Breaking Down the EMV Liability Shift

Who's Liable for What & When

ingenico GROUP

Introduction

The EMV liability shift is a burning hot topic in the payments industry and if you are looking to better understand what it means, how it works, and why it matters - you have come to the right place. This ebook is designed to educate merchants, service providers, and other stakeholders within the payments ecosystem in the U.S. about the upcoming EMV liability shift in a simple and clear manner. The ebook is divided into three short chapters starting with a brief overview of how EMV technology works and then moving into the more granular elements of the liability shift – breaking down who is liable for what and when.

Table of Contents

Why EMV?

Credit card fraud

Over the past few decades, credit cards have provided shoppers with the convenience of paying for goods and services they want with a simple swipe of a card.

Even though these credit cards are simple to use, every now and then a question arises - are they secure? Criminals around the world have found ways to steal credit card information and use it for their own benefit resulting in credit card fraud. The United States has seen a significant rise in credit card fraud over the last decade.

To help solve this problem, card networks such as VISA, MasterCard, etc. are pushing merchants in the U.S. to upgrade their payment solutions to accept EMV chip card transactions.

How does EMV help?

EMV, which stands for Europay, MasterCard, Visa, is a global payment standard that relies on the microprocessor chip embedded in cards as opposed to the less secure magstripe cards that store data on a band of magnetic material on the card which can easily be retrieved.

The EMV payment standard has been in place in most countries around the world for years and been successful in helping curb card-present credit card fraud. EMV migration is finally coming to the U.S. and will be instrumental in creating secure credit/debit card transactions.

Smart Metric
PROTECTING THE WORLD DIGITALLY

Americans lose $8.6 billion to credit card fraud, according to the Aite Group, and this number is expected to reach $10 billion by 2015, according to the Nilson Report.

– SmartMetric, Inc.[1]

EMV helps in the following ways:

PROTECTS CARD DATA

Unlike magstripe cards, every time an EMV chip card is used at an EMV-enabled payment terminal or on a mobile point of sale (mPOS) device, the microprocessor chip creates a one-time unique transaction code that cannot be used again.

REDUCES FRAUD

Counterfeit magstripe cards created from EMV chip cards or transaction data will not work at EMV-enabled payment terminals or mPOS devices.

COMPLEMENTS PAYMENT SECURITY

EMV complements the payment security ecosystem and provides an added layer of protection when used with other payment security standards such as point-to-point encryption (P2PE) and technologies such as tokenization.

Reasons to use EMV:

SECURITY

When purchases are made using an EMV chip card at EMV-enabled terminals, the transaction is more secure because of the unique process used to authenticate the card.

GLOBAL INTEROPERABILITY

EMV is a global payment standard and U.S. is the last developed country to migrate.

EMV SUCCESS

EMV has been successful in curbing credit card fraud in every country in which it has been implemented.

In the U.K., counterfeit fraud has fallen 56 percent since the country rolled out EMV cards in 2005. In Australia, counterfeit fraud is down 38 percent and in Canada it is down 49 percent.

– Aite Group report from 2014[2]

EMV Liability Shift

What is the liability shift?

Card brands have been driving the EMV migration in the U.S. by setting a liability shift deadline of October 2015 for the merchants to upgrade their payment infrastructure. As this liability shift gets closer, confusion and misinformation are running rampant. What is the liability shift, who is liable for what, and when?

Today, the liability of a chargeback from credit card fraud always falls on the issuer. After October 2015, this liability will shift to the merchant in certain scenarios. It's important to note that this liability shift is dependent on two important components. First is the use of EMV cards and second is the use of EMV chip-enabled payment solutions (mobile and smart terminals). Where the liability falls depends on both what type of card is being used by the customer and the capabilities of the terminal used by the merchant (EMV-enabled or magstripe). We will explore the different types of liability shifts later in this ebook.

Determining the type of liability shift

Confusion around liability shifts are common. What a lot of people don't realize is that there are two types of liability shifts. But, before we break those down for you, it helps to first define the type of fraud we have at hand – is it a counterfeit card fraud or a stolen card fraud?

Next, you should follow the general premise that the party supporting the superior technology for each fraud type will prevail in a chargeback. For the issuer, that technology is represented by the EMV chip cards and for the merchants - the EMV-ready terminals. In case of a technology tie, the fraud liability remains as it is today – with the issuer.

There are two types of liability shifts:

LIABILITY SHIFT FOR COUNTERFEIT CARDS

LIABILITY SHIFT FOR STOLEN CARDS

Liability shift for counterfeit cards

This scenario applies to Visa, MasterCard, American Express, and Discover

Let's examine the first scenario where a counterfeit credit card is in play in a fraudulent transaction. Post October 2015, if a merchant accepts a counterfeit magstripe card (created from an EMV chip card or transaction data) at a payment terminal or mobile point of sale (mPOS) device that is not EMV-ready, the merchant will be liable for the chargeback resulting from the fraud.

The counterfeit card created from an EMV card or transaction data can only be processed at a magstripe-only terminal. If the merchant's payment solution is ready to accept EMV transactions, this counterfeit card will not be processed, thus, saving the merchant from the liability.

Here are some other instances which show the liability shift in case of counterfeit cards:

Timeline	Card Type	Terminal Type	Liability
Current	Magstripe	Magstripe	Issuer
Post October 2015	Magstripe	Magstripe	Issuer
Post October 2015	Magstripe	EMV*	Issuer
Post October 2015	Chip*	Magstripe	Merchant
Post October 2015	Chip*	EMV*	Issuer

** With or without PIN*

The only caveat here is in the case of a fallback transaction – which is a transaction that is initiated between a chip card and a chip terminal but chip technology is not used (due to card reader error, damaged EMV chip, etc.) and the transaction is completed via magstripe. Since fallback transactions are initiated as an EMV transaction but end up as magstripe, the liability remains with the card issuer.

Liability shift for stolen cards

This scenario applies to MasterCard, American Express, and Discover

The second scenario is where a stolen EMV chip card is in play in a fraudulent transaction. Post October 2015, if a merchant accepts a stolen EMV chip card that requires a PIN using a payment terminal or mPOS device that does not support EMV with PIN entry, the merchant will be liable for the chargeback resulting from the fraud.

This liability shift does not include No CVM (Cardholder Verification Method) transactions that meet the No CVM requirements of the card brand or network. No CVM transactions are typically low-dollar transactions with merchants in low risk categories such as fast food, convenience and grocery stores. In this situation, the issuer-set transaction threshold allows for the payment to go through without the need for a PIN or signature.

Liability shift for stolen cards

This scenario applies to MasterCard, American Express, and Discover

Here are some other instances which show the liability shift in case of stolen cards:

Timeline	Card Type	Terminal Type	Liability
Current	Magstripe	Magstripe	Issuer
Post October 2015	Magstripe	Magstripe	Issuer
Post October 2015	Magstripe	EMV	Issuer
Post October 2015	Chip & PIN	Magstripe	Merchant
Post October 2015	Chip & Sign	Magstripe	Issuer
Post October 2015	Chip & Sign	EMV	Issuer
Post October 2015	Chip & PIN	EMV only	Merchant
Post October 2015	Chip & PIN	EMV with PIN	Issuer

The only caveat to this scenario is in case of a PIN bypass. In a chip and PIN transaction, a cardholder can bypass the PIN and process the transaction without it being entered, only if the merchant's terminal provides the cardholder the option. In this scenario, PIN bypass indicators are sent in the authorization request to the issuer. If the issuer chooses to approve the transaction, they accept the liability on that transaction.

Risks of not migrating to EMV

So far we've learned how liability of a fraudulent card transaction shifts to the merchant in certain scenarios. Let's take a look at the risks merchants face if they are not ready to accept EMV transactions post the deadline.

FINANCIAL IMPACT

- With credit card fraud rampant in the U.S., the total volume of chargebacks from fraudulent transactions could result in heavy costs for the merchants post October 2015.

- If merchants are victims of a data breach, card companies like VISA and MasterCard can charge them penalties for lack of a secure system. However, they also waive these data breach penalties for merchants that are processing 95% or more of their transactions through an EMV-ready payment solution in the form of smart terminals or an mPOS device. Merchants who don't upgrade with EMV-ready payment solutions will be subject to these penalties if the card data from their servers is stolen.

- The best way for merchants to protect themselves against any potential chargebacks and penalty fees resulting from credit card fraud and data breaches is to make sure their business is equipped with EMV-ready payment solutions.

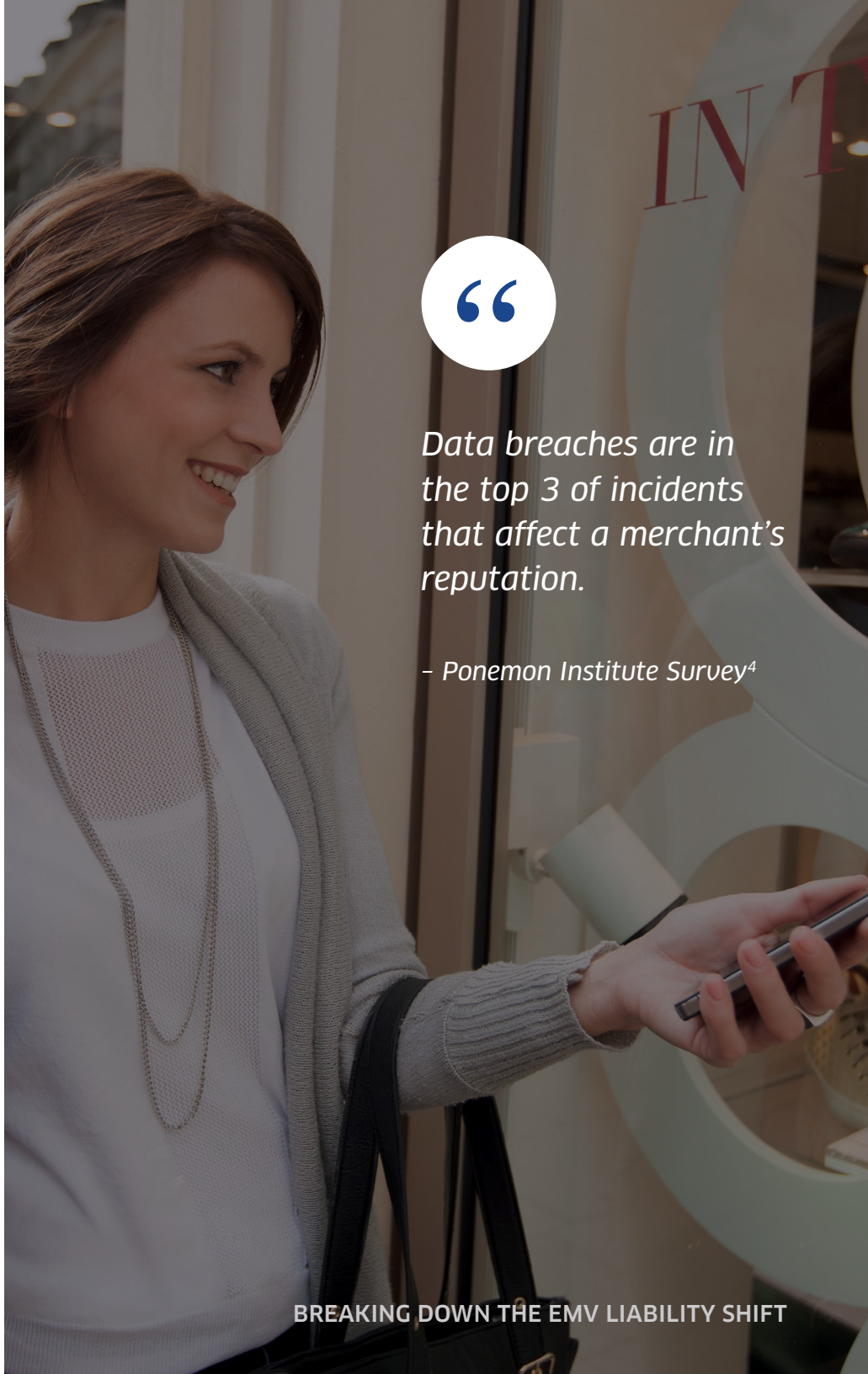
Risks of not migrating to EMV (cont.)

BRAND IMAGE

- Merchants face the risk of harming their brand's reputation in events of a credit card fraud or a data breach. High frequency of these events have made customers across the U.S. wary of where they use their credit cards and form a negative brand perception of merchants who use outdated payment technology. Using EMV chip cards at EMV-ready terminals is one step towards better payment security. EMV-ready payment terminals and mPOS devices provide a safer transaction environment to customers making them feel more secure about using their credit cards at these merchants and improves brand perception.

- In 2013, Target (one of the biggest retail chains in the U.S.) was a victim of a data breach where credit card information of over 40 million accounts was compromised. The aftermath of the breach saw lay-offs and executive changes within Target, which added more fuel to the bad publicity the company was already receiving at that time. Target's profits fell by 46% percent by the fourth quarter of 2013 and were attributed to the breach.[3] In 2014, the slew of data breaches continued with many brands such as Neiman Marcus, UPS, PF Changs, and others being hacked, resulting in stolen credit/debit card information.

- By upgrading their payment infrastructure to support EMV, merchants not only protect themselves from any fraudulent transaction liability but also safeguard their brand image in the eyes of the consumer.



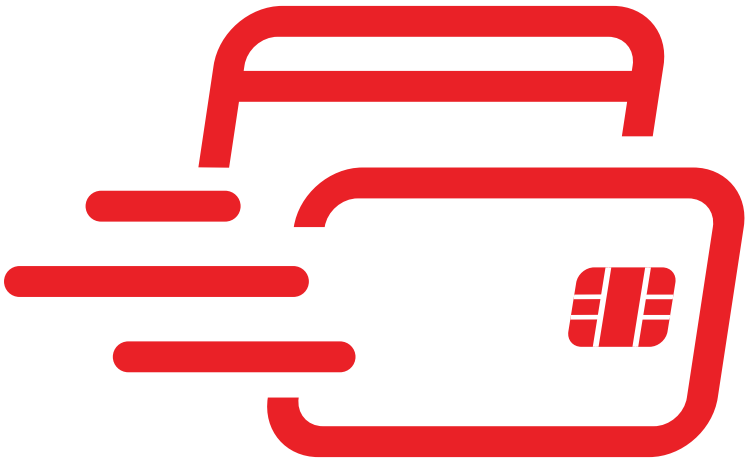
Data breaches are in the top 3 of incidents that affect a merchant's reputation.

– Ponemon Institute Survey[4]

Moving Forward

While most card issuers are doing their part in helping consumers get ready for this shift, chip cards are just one small piece of the big EMV migration puzzle. It is the combination of using an EMV chip card in conjunction with an EMV-enabled terminal or mPOS solution that makes the transaction more secure.

A large number of issuers have already deployed EMV chip cards to their customers across the country which means that post October 2015, merchants who have not migrated to EMV can be liable for a chargeback from credit card fraud. By not migrating, merchants put their business, their customers and their brand at risk.



Navigate the EMV waters with the right technology partner

Migrating to EMV can seem like a daunting task, and merchants of all sizes and across industries are looking for the simplest, fastest, and most secure path to get them where they need to be.

That's why it's imperative that merchants and other industry stakeholders find the right technology partner with the experience and the know-how to advise them as they navigate the uncharted waters of this important transition.

With over three decades of leadership in the payment industry, Ingenico Group is the trusted, strategic partner of choice for both merchants and payment industry players in the U.S. and worldwide. Our team of EMV experts hold board level advisory seats on the key EMV regulatory and standards bodies, including EMVCo, EMV Migration Forum, Smart Card Alliance and PCI SSC. Today, more than 14 million of Ingenico Group payment solutions are already EMV-enabled and securely process smart card transactions daily. We have partnered with card brands, acquirers, processors, merchants, retailers, and financial institutions in the U.S. to successfully plan, test and complete their migrations to EMV.

Want to learn how we can help you streamline your EMV implementation and avoid putting your business, customers and brand at risk? Contact us to to get started: info.us@ingenico.com.

If you would like to learn more about EMV, please visit these links:

OTHER EMV RESOURCES:

- VISA Chip Card Technology
- MasterCard EMV Chip Card Technology
- GoChipCards
- EMVCo's Guide to EMV Chip Technology

SOURCE LINKS:

1 http://www.marketwired.com/press-release/credit-card-fraud-continues-grow-with-estimated-usa-fraud-losses-reaching-10-billion-otcqb-smme-2044529.htm

2 http://aitegroup.com/report/emv-lessons-learned-and-us-outlook

3 http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/

4 http://www.darkreading.com/study-data-breaches-make-huge-impact-on-brand-reputation/d/d-id/1252742

ingenico
GROUP

800.252.1140
info.us@ingenico.com
www.ingenico.us