835

[Ian.Macoy@fiscal.treasury.gov](mailto:Ian.Macoy@fiscal.treasury.gov)

- **Secondary Contact**

Lynette Newby

CAS Program Specialist

(202) 874-9208

[Lynette.Newby@fiscal.treasury.gov](mailto:Lynette.Newby@fiscal.treasury.gov)

- **Additional Contacts**

Card Acquiring Service

[CardAcquiringService@fiscal.treasury.gov](mailto:CardAcquiringService@fiscal.treasury.gov)

Agency Relationship Management

[ARM@fiscal.treasury.gov](mailto:ARM@fiscal.treasury.gov)

Vantiv Customer Support

[rmtreasury@vantiv.com](mailto:rmtreasury@vantiv.com)

(866) 914-0558