Ignite Payment's Program on EMV™

EMV™ Overview

Ginger Smith, Director, Product Management

EMV™ is a trademark owned by EMVCo LLC.

What is EMV™?

- EMV™ – micro-chip payment standard created by **E**uropay®, **M**asterCard®, **V**isa® over 10 years ago and has been implemented globally
- EMVCo – organization owned by the global brands that manages the standard for global inter-operability
- EMV™ payment cards improve security over magnetic stripe technology through an embedded computer chip
  - Card validation ensures the card is legitimate
  - Cardholder authentication reduces fraud from lost and stolen cards

Ignite Payments™ | First Data. Authorized Partner

How EMV™ works

At the point of sale, a negotiation between the card and terminal determines which CVM will be used…

Payment Card is…

1. Inserted into chip-enabled slot reader (contact)

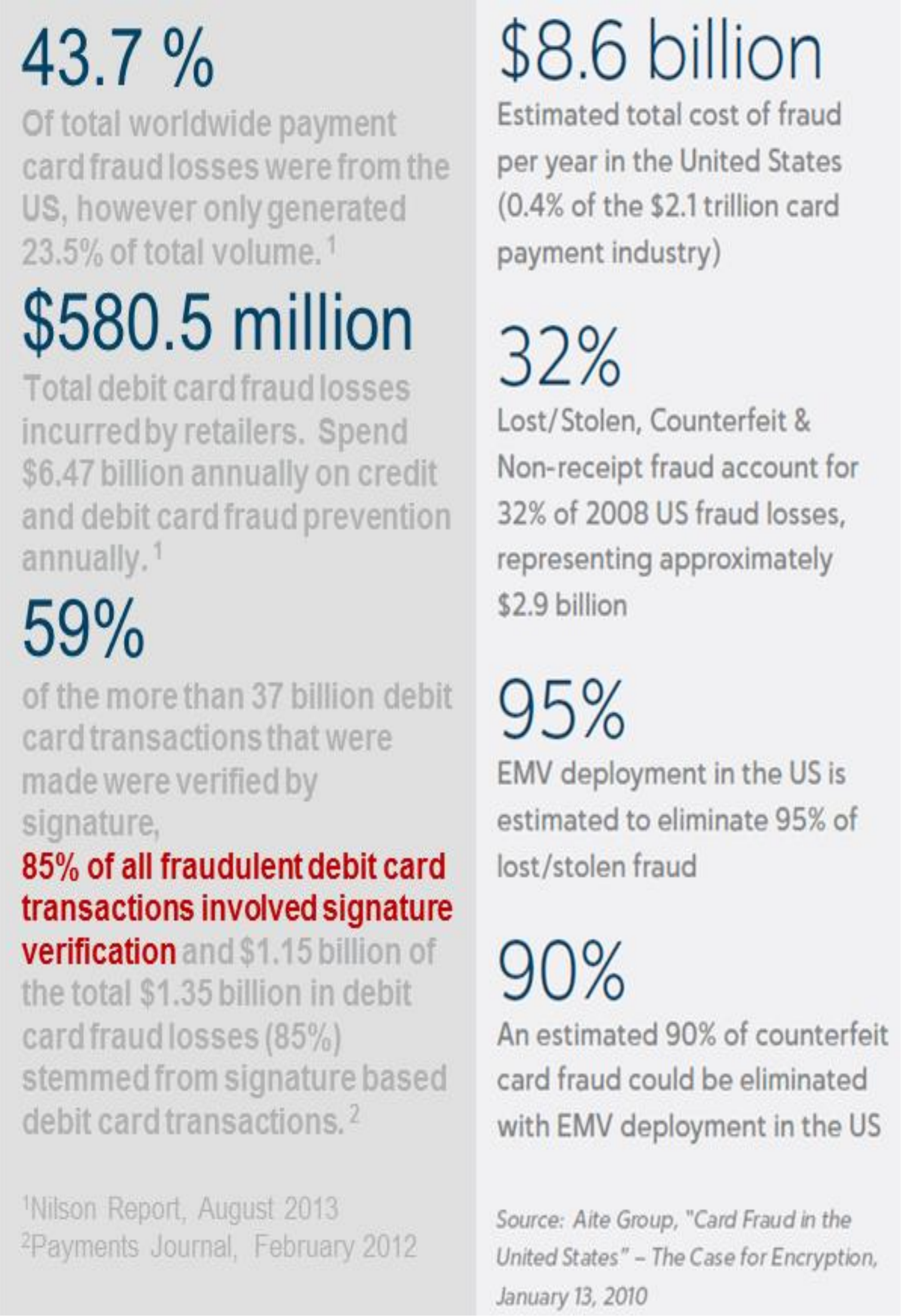
OR

2. Waved above the device (contactless)

- Data on the chip ensures the card is ***authentic***
  - Blocks the ability to copy the contents of the chip to another card
  - Prevents the use of skimmed or counterfeit cards
- PIN or signature ensures that the person presenting the card is the ***rightful cardholder***
  - PIN applies to Credit & Debit cards

EMV™ – Recent U.S. history

- **2011**: Global payments brands introduced roadmaps for EMV technology and encouraged its adoption
- **April 2013**: First domestic milestone required processors like First Data to accept EMV™ –based payments from merchants
- **4Q 2013**: Retailer data breaches occur
- **1Q 2014**: First Data reaches agreement with Visa & MasterCard to utilize Common AID for unaffiliated debit network routing (Durbin Amendment)
- **October 2015**: Next milestone – fraud liability shift to all point-of-sale devices (except Automated Fuel Dispensers Oct. 2017) will take effect
  - Liability for counterfeit fraud transactions shifts from financial institution to merchant if the merchant does not accept EMV transactions



43.7 %

Of total worldwide payment card fraud losses were from the US, however only generated 23.5% of total volume.[1]

$580.5 million

Total debit card fraud losses incurred by retailers. Spend $6.47 billion annually on credit and debit card fraud prevention annually.[1]

59%

of the more than 37 billion debit card transactions that were made were verified by signature, **85% of all fraudulent debit card transactions involved signature verification** and $1.15 billion of the total $1.35 billion in debit card fraud losses (85%) stemmed from signature based debit card transactions.[2]

[1]Nilson Report, August 2013

[2]Payments Journal, February 2012

$8.6 billion

Estimated total cost of fraud per year in the United States (0.4% of the $2.1 trillion card payment industry)

32%

Lost/Stolen, Counterfeit & Non-receipt fraud account for 32% of 2008 US fraud losses, representing approximately $2.9 billion

95%

EMV deployment in the US is estimated to eliminate 95% of lost/stolen fraud

90%

An estimated 90% of counterfeit card fraud could be eliminated with EMV deployment in the US

Source: Aite Group, "Card Fraud in the United States" – The Case for Encryption, January 13, 2010

The Marketplace at the end of 2015

- The U.S. is set to transition more than 1.2 billion payment cards and 8 million point-of-sale (POS) terminals to meet the requirements for EMV™ smart card payments to be ubiquitous
- Physical EMV™ hardware (cards and POS terminals) will cost issuers and merchants more than $6.8 billion in the U.S.
- It is forecast that more than 575 million EMV™ chip-enabled payment cards will be in circulation in the U.S. (48% of the total 1.2B)[1]
- More than 50% of U.S. retail locations are projected to be EMV™ -capable
- The long tail of EMV™ migration will be small and micro businesses
- The EMV™ transition will help fix an important loophole in card fraud: counterfeiting
    - However, based on experiences in other markets, card fraud is expected to migrate to the point of least resistance: the card-not-present environment.

Ignite Payments™ | First Data. Authorized Partner

Liability implications of EMV™

- In U.S. today:
  - Fraud in card-present environments absorbed by Bank/Issuer unless merchant fails to meet POS acceptance and dispute resolution requirements
  - Losses are offset when dispute resolution requirements allow liability to be shifted through “chargeback process” to Acquirer/Merchant
  - Merchant/Acquirer takes liability for merchant data breaches or skimming attacks

- In 2015 with EMV™ :
  - However, based on experiences in other markets, card fraud is expected to migrate to the point of least resistance: the card-not-present environment and merchants that are not EMV™ capable

Visa

Counterfeit fraud losses “shift” to party who does not enable EMV™ if fraud would have been avoided if EMV™ had been used

MasterCard Liability Hierarchy

Party that cannot support a lower-risk option holds the liability. Equal capabilities = issuer holds liability.

Issued Device/Card		Acceptance Terminal
Magnetic stripe and contactless magnetic stripe	Higher Risk	Magnetic stripe and/or contactless magnetic stripe
EMV contact or EMV contactless (signature CVM)		EMV contact or EMV contactless (not PIN capable)
EMV contact or EMV contactless (online or offline PIN CVM)	Lower Risk	EMV contact or EMV contactless (online or offline PIN capable)

Note: Above interpretation based on Visa and MasterCard requirements. Issuers should review this internally.

Why implement EMV™?

Financial Institutions

Reduce fraud

- Potential to reduce POS counterfeit fraud losses with use of chip
- Shift fraud liability to merchants that do not support EMV™

Improve market perception

- Demonstrate to customers and market that cardholder security is important
- Poor brand perception by cardholder if their issuer is last to implement EMV™

Avoid increased exposure to cybercriminals

- Late adopters will be the weakest link for cybercriminals – they will find the path of least resistance to identify weakness
- As the market of non-chip card dwindles, the criminals will target non-chip cards

Merchants

Increase security at the POS

- A primary way cybercriminals use stolen credentials is to create a false card to impersonate the actual card
- Historically, as cybercriminals recognize EMV™ implementation is underway, they increase activity

Reduce liability costs

- The global card brands have announced
  a Liability shift for Oct 2015
- In 2015, if the merchant does not support EMV™ , that liability will shift to the merchant

Avoid increased exposure to cybercriminals

- Criminals will find the path of least resistance through late adopters to identify weakness
- As the population of non- EMV™ locations dwindles, the criminals will concentrate
  on non EMV™ -locations

Ignite Payments | First Data Authorized Partner

The First Data Approach

Multi-layered Security & Compliance

COMPLIANCE

A step-by-step, self-guided approach to help small and mid-size merchants complete the SAQ

PCI Rapid Comply®

FRAUD PREVENTION

Fraud reduction technology that can help protect against losses from accepting counterfeit and lost or stolen payment cards at the point-of-sale

DATA SECURITY

Powerful payment card security that combines encryption with random number tokenization

The TransArmor® Solution

PROTECTION

Value added services for Level 4 merchants to increase data security, protect against fraud, and provide coverage in the event of a data breach.

First Data can provide you with the tools to help protect your customer's data from cyber criminals.

EMV™ & Data Security – How do they relate?

Multi-layered security solution

- Today’s advanced technology broadens the threat landscape for clients and offers multiple ways for cyber criminals to try and steal cardholder data
  - Data in motion (e.g., with memory-scrapers) or
  - Data at rest (e.g., from a database)
- Then they use the stolen data to produce
  - Counterfeit cards, or for
  - Fraudulent online transactions

Focusing on only one or two of these points of entry can still leave vulnerabilities

	Security Needs		Security Solutions
EMV™	Protecting Your Data Against Card Counterfeiting	✓	**EMV™** Chip-based technology reducing the risk of accepting counterfeit cards. PIN reducing the risk of misuse of lost or stolen cards.
TRANSARMOR	Protecting Your Data in Transit	✓	**Encryption** Protecting cardholder data in motion from the swipe of the card until it reaches our secured processors.
	Protecting Your Data at Rest	✓	**Tokenization** Making it impossible to steal data at rest from merchant servers or POS, while reducing the cost and complexity of compliance

Ignite Payments

First Data Authorized Partner

First Data EMV^{TM} Readiness

First Data's EMV™ capabilities

Current EMV™ capabilities

- First Data is producing EMV™ -enabled credit cards and processing EMV™ credit transactions **TODAY**
- First Data has been processing real-time EMV™ transactions with the largest retailer for 3+ years
- In 2013, First Data processed 10M+ U.S.-based merchant EMV™ transactions
- First Data's issuing business processes over one million EMV™ transactions a month
- First Data has issued over 10 million EMV™ cards

Current State

Merchant Acquiring Platforms

- We are ready for EMV™ today
- We have a process to help clients implement now
- We have EMV™ -capable terminals ready now
- We will continue to add more networks for debit, as the networks adopt Common AID
- Security at the point-of-sale should be a priority; clients should not wait to begin implementing EMV™

Ignite Payments™

First Data® Authorized Partner