



EMV OVERVIEW

July 2014

- EMV Overview
- EMV Industry Announcements
- EMV Transaction Differences, What to Expect
- Solution Decisions
- Market Certification Considerations
- Questions

What is EMV?

- Global Standard for chip cards to facilitate electronic payment transaction
- Born out of transit payment programs in Europe
- Protects against duplicate card fraud



EMV is not...

- Chip and PIN – PIN as a cardholder validation method is only **one** implementation option
- A Silver Bullet for PCI Compliance – PAN data is still presented in the clear and valuable for card not present transactions
- Cure All for Chargebacks – The programs put in place will help with duplicate card fraud chargebacks, but will not impact others



WHO IS EMVCO?

- EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa

ROLE OF EMVCO

- Owns, manages, and maintains the global payment industry specifications to define interoperability requirements between chip based payment cards and acceptance terminals
- Administers the testing and approval process for both chip payment cards and chip acceptance terminals
- EMVCo is **not** responsible for specific card brand certifications
- EMVCo maintains specifications for both contact and contactless payment schemes
- EMV Contactless specification published to define a common contactless interface to be used by the card brands
- Currently each card brand uses its own proprietary application
 - MasterCard M/Chip, Visa qVSDC
 - Applications are similar, both follow EMVCo standards

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribean	401M	49.2%	5.6M	78.5%
Asia Pacific	372M	26.7%	5M	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 States†				
TOTALS	1.62B	44.9%	23.8M	75.7%

* 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.

† Figures do not include data from the United States.

U.S. INCENTIVE DATES

PCI Relief

Visa
• October 2012

MasterCard
• October 2012
• October 2013

AMEX
• October 2013

Discover
• October 2013

Acquirer Support of EMV

Visa
• April 2013

MasterCard
• April 2013

AMEX
• April 2013

Discover
• April 2013

Fraud Liability Shift

Visa
• October 2015

MasterCard
• October 2015

AMEX
• October 2015

Discover
• October 2015

AFD Compliance

Visa
• October 2017

MasterCard
• October 2017

AMEX
• October 2017

Discover
• October 2017



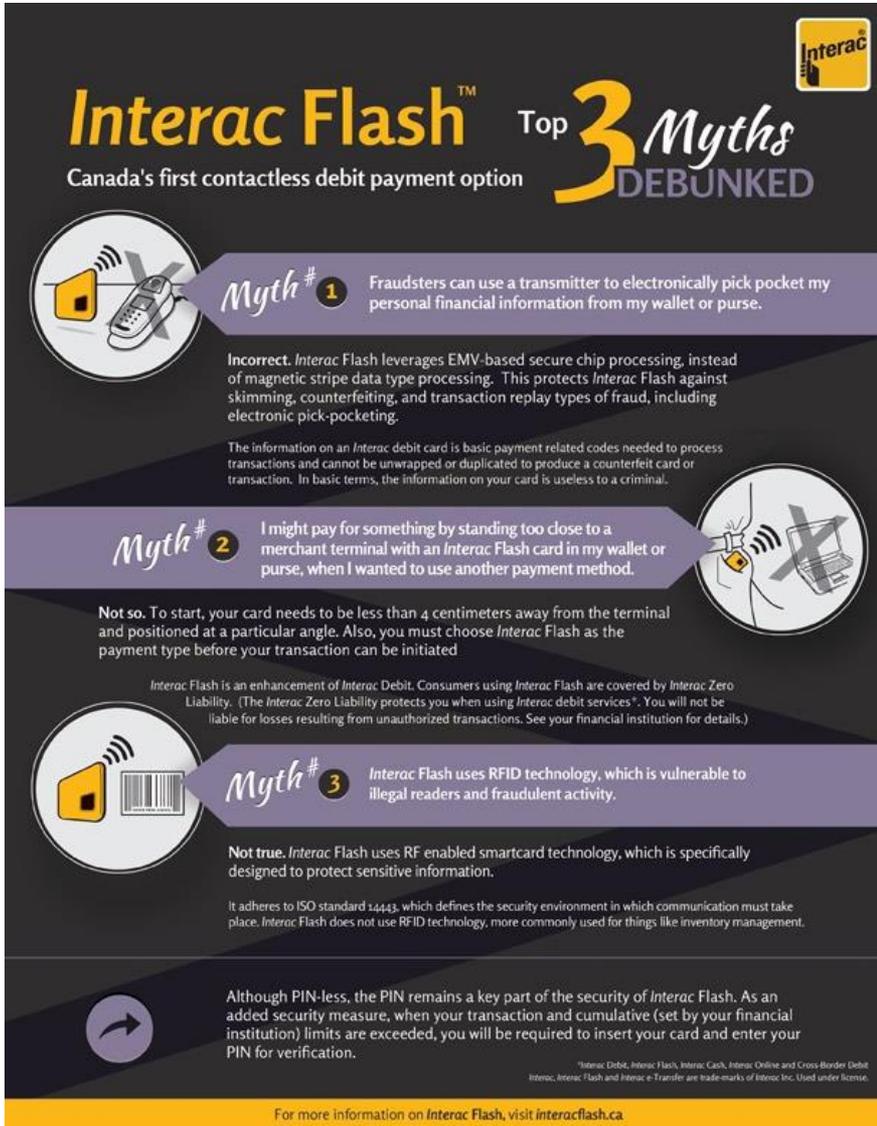
Today

- Devices are deployed, and in some cases, not touched for years
- Merchants are reluctant to be reprogrammed, to give time for the activity
- Infrastructure (dial lines, ..etc) not setup to handle large downloads

Tomorrow, EMV Challenges (Contact and Contactless)

- EMV components, kernels for contact and contactless can and will change
- New cards issued with new functionalities happen, require downloads to accept the card
- Interoperability will be impacted if devices are not kept up to speed
- Contactless software components, EMV and for NFC initiatives, will require updates and changes to remain field-ready for new cards

- Statistics from the EMV roll-out in Canada.
 - Very similar to the experience in other countries including the UK.
 - 49% of installed terminals supported EMV (smart card readers) by the liability shift date (October 2015 for US)
 - 79% terminals installed one year later supported EMV
 - Just over 90% of terminals installed 2 years later supported EMV
 - It took 6 years to get to 90% of all transactions to be EMV transactions
 - All Canadian cards still have Mag-Stripes
 - Only 28% of UK Amex EMV cards also have contactless support
- (Note: Canada has 8 issuing institutions, the US has 9,500)**



Interac Flash™ Top 3 Myths **DEBUNKED**
Canada's first contactless debit payment option

Myth # 1 Fraudsters can use a transmitter to electronically pick pocket my personal financial information from my wallet or purse.

Incorrect. Interac Flash leverages EMV-based secure chip processing, instead of magnetic stripe data type processing. This protects Interac Flash against skimming, counterfeiting, and transaction replay types of fraud, including electronic pick-pocketing.

The information on an Interac debit card is basic payment related codes needed to process transactions and cannot be unwrapped or duplicated to produce a counterfeit card or transaction. In basic terms, the information on your card is useless to a criminal.

Myth # 2 I might pay for something by standing too close to a merchant terminal with an Interac Flash card in my wallet or purse, when I wanted to use another payment method.

Not so. To start, your card needs to be less than 4 centimeters away from the terminal and positioned at a particular angle. Also, you must choose Interac Flash as the payment type before your transaction can be initiated.

Interac Flash is an enhancement of Interac Debit. Consumers using Interac Flash are covered by Interac Zero Liability. (The Interac Zero Liability protects you when using Interac debit services*. You will not be liable for losses resulting from unauthorized transactions. See your financial institution for details.)

Myth # 3 Interac Flash uses RFID technology, which is vulnerable to illegal readers and fraudulent activity.

Not true. Interac Flash uses RF enabled smartcard technology, which is specifically designed to protect sensitive information.

It adheres to ISO standard 14443, which defines the security environment in which communication must take place. Interac Flash does not use RFID technology, more commonly used for things like inventory management.

Although PIN-less, the PIN remains a key part of the security of Interac Flash. As an added security measure, when your transaction and cumulative (set by your financial institution) limits are exceeded, you will be required to insert your card and enter your PIN for verification.

*Interac Debit, Interac Flash, Interac Cash, Interac Online and Cross Border Debit, Interac, Interac Flash and Interac e-Transfer are trade marks of Interac Inc. Used under license.

For more information on Interac Flash, visit interacflash.ca

Interac debit card fraud skimming losses plummet to lowest level on record. Losses down 73 per cent in last three years—Interac Association reported today that Interac debit card fraud losses, as a result of skimming, are the lowest on record since 2003—decreasing to \$38.5 million in 2012 from a high of \$142 million in 2009. This represents 0.012 per cent of domestic Interac debit card volume and the lowest volume of fraud losses since data were recorded in 2003. Further, the number of cardholders reimbursed fell to 93,800 in 2012 from 238,000 in 2009. Cardholders are protected from losses under the Interac Zero Liability Policy.

MERCHANT QUESTIONS ABOUT EMV

- **What to do for the October 2015 liability shift?**
Action is required now to be prepared
- **How will EMV affect my current POS?**
Updates required to POS / Processing
- **How will EMV affect the checkout experience?**
Changes user experience and transaction flow
- **What is this about Certifications?**
Any change that is made requires new certification
- **How long does certification take?**
Updates require 4-6 months
- **How much does certification cost?**
Ranges from \$7500 to \$25000 per processor, per update
- **EMV Test Cases & Test Kits**
\$7,500 per kit & 800 test cases versus 200 for current payment processes



POTENTIAL IMPACT TO USDA PROGRAMS

Merchants are Spending to Upgrade Systems

- Merchants are upgrading devices, software, encryption and more to meet the October 2015 deadline
- Merchants may not be excited to upgrade multiple eWIC programs due to EMV recertification costs
- A day may come when EMV cards are the preferred tender (magstripe becomes the new “paper check”). What is the SNAP and WIC strategy?

Fraud Migration and Security

- With EMV cards reducing fraud, fraud could migrate to other programs
- Merchants may require added security from SNAP, WIC programs or shift liability

EBT and WIC devices and services

- Commercial terminals will require EMV readers. Added expense for merchants with new commercial model
- Payment processors may add transaction fees to support “at risk” transactions or request a waiver.
- Retailers are spending \$\$\$ to implement End to End encryption for payment transactions. Currently need to have “BIN exclusion” for SNAP. This exposes their systems.

QUESTIONS?