

The nuvei logo is displayed in white lowercase letters on a teal square background. The letters are bold and modern, with a small dot over the 'i'.

Payment Technology Network

EMV

Corporate Sales Training



Agenda

- Introduction to EMV
- The 4 W's of EMV
- EMV Technology & Security
- Equipment Options
- Fraud Statistics
- Liability Shift



EMV: What is it?

EMV is a standard for globally interoperable, secure payments.

The key element of EMV involves including dynamic digital data in every transaction. This makes these types of transactions extremely secure and reduces the risk of fraud.¹

The distinguishing feature of EMV chip transactions is that the payment application is resident in a secure chip that is embedded in a plastic payment card (often referred to as a chip card or smart card), a personal device such as a mobile phone or other form factors such as wristbands or watches.

The secure chip provides three key elements:

- It can perform processing functions.
- It is able to store confidential information very securely.
- It can perform cryptographic processing.²

THE 4 W'S OF EMV

WHAT

EMV refers to the global specifications that ensure interoperability of chip cards, POS terminals and ATMS for chip based transactions. Originally referred to the founding organizations from 1994—Europay, MasterCard and Visa—today the EMV trademark is owned by all of the equity owners of EMVCo: American Express, JCB, Discover, MasterCard, UnionPay, and Visa.

WHEN

Many parts of the world have already implemented EMV and seen considerable reduction of fraud at the point-of-sale. The US is now in the process of migrating to EMV and the card brands are making a push for it by instituting deadlines including the fraud liability shift of October 2015.

WHO

The players affected by EMV include the card issuers, consumers and merchants.

- ISSUERS will need to ensure their customers are equipped with EMV cards and know how to use them.
- CARDHOLDERS will need to adapt to a new way of paying via contact or contactless EMV chip technology.
- MERCHANTS will need to upgrade their POS terminals to be able to process EMV cards and understand how they work.

WHY

EMV provides better protection from fraudulent activity such as skimming and the creation of counterfeit cards. In parts of the world where EMV has been implemented, there has been a significant reduction in incidents of fraud at the point-of-sale.

MAGNETIC STRIPE CARDS

Magnetic Stripe technology hasn't changed significantly since the 1960's.

Vulnerabilities of Magnetic Stripe cards include:



- Skimming
- Shoulder Surfing
(Watching cardholder PIN input)
- E-Commerce/CNP Fraud
(Static data transmission)
- Counterfeiting



SECURITY

What Makes EMV More Secure?

Cardholder data is more secure on a chip-embedded card that utilizes dynamic authentication, than on a static mag-stripe card. With EMV, both the terminal and the card play important roles in the authentication process which is not the case when using magnetic stripe technology.

MAGNETIC STRIPE	EMV
	
<ul style="list-style-type: none">• Cardholder data resides on a magnetic stripe on the back of the card.• Data is static and can be easily skimmed and used to create counterfeit cards.• The terminal performs all the processing and applies the rules for payment.	<ul style="list-style-type: none">• Cardholder data resides in a secure chip embedded in a plastic payment card or personal device such as a mobile phone.• Dynamic values exist within the chip itself that, when verified by the point-of-sale device, ensure the authenticity of the card.• Fraudsters need physical access to the card and even then, the card itself is extremely difficult to clone, thus limiting any potential damage.

CARD INSURANCE TYPES

Chip & PIN / Chip & Signature

There are 2 types of cards being issued with EMV, Chip & PIN and Chip & Signature.

The choice is driven by the card issuer. The U.S. favors chip & signature currently.

Chip and PIN requires the cardholder to enter a four digit PIN (could be more digits), which must correspond to the chip embedded in their card. Chip and Signature requires the cardholder to sign in order to authorize the transaction.

While chip and PIN is the more secure option, issuing banks in the US will begin by providing their customers with **Chip and signature** Cards. An EMV terminal will still be required to read the chip so requirements for merchants remain unchanged by this.

CARD INSURANCE TYPES

Chip & PIN / Chip & Signature

An excerpt from 'EMV: Where the Merchants Are' published by TransactionTrends

“Sources from various merchant groups say the use of chip and signature instead of chip and PIN continues to be a hot-button topic for merchants. The point of contention centers on the decision to not require PIN in the United States. **Chip cards and PINs each address a different type of fraud**, according to SellSafeInfo.org, a consumer-facing website of the ETA. **With or without a PIN, chip cards prevent counterfeit fraud while the PIN prevents lost and stolen fraud.** In 2014, counterfeit fraud accounted for \$3 billion in losses, while lost/stolen fraud accounted for \$800 million, according to data from Aite Group reported by Statista.

While proponents of chip and PIN EMV cards contend that most of the world uses that system instead of chip and signature, Drieling says that is a misconception. “When we look at EMV adoption around the globe, it’s almost evenly split between PIN and sig,” he contends.

But reissuing EMV chip and signature cards as chip and PIN doesn’t strike Drieling as likely because of the expense. The issuers say they chose signature because **some merchants don’t have PIN pads and because some consumers might find entering a PIN too much of a change from signing their name.**”

TRANSACTION FLOW

How It Works: Typical EMV Transaction Flow

EMV-enabled payment terminals and peripherals are able to read and process the information either by direct contact with the chip, or by close proximity through contactless (NFC) technology.

CONTACT EMV TRANSACTION

A contact EMV transaction consists of the following steps:

1. Cardholder inserts the chip into the chip reader.
2. Cardholder follows prompts which may include: Language selection, card brand selection, confirmation of amount or PIN entry.
3. Result of the transaction is displayed a receipt may be printed.
4. Cardholder removed the chip card.
5. In some cases a signature may be required to authorize the transaction.

CONTACTLESS EMV TRANSACTION

A contactless EMV transaction consists of the following steps:

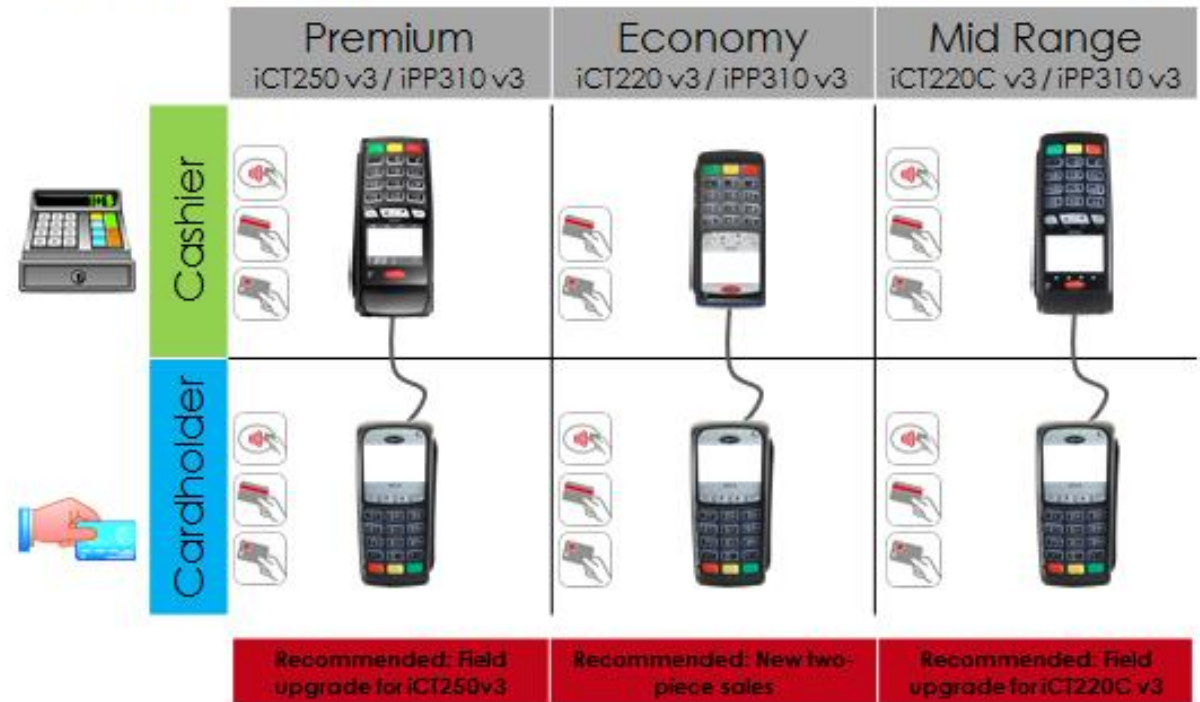
1. Cardholder taps or waves the card or smart device over the terminal.
2. No signature or PIN is required for purchases under the merchant's set limit.
3. For purchases over the merchant's set limit, the customer may be asked to sign, swipe or insert their card.
4. A receipt is printed and the transaction is complete.

EQUIPMENT OPTIONS

Equipment Options – Ingenico

The design of EMV payments is to encourage the payment card to stay with the consumer during the sale. In order to accomplish this, merchants need to direct the terminal over to the consumer or have a peripheral device, such as a PIN pad available to the consumer that is NFC and EMV enabled.

Countertop / PIN pad Two-Piece Strategy



EQUIPMENT OPTIONS

Equipment Options – Verifone

The design of EMV payments is to encourage the payment card to stay with the consumer during the sale. In order to accomplish this, merchants need to direct the terminal over to the consumer or have a peripheral device, such as a PIN pad available to the consumer that is NFC and EMV enabled.



Verifone Vx520 Terminal
EMV & NFC Compliant
(\$318.10 U.S. Cost)



Verifone Vx805 PIN pad
EMV & NFC Compliant
(\$147 U.S. cost including encryption & shipping)

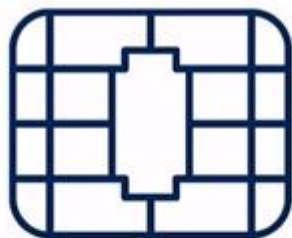
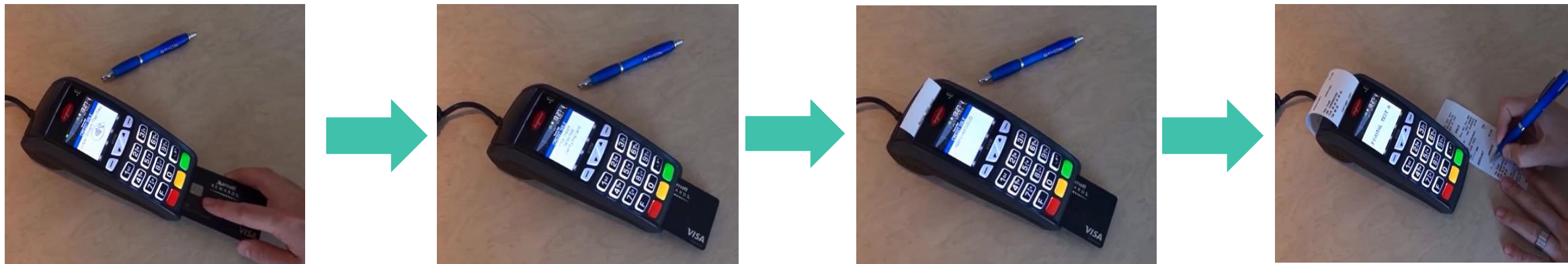
MERCHANT TIPS

Merchant Tips (Restaurant/Retail with Tip)

TSYS has released an application update which supports a tip line on the receipt. Prior to this release, EMV applications were tip at the time of sale only, which caused the merchant to hand the terminal or peripheral device to the cardholder to enter the tip if desired.



TRANSACTION FLOW



EMV "Chip Card"
Transaction

- Cardholder may be prompted to enter PIN, three digit code or sign for the transaction.
- Card stays in the terminal dip reader for the full cycle of the transaction, up until the receipt prints.

TRANSACTION DATA COMPARISON

EMV Transaction: DYNAMIC

00 A4 04 00 0E - 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 6F 24 84 0E 31 50 41 59 2E 53 59
53 2E 44 44 46 30 31 A5 12 88 01 01 5F 2D 08 65 73 65 6E 66 72 64 65 9F 11 01 01 90 00 00 B2
01 0C 00 70 2A 61 28 4F 07 A0 00 00 00 04 10 10 50 0A 4D 43 52 44 43 52 45 44 49 54 87 01 01
9F 12 0D 43 52 45 44 49 54 4F 44 45 4D 43 52 44 90 00 00 B2 02 0C 00 No data6A 83 00 A4 04 00
07 - A0 00 00 00 04 10 10 6F 32 84 07 A0 00 00 00 04 10 10 A5 27 87 01 01 9F 38 12 9F 1A 02 9F
33 03 9F 40 05 9F 1B 04 9F 09 02 9F 35 01 5F 2D 08 65 73 65 6E 66 72 64 65 9F 11 01 01 90 00
80 A8 00 00 13 - 83 11 08 40 E0 B0 C0 D0 00 F0 A0 00 00 00 00 00 01 22 80 0E 5C 00 08 01 01
00 10 01 03 01 18 01 03 00 90 00 00 B2 01 0C 00 70 3E 5F 20 0F 4D 43 52 44 20 46 55 4E 43 54 49
4F 4E 41 4C 57 11 51 05 10 51 05 10 51 00 D1 01 22 01 01 23 45 67 89 9F 1F 16 30 31 30 32 30 33
30 34 30 35 30 36 30 37 30 38 30 39 30 41 30 42 90 00 00 B2 01 14 00 70 0E 5A 08 51 05 10 51 05
10 51 00 5F 34 01 01 90 00 00 B2 02 14 00 70 4C 8C 17 95 05 9B 02 9F 02 06 9F 03 06 9F 1A 02 5F
2A 02 9A 03 9C 01 9F 37 04 8D 19 95 05 9B 02 8A 02 9F 02 06 9F 03 06 9F 1A 02 5F 2A 02 9A 03 9C
01 9F 37 04 9F 0E 05 00 00 00 00 9F 0F 05 F0 20 04 98 00 9F 0D 05 F0 20 04 00 00 90 00 00 B2
03 14 00 70 39 5F 25 03 95 07 01 5F 24 03 10 12 31 5F 28 02 08 40 9F 07 02 FF C0 8E 12 00 00 00
00 00 00 00 00 41 03 42 03 5E 03 43 03 1F 00 9F 08 02 00 8C 5F 30 02 02 01 9F 42 02 08 40
90 00 00 B2 01 1C 00 70 65 8F 01 97 90 60 24 0E 0E A6 D2 1E 65 52 B2 ED 3F AD C2 F1 D2 80 D1 AD
91 3E 62 2E 2C 35 21 AA DF 2A 47 B3 AC F6 6B 67 1D 4B 12 36 81 9A D1 B1 FA 9F A6 AC DE 38 66 5B
6B DE 53 C3 80 A1 53 16 9A BA AB 94 83 90 2F B7 63 E9 EA A7 AB 27 8A 5D 39 D3 A5 0E 15 98 B8 4C
22 13 9D 43 A7 48 6F 71 AA 0E C3 90 2D 26 90 00 00 B2 02 1C 00 70 1A 9F 32 01 03 92 14 CF B8 D4
88 5D 96 09 67 17 9F 98 2D 42 CE 54 EC C2 05 46 83 90 00 00 B2 03 1C 00 70 52 93 50 11 0B B9 DF
2D 21 98 19 06 B2 9A 30 14 11 F9 FA 60 CF 49 4D BA BA BF 54 B1 79 7C 9C 4B 5D 99 B5 E6 7A B7 30
49 E7 71 FC 5F DC 23 E5 83 50 B7 81 00 53 24 D3 1D C8 7A D0 FB F6 36 73 38 08 05 6D 66 07 46 32
71 1E 7C BF 14 07 37 96 E1 B6 0D 4D 90 00 80 CA 9F 17 00 9F 17 01 03 90 00 00 20 00 80 08 - 24
12 34 FF FF FF FF FF No data 90 00 80 AE 80 00 1F - 40 80 00 80 00 C8 00 00 00 00 00 10 00 00 00
00 00 00 00 08 40 08 40 06 01 30 00 90 86 27 40 77 1E 9F 27 01 80 9F 36 02 45 67 9F 26 08 CA 3C
A2 03 D2 6C 67 7B 9F 10 07 06 01 1A 03 90 00 00 90 00 80 AE 00 00 21 - 40 80 00 80 00 E8 00 35
31 00 00 00 00 10 00 00 00 00 00 00 08 40 08 40 06 01 30 00 90 86 27 40 77 1E 9F 27 01 00 9F
36 02 45 67 9F 26 08 01 B7 8D 05 86 AC E4 F8 9F 10 07 06 01 1A 03 60 00 00 90 00

Non EMV Transaction STATIC

B370261765230537^71171
VALUEDCUSTOMER00007^1309101091099116
370261765230537=130910109109911600007

EMV AROUND THE WORLD

HOW DOES EMV SECURITY WORK?

Because the cryptogram changes with every transaction, even if the card data is stolen, the information can't be used to create counterfeit cards because the cryptogram would have already "expired."



EMV AROUND THE WORLD

EMV DEPLOYMENT MAP

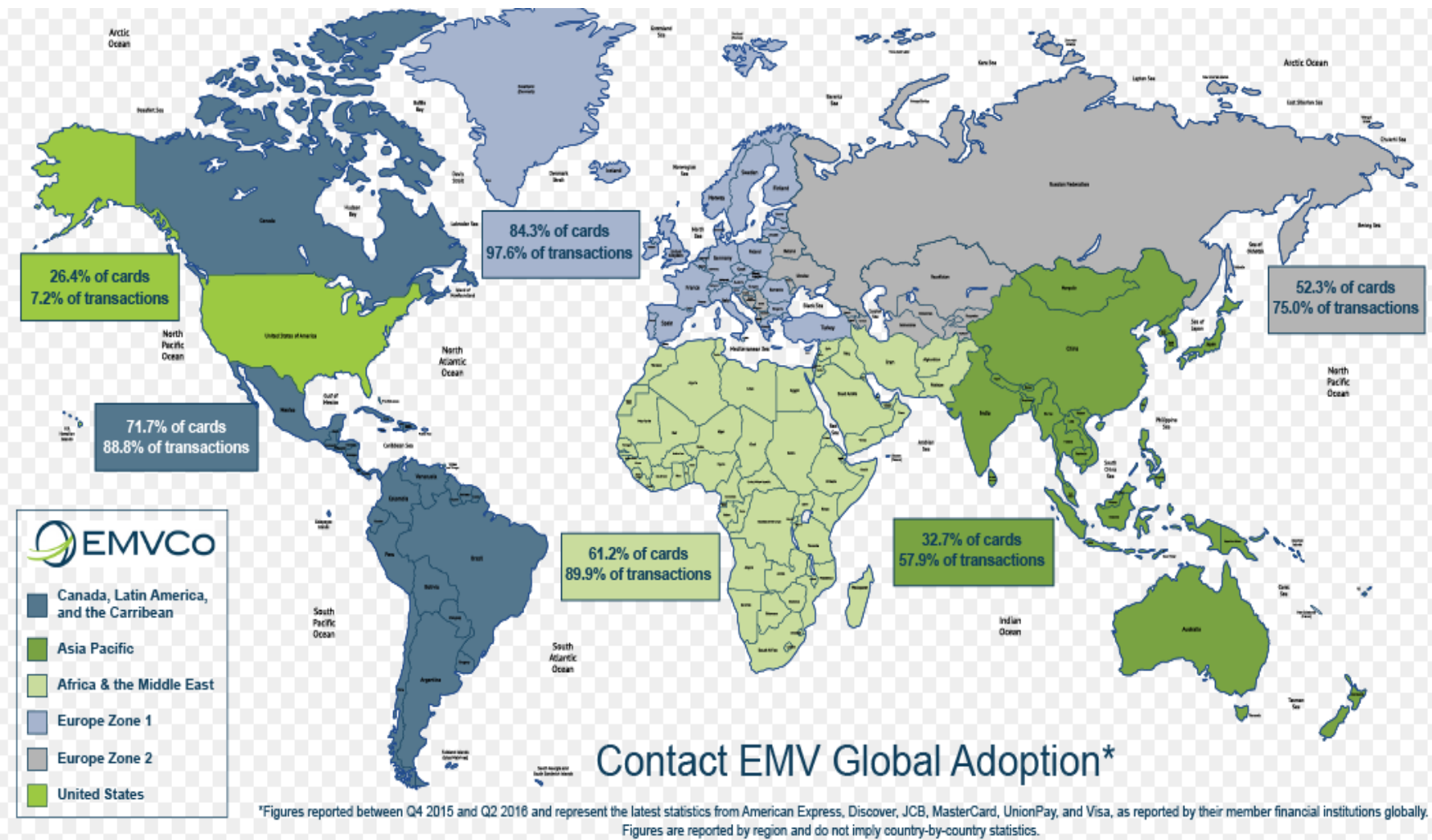


According to the latest figures from EMVCo, there are 80 countries across the globe in the process of migrating to the EMV standard, many of which are at different stages of their migrations. Simply put – the majority of the world, with the exception of the U.S., is utilizing EMV payment cards.

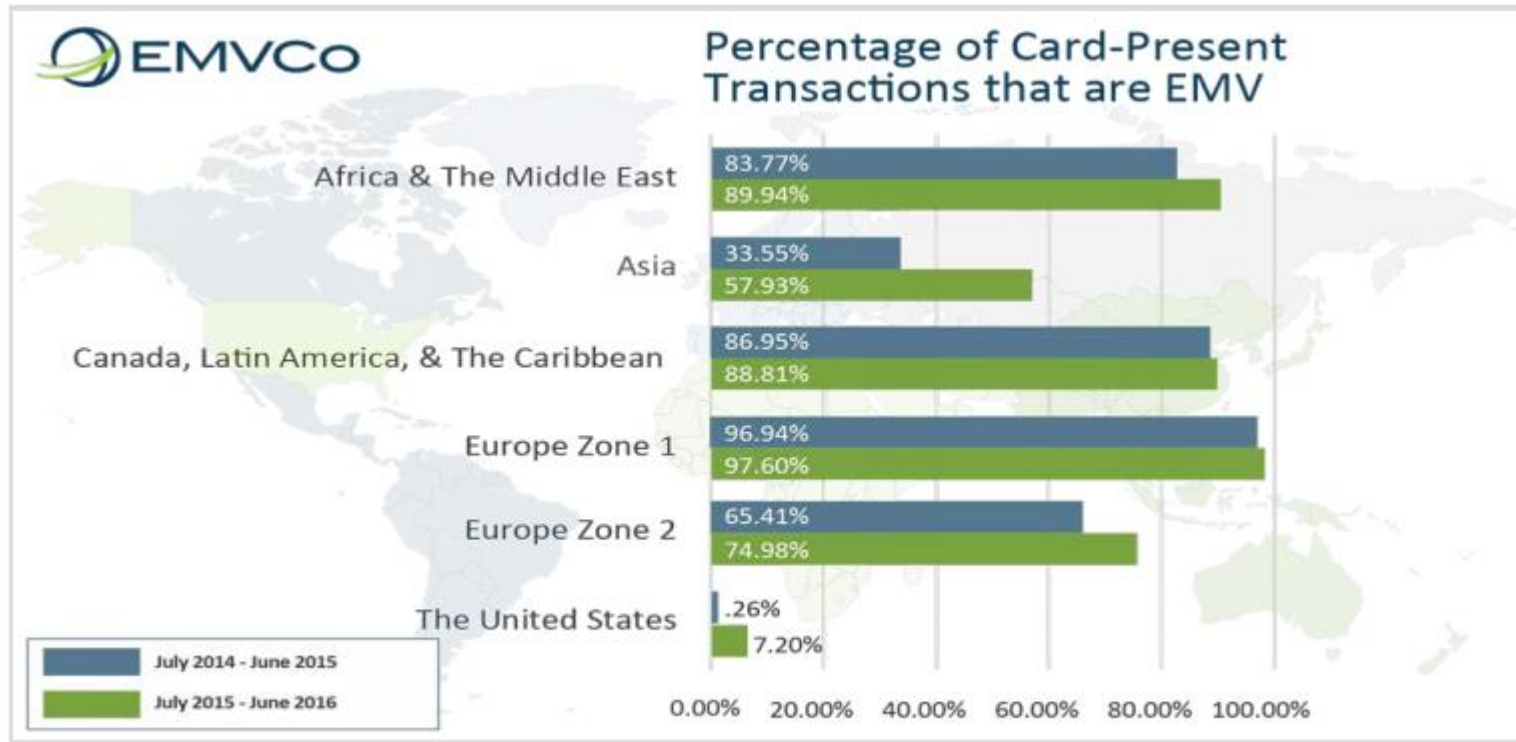
REGION	EMV CARDS	ADOPTION RATE	EMV TERMINALS	ADOPTION RATE
Canada, Latin America, and the Carribbean	741M	54.2%	7.1M	84.70%
Asia Pacific	942M	17.4%	15.6M	71.70%
Africa & the Middle East	77M	38.9%	699K	86.30%
Europe Zone 1	794M	81.6%	12.2M	99.90%
Europe Zone 2	84M	34.4%	1.4M	91.20%

*Figures reported in Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay and Visa, as reported by their member institutions globally.

EMV AROUND THE WORLD



EMV AROUND THE WORLD



Figures represent the percentage of all card-present transactions processed by each member institution that are EMV transactions (Contact or Contactless). The reported data (blue bar) is from the twelve months of July 2014 through June 2015 and (green bar) the twelve months of July 2015 through June 2016; the data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa during this period. To qualify as an "EMV transaction" for the purpose of this methodology, both the card and terminal used during a transaction must be EMV-enabled. Data is reported from the acquirer perspective. These figures do not include offline transactions, "on us" transactions (defined as a transaction handled exclusively by another processor), and/or transactions processed by

Figures represent the percentage of all card-present transactions processed by each member institution that are EMV transactions (Contact or Contactless). The reported data (blue bar) is from the twelve months of July 2013 through June 2014 and (green bar) the twelve months of July 2014 – June 2015; the data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa during this period. To qualify as an "EMV transaction" for the purpose of this methodology, both the card and terminal used during a transaction must be EMV-enabled. Data is reported from the acquirer perspective. These figures do not include offline transactions, "on us" transactions (defined as a transaction handled exclusively by another processor), and/or transactions processed by non-EMVCo-member institutions, such as local schemes.

http://https://www.emvco.com/documents/EMVCo_Card_present_EMV.pdf

FRAUD STATISTICS

On the whole, EMV supporters believe that migration to EMV in the U.S. will have more benefits than these potential instances of misalignment. Savings from counterfeit fraud prevention across all issuers could total as much as \$700 million annually. Additionally, to the extent that the U.S. issuers implement chip-and-PIN, the industry will also reduce the instances of lost/stolen card fraud, which account for \$300 to \$350 million in losses annually.

Fraud

INTERAC debit card fraud* losses
Losses to Financial Institutions

Year	Dollars lost to INTERAC debit card fraud	Cardholders Reimbursed
2015	11.8m	24,795
2014	16.2m	32,560
2013	29.5m	72,220
2012	38.5m	93,800
2011	70m	154,170
2010	119m	205,200
2009	142.3m	238,000
2008	104.5m	148,000

<http://www.interac.ca/en/stat-fraud>

LIABILITY SHIFT

October 2015 – Liability Shift

After October 2015, when credit card fraud takes place, liability for the costs will fall on the entity using the lesser technology. In 2015, that liability in the United States is estimated to total more than \$10 billion.

Examples of who the liable party becomes after the October 2015 deadline:

**Gasoline Retailers (AFD) liability shift is October 2020*

After the liability shift, if a merchant is still using the “swipe and signature” methodology and the customer has a smartcard, the merchant is liable.

If the merchant has the new Chip and PIN technology but the bank hasn’t issued the customer a Chip and PIN card, the bank is liable.

If the merchant uses Chip and PIN technology on a customer’s smartcard and fraud still takes place, the credit card company bears the liability, as is the case today.

LIABILITY SHIFT

Merchant Adoption of EMV Technology

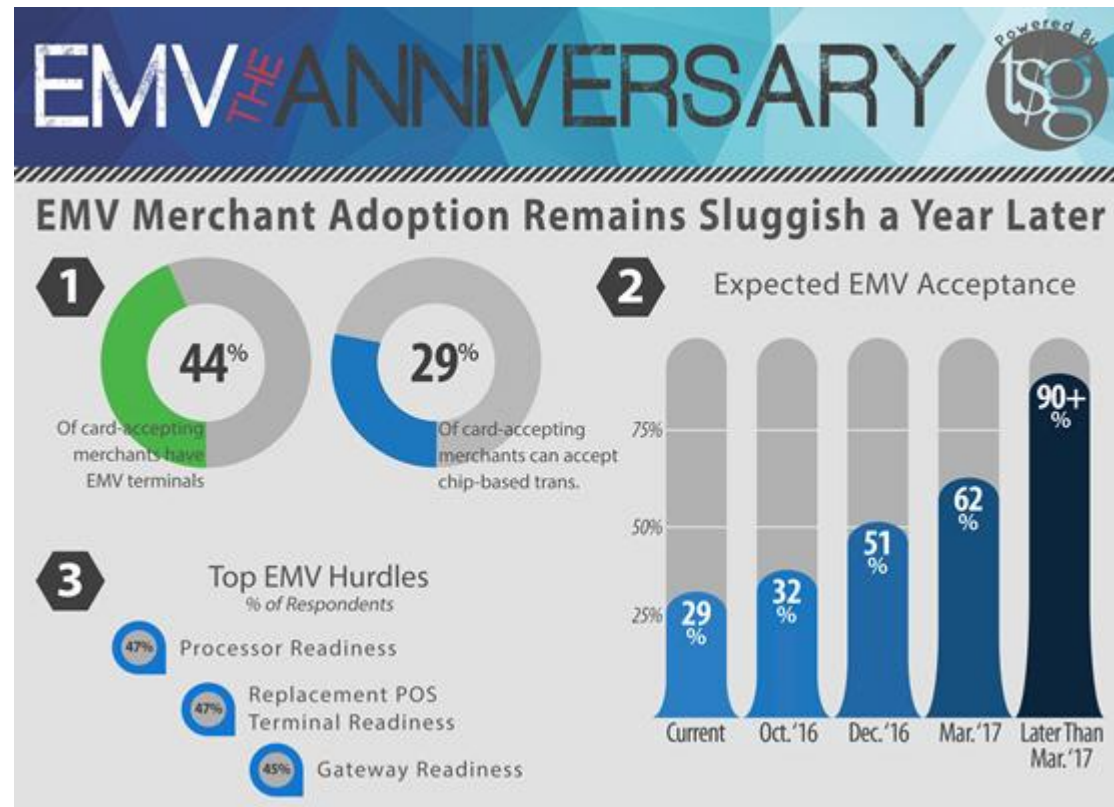
The liability shift in October 2015 should push merchants to upgrade their terminals and POS systems.

- Technology advancements
- Decreased fraud
- Reduction of chargebacks
- Interchange implications



LIABILITY SHIFT

Merchant Adoption of EMV Technology



LIABILITY SHIFT

October 2015 – Liability Shift

“... On the October 1, 2015 EMV migration date, only 2% of transactions were chip-on-chip. As of this June, 46% of transactions were chip-on-chip, and 70% of the cards presented to merchants were chip-cards.”¹

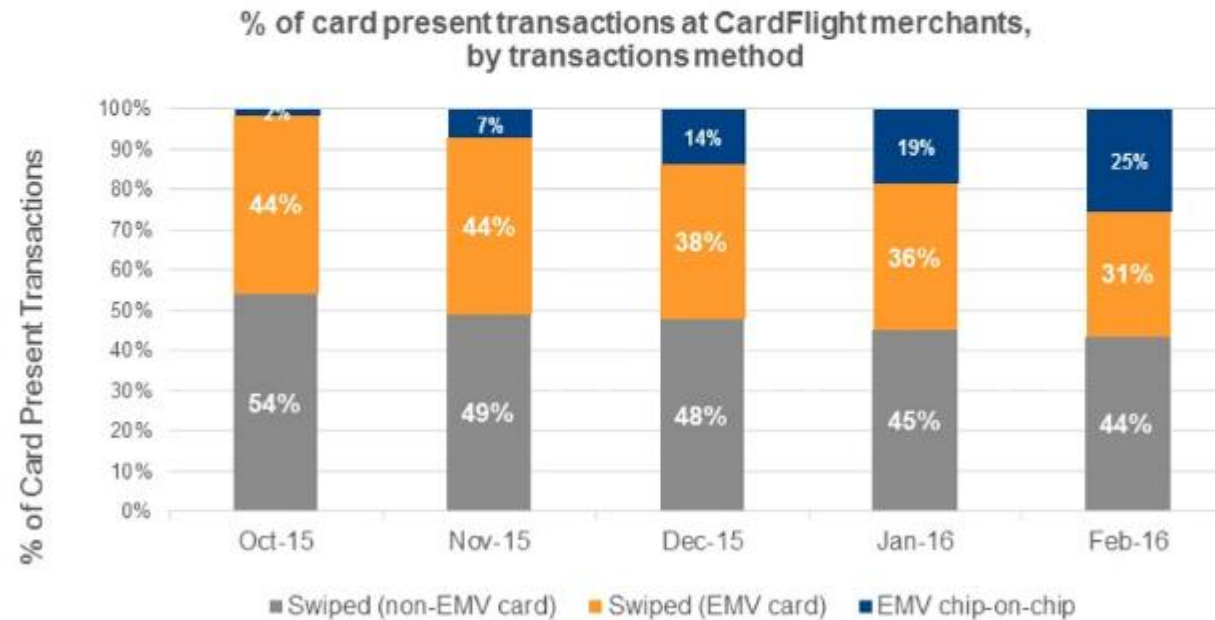
“... Following the October 2015 liability shift and transition to EMV chip-enabled cards, counterfeit activity fell 18 percent in the first quarter of 2016, according to new data from Auriemma Consulting Group (ACG).”²

EMV AROUND THE WORLD

Trends in Merchant Adoption of EMV



The percent of EMV cards presented that were processed as true EMV transactions has grown over 11x



Source: Card present transactions processed by CardFlight payment gateway

LIABILITY SHIFT

EMV IS NOT:

A silver bullet for PCI

A cure-all for
chargebacks

CONSIDERATIONS:

IP vs. Dial
(Transaction Time)

Liability Shift

NUVEI EMV STRATEGY

You're In Good Hands With Nuvei

As your trusted partner, Nuvei has years of real-world EMV implementation and support experience that can address your requirements. Our turnkey solutions are ready now.

EMV IMPLEMENTATION EXPERIENCE

- 5 Years of EMV Product experience in Canada.
- Technical expertise in all implementations of EMV.
- EMV technology, ready now!
- EMV knowledgeable client care team and support.
- Provides you with a unified EMV strategy.

KEY FACTS AND FIGURES

- Founded in 2003.
- Over 70,000 merchants.
- \$12 billion in processing.
- Over 1,500 sales partners.
- Over 500 employees.



THANK YOU

