



CAS 101

A High-Level Introduction to the Card Acquiring Service

Ian Macoy, Director, Settlement Services Division

Eric Cofer, Vantiv

June 8-9, 2016

Presentation Outline

- CAS Program 101
 - Program Highlights
 - Key Program Metrics
 - Getting Started With CAS
 - Key Terminology
 - CASA Process
- Vantiv Report on Current Card Issues
- Q&A

CAS Program 101

What is CAS? CAS is a Fiscal Service federal program that provides merchant acquirer services to federal agencies.

Services: Enables agency acceptance of credit, debit, electronic benefit transfer (EBT), and branded stored value (e.g. gift, etc.) cards

Acceptance Points:

- Traditional standalone point-of-sale (POS) terminals
- Integrated POS systems (e.g. electronic cash registers)
- Vantiv Accept (mobile)
- Kiosks
- Internet-based software applications (e.g. pay.gov)

Financial Agent: Fifth Third Bank

- Merchant Acquirer: Vantiv

Program Highlights

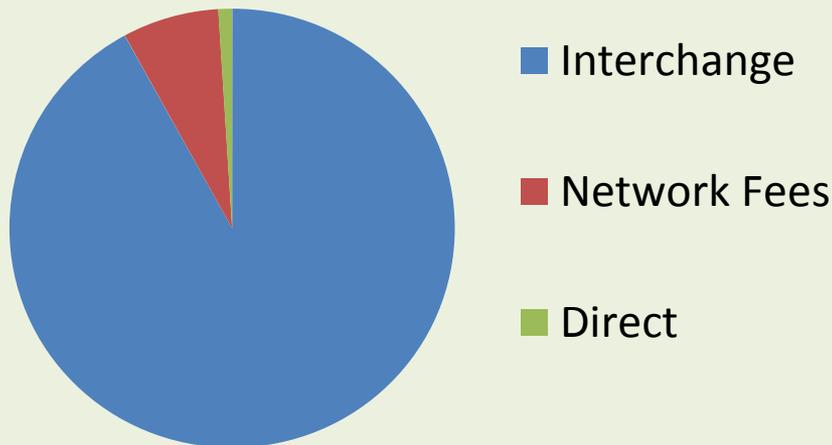
- Collected 12 billion in sales in FY 2015 and currently on target to exceed this sales volume in FY 2016
- Currently partners with over 105 agencies (excluding pay.gov), bureaus and administrations across program, representing over 800 chains (distinct business lines) and 8,500 merchant identification numbers (business locations)
- Completed EMV Phase I in October 2015
 - Over 3500 standalone terminals replaced with “Chip and Pin” or retired
- Completed EMV Phase II in May 2016
 - Received a survey response rate of over 90%
- Identified a strategy for tokenization and point to point encryption for agency partners
 - Fiscal Service will bear the cost associated with the initial implementation and monthly maintenance/usage fees for program partners
 - Technology will improve data security infrastructure
 - Strategy is tentatively planned to be implemented during FY 2017
- CAS is evaluating various cost reduction strategies for program

Key Metrics*

~10,000 Acceptance points

- 38% Terminals
- 40% Software
- 21% Pay.gov

2015 CAS Program Costs



How much is collected?

Transaction Volume (dollars):

- \$11.8 billion collected
 - Integrated POS System & Standalone Terminals: 49%
 - Pay.gov: 51%

Transaction Count:

- 127.6 million transactions
 - POS: 74%
 - Pay.gov: 26%

Program Costs:

- \$159+ million in interchange fees (avg./CC transaction \$1.80)
- \$13 million+ in network fees (avg./CC transaction \$0.14)

*NOTE: As of Fiscal Yearend 2015

Getting Started With CAS

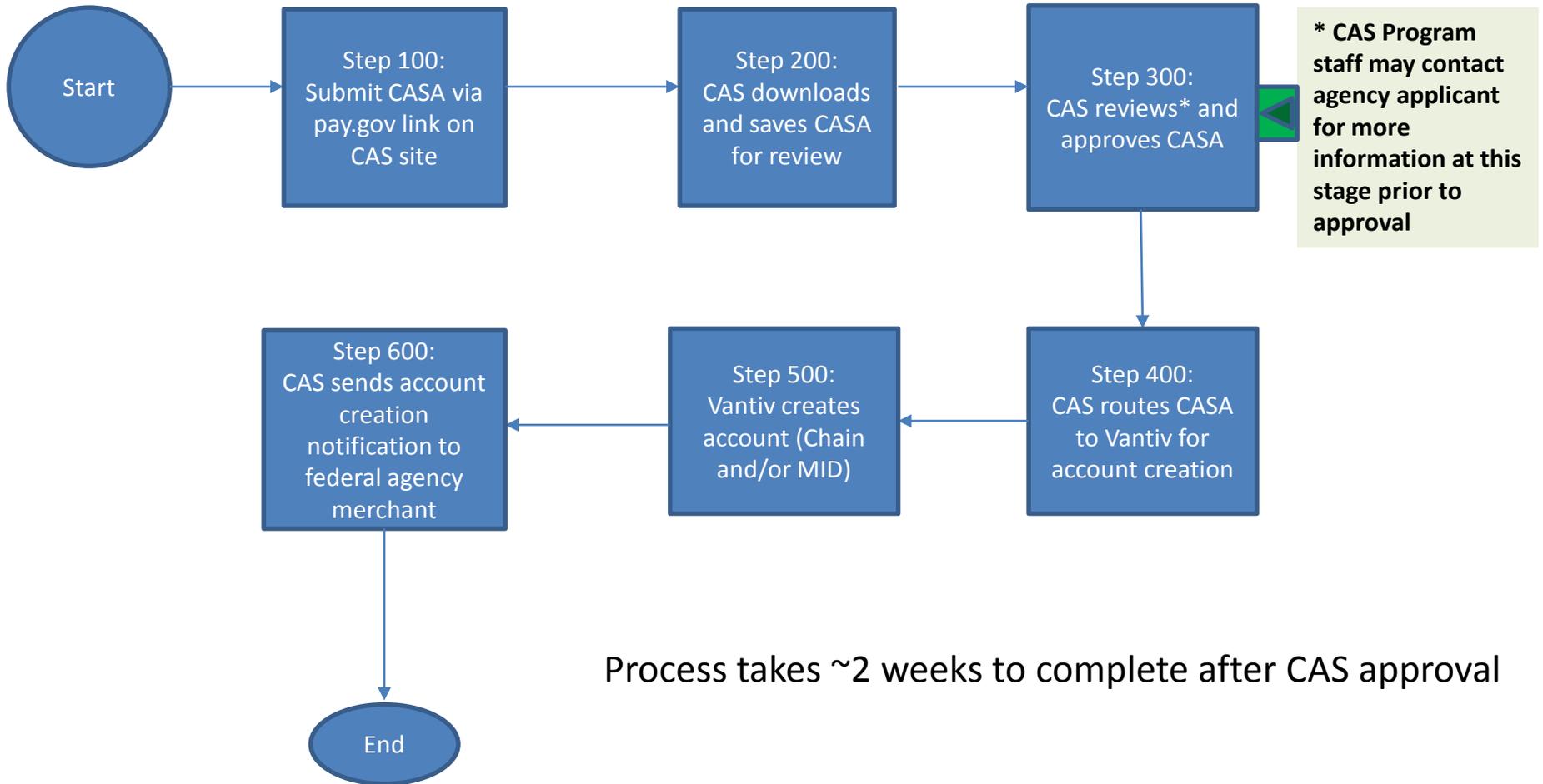
Preliminary Steps:

- Determine your account creation strategy (e.g. new chain and/or new Merchant ID)
- Determine your estimated card volumes (may need to work with subject matter experts or benchmark other similar organizations to determine projections)
- Estimate your largest itemized card transaction (e.g. largest card individual transaction is estimated to be \$1000)
- Complete and submit CAS Application (CASA) online at Pay.gov (see Pay.gov or CAS website for more info)

Key Terminology

- **Merchant ID (MID)** - unique designator assigned by acquirer to reflect location of processing
- **Terminal ID (TID)** - unique designator assigned by acquirer to reflect each terminal
- **Chain Number** - alphanumeric designator assigned by acquirer to reflect unique channel of processing
- **Division Number** - additional 3 digit value assigned under a chain to designate unique lines of accounting

CASA Process (Happy Path)



Vantiv Report: Current Issues in Card

- PCI updates
- Visa eliminating CVV2 in lieu of imprint
- Visa allowing merchants to discontinue chip transactions.
- MasterCard new 2 series BIN
- EMV
 - Stats on merchant penetration, # cards in market, loss stats
 - Current litigation and other implementation issues

Self-Assessment Questionnaires

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels.</i>
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Applicable only to e-commerce channels.</i>
B	Merchants using only: <ul style="list-style-type: none"> • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
D	<p>SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.</p> <p>SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.</p>

* New for PCI DSS v3.0

New Visa Small Merchant Mandates

<https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-faq.pdf>

- **(NEW)** Effective 31 March 2016, acquirers must communicate to all Level 4 merchants that beginning 31 January 2017, they must use only Payment Card Industry (PCI)-certified Qualified Integrators and Reseller (QIR) professionals for point-of-sale (POS) application and terminal installation and integration.
- Effective 31 January 2017, acquirers must ensure that Level 4 merchants using third parties for POS application and terminal installation and integration engage only PCI QIR professionals.
- Effective 31 January 2017, acquirers must ensure Level 4 merchants annually validate PCI DSS compliance or participate in the Technology Innovation Program (TIP).

Note that single-use terminals without Internet connectivity are considered low risk and may be excluded from these requirements.

To qualify for TIP and receive its benefits, a merchant must meet the following criteria:

- Confirm that sensitive authentication data (i.e., the full contents of magnetic stripe, CVV2 and PIN data) are not stored subsequent to transaction authorization, as defined in the PCI DSS.
- Ensure that at least 75 percent of all transactions originate through one of the following secure acceptance channels:
 - Enabled and operating EMV chip-reading terminals
 - OR
 - A [PCI SSC-validated P2PE solution](#)

Helpful PCI Resources

- **PCI Security Standards Council – www.pcisecuritystandards.org**
 - PCI DSS, PA DSS, PTS, & P2PE Standards
 - Downloadable Self Assessment Questionnaires
 - List of ASVs, QSAs, PFIs, PA QSAs, QIRs, etc.
 - List of PA DSS Validated Payment Applications, validated P2PE solutions, validated PTS devices
 - Searchable FAQ Tool
 - PCI Supporting Documents
- **Visa® CISP website – www.visa.com/cisp**
 - Merchant & Service Provider Levels Defined
 - List of CISP Compliant Service Providers
 - Important Alerts, Bulletins and Webinar
- **MasterCard® SDP website – www.mastercard.com/sdp**
 - Merchant & Service Provider Levels Defined
 - List of CISP Compliant Service Providers
 - PCI 360 Merchant Education Program – on demand educational webinars

Fraud Update - Malware

Cyber criminals continue to develop ***malware*** targeting point-of-sales systems. Vantiv observed an increase in the number of data compromises that were tied to ***malware***.

Install application whitelisting on Point of Sale systems.

- In addition to anti-virus and anti-malware security, application whitelisting programs are designed to only allow known and trusted executables to be installed and operate. This technology makes it much more difficult to introduce malware onto POS systems.

Keep operating system patch levels up to date.

- For Windows, this means ensuring Windows Update is functioning and automatically applying monthly security patches. For non-supported operating systems like Windows XP, there should be a plan to migrate to a current operating system as soon as possible.

Fraud Update - Malware

Control the Windows Administrator account. Make privilege escalation difficult.

- Assign a strong password for all accounts on the POS system.
- Create a unique local Administrator password for every POS system.
- Do not allow users to be local Administrators on a POS system.
- Change passwords frequently across the enterprise (at least 90 days).
- Do not share passwords.

Closely monitor activity on Point of Sale systems.

- Be aware of anomalous behavior and investigate all suspicious activity on the POS. Signs may include:
 - New files created in c:\Windows\Installer directory
 - Communication established to external IP addresses over HTTP
 - POS application malfunction (application crashes)
 - Data transfer services (email, FTP) transiting data outside the network

Fraud Updates - Skimming

Prevention Through Device Inventory Management

- PCI DSS Requirement 9.9 – ensure implementation of security controls to protect POS devices from tampering and substitution.
 - Maintain a list of devices including serial number
 - Keep a list of devices by location (store) and placement within a store (kiosk, retail counter, etc...)
 - Train personnel on suspicious behavior.
 - Verify identity of any third party servicing the devices.

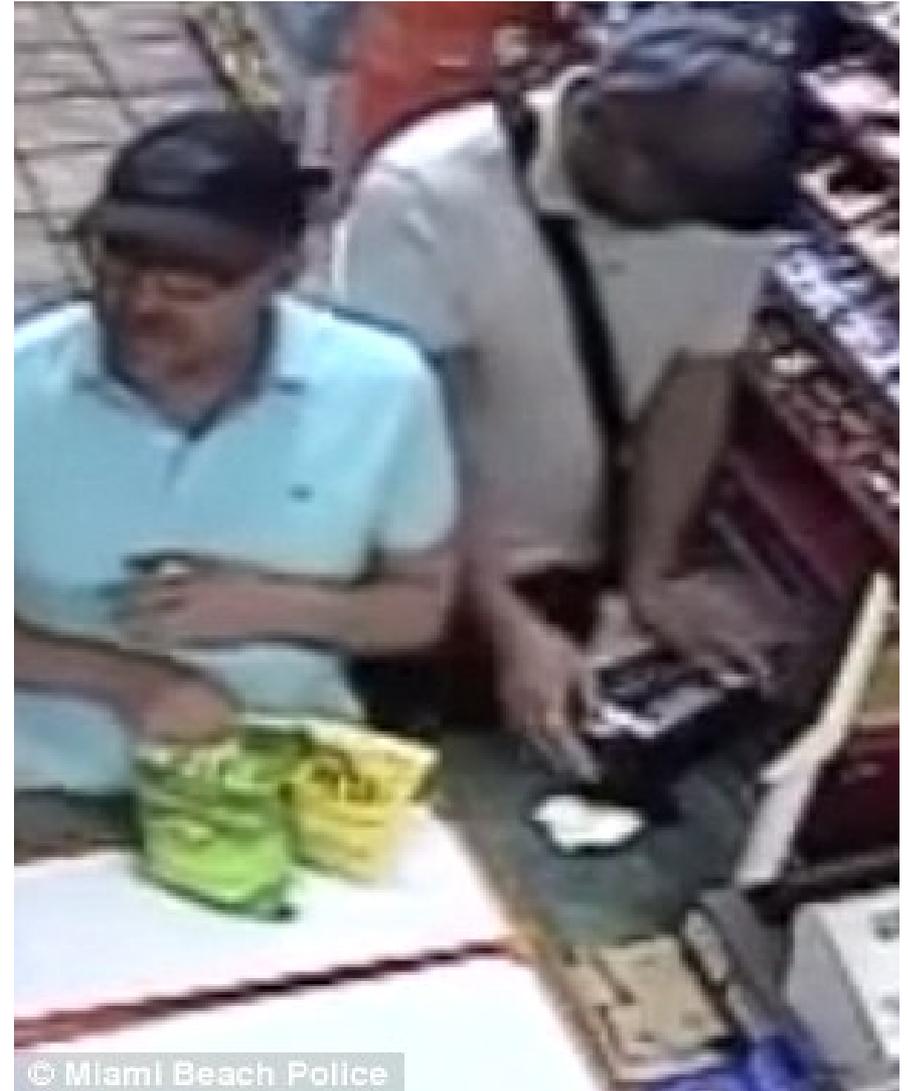
Fraud Updates - Skimming

- Physical Inspection of POS Devices
 - Implement security controls to inspect devices 2 times a day at random times.
 - Physically examine the device – a good grab and pull works well!
- Device Recovery Response
 - If a skimming device is found, try not to handle it as you may destroy evidence.
 - Activate your account data compromise plan, which should include notifying local law enforcement, the FBI, Vantiv, and Fiscal Service.

Skimming in Action



Skimming in Action



Visa's U.S. EMV Migration Report – March 2016



Credit

- **265 million EMV chip cards issued;** 10% increase from previous month
- **131 million EMV credit cards issued;** 7% increase from previous month



Debit

- **133.9 million EMV debit cards issued;** 13% increase from previous month
- **7.8% of ATMs** in the U.S. accept chip transactions



Acquirers / Terminals

- **Domestic EMV PV increased 18%** from \$15.7 billion in previous month to \$18.5 billion

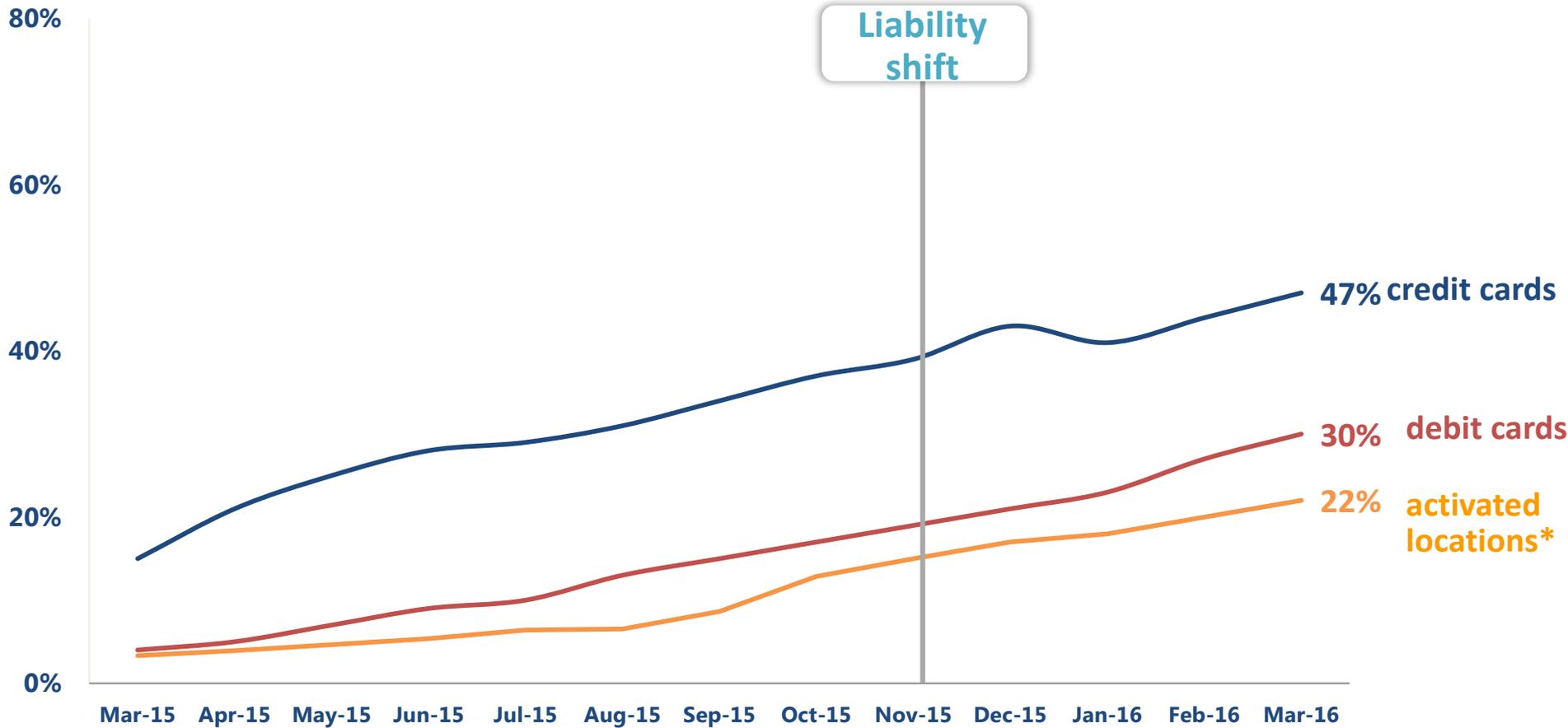


Merchants

- **1,025 thousand EMV chip activated merchant locations,** 11% increase from previous month

U.S. EMV chip migration

EMV chip as % of U.S. total



*Total Face to Face merchant locations is 4.6M. Previous calculations used the total number of merchant locations which included non Face to Face locations, and totaled 8.0M.

Speeding Up EMV At the Point of Sale

Visa Quick Chip and MasterCard M/Chip Fast include the following benefits:

- Reduced transaction wait times through streamlined transaction processing
- Parallel processing, which results in shortened card-in-terminal times, so customers can remove their cards sooner.
- Improved customer perception of wait time without changes to current terminal prompts, minimizing cardholder friction at the end of the transaction.
- Easy Implementation. Quick Chip does not require any changes to standard EMV processing or to the chip card, and no additional EMV testing or certification.

Processing options:

Option 1 - Remove Card Before Authorization Response - Generate the EMV chip cryptogram based on the final transaction amount, but allow the card to be removed before the authorization response.

Option 2 - Generate Cryptogram Without Final Sale Amount - Generate the EMV chip cryptogram before the final sale amount is known and prompt the cardholder to remove the card. The final amount will be included in the non-EMV transaction data.

EMV Litigation

Walmart is currently suing Visa over their honor their all card rules.

- The key issue is merchant routing choice verse cardholder routing choice for debit cards.

B&R Supermarket Inc. and Grove Liquors LLC, two Florida retailers, are suing seven card networks, including Visa, MasterCard and American Express; 10 banks, including JPMorgan Chase, Capital One and Wells Fargo; and EMVCo.

- The issue here is the liability shift and merchant ability to meet the dates created to implement EMV before the liability shift.
- Also at issue merchants are no paying the costs of fraud that were typically an Issuer expense. Merchant interchange has not been adjusted comparably.
- Seeking class status

Network Update: MasterCard 2 Series BIN

The Program: MasterCard is adding new primary account **BIN ranges 222100-272099** to be processed in the same manner as existing range 510000-559999.

The Change: The payments ecosystem must be ready to support the 2-Series MasterCard BINs by **October 14, 2016**. All Vantiv platforms will support the MasterCard 2-Series BIN range.

The Impact: Merchants must be able to accept the new MasterCard BIN range in both card-present and card-not present payment acceptance channels.

The Timing: October 14, 2016 – Payments ecosystem to be ready to support the new 2-Series BIN. January 2017 – Issuers will be assigned the new 2-Series BINs, merchants should be prepared to accept the new BIN as cards begin to appear in the market shortly thereafter. Merchants identified as not being able to support the new 2-Series BIN may be subject to noncompliance fines.

Contact Information

Primary Contact:

Richard Yancy

CAS Program Manager

Richard.Yancy@fiscal.treasury.gov

202-874-5217

CAS Online:

https://www.fiscal.treasury.gov/fsservices/gov/rvnColl/crdAcqgServ/rvnColl_cas.htm