SOLUPAY

PAYMENT SOLUTIONS. **SIMPLIFIED.**

EMV: Europay, MasterCard and Visa

Are You Ready For the Revolution?

With October 2015 fast approaching for the Chargeback Liability Shift, EMV is a trending topic, whether you are a merchant, bank, or payment processor.

The EMV Chargeback Liability Shift pertains to card present transactions only. We have put together this eGuide to assist in educating and guiding your understanding of EMV and how it impacts you.

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

AN INTRODUCTION TO EMV

EMV (Europay, MasterCard and Visa) is now the global standard for inter-operation of integrated circuit cards, or "chip cards". It is a form of contactless payment, and it's actually pretty simple to understand. You might also hear EMV referred to as "chip cards," "chip and PIN," and "chip and signature."

The term "EMV" comes from the developers of this technology – Europay, Mastercard, and Visa. Some credit/debit cards already use this in the US, while other regions of the world such as Europe, China and Canada have been using this for years. EMV uses a small microprocessor that's embedded into your credit or debit card. Banks and credit card companies want you to use them because they're more secure than magnetic strip cards. More on security later.

For now, most cards in the U.S. do not have this embedded chip. Some cards will have both a magnetic strip and chip, and eventually magnetic strips will go away entirely. The reason that EMV is receiving so much attention is that there will be a chargeback liability shift to merchants from card issuing bank to the merchant not accepting EMV technology starting in October 2015. Just keep in mind that this date will come and go for most merchants as they have a low incidence of chargebacks today. But for merchants that are fraud targets or have high ticket items that can be easily resold on the streets, October 2015 will have a much greater impact on them.

Some quick questions to ask yourself before reading on:

Q: Are you a Card Present environment where you are face to face with your customers and you are swiping credit cards within a Point of Sale or a terminal?
A: If **Yes**, it is important for you to understand the impact EMV will have on your business, and you should have this document at the ready, especially the sections on chargeback liability and security.

Q: Are you a Card Not Present environment where you only accept credit card payments over the phone or over the web?
A: If **Yes**, you do not need to worry too much about EMV, but you will want to be aware of the changes and how they could impact Card Not Present transactions, as detailed in the Chapter 4: Chargebacks – Card Not Present Transactions.

Q: Are you accepting payments both via face-to-face and over the phone or over the web?
A: If **Yes**, then this document in its entirety should be a great resource for you.

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

EMV CONVERSION IN THE U.S. IS SET TO EXPLODE

EMV is already largely used in Europe and China and Canada, and the world is bracing for a revolution in credit card transactions as EMV becomes not only something available in some locations, but the norm for consumers. Merchants who are in the midst of upgrading their terminals need to prioritize EMV, no matter how large a merchant may be. According to an article written by The Members Group, "U.S. EMV Conversion Expected to Drive SmartCard Shipments," the US will be a large driving factor to this worldwide movement:

> "Global EMV card shipments are expected to total more than 3 billion by 2019. Although moves by China are driving much of that total, the U.S. is expected to have a great impact on worldwide shipment numbers in the coming years.
>
> According to a recent ABI Research report, 1.7 billion EMV chip cards were shipped worldwide in 2013 (a 27-percent increase from 2012). In 2013, 442 million chip cards went to China, which is in the midst of an EMV card conversion to the People's Bank of China card standard. Fifty-six percent of the 442 million cards sent to China were contactless.
>
> ABI is forecasting double-digit annual growth in EMV card shipments through 2017. However, if not for China, global growth year-over-year would have totaled just 8.5 percent instead of 27 percent between 2012 and 2013. This illustrates the impact a single country's card conversion can have on total global card shipments. ABI researchers predict with nearly 2 billion payment cards currently in circulation in the U.S., a similar "China effect" could occur as the U.S. migrates to EMV.
>
> EMV card issuance in the United States has been slow going so far, but ABI Senior Analyst Phil Sealy expects it to pick up over the next few months as October 2015 looms. Indeed, new numbers released by the Payments Security Task Force (PSTF) support Sealy's expectation. The PSTF, composed of nine of the U.S.'s largest payment card issuers, recently announced an estimated 575 million U.S. payment cards will feature EMV by 2015.
>
> These statistics underscore the importance of issuers getting into EMV conversion queues with their processors and vendors now. As more merchants re-terminalize, more cardholders receive smart cards from major issuers and more fraud-prevention proponents tout the benefits, those EMV project lines will only get longer."

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

EMV AND CHARGEBACK LIABILITY

As we stated, the EMV Chargeback Liability Shift is coming up on October 1, 2015. But what exactly do we mean by Chargeback Liability Shift? What's going to happen is this: All the major credit card companies – Visa, MasterCard, Discover, and American Express - have said that if EMV capability has not been implemented on your POS terminals, you (the merchant) will be liable for all counterfeit transactions if they are made.

Note that this DOES NOT MEAN you as a merchant must be set up to accept chip payments by October 2015. There is no law or statute that will put you out of PCI compliance by not being EMV compliant. As a reminder, this DOES NOT APPLY to merchants that only accept Payments by Online or Telephone, and this applies ONLY to Card Present transactions where payments are accepted face to face with customers.

Even though liability is going to shift, the rules won't simply be black-and-white. Visa, MasterCard, and American Express all have their own detailed requirements that define when liability shifts for transactions. You can view these on their websites, and do so diligently as these can change. Working closely with a payment solutions provider, such as Solupay, will ensure you are up to date on any changes.

So how does a merchant become EMV compliant? Given that EMV compliance is fairly complex, here are some quick tips to make sure you stay compliant with this liability shift:

- Start months ahead of time – like now. You can bet EMV will change in the future – buy devices and systems that you can scale over time.
- Communicate with everyone involved in the change process so they understand, which makes the transition easier
- Make a list of suppliers, identify the questions you'll ask them, and choose the one that best meets your needs
- Create your budget – Expense will be driven by options. Choose a provider that has more than one EMV solution.

Even though you don't have any legal obligation to comply with this shift, it's still wise to do so. Your company may be able to sustain the new losses because of your increased liability…for a while. But at some point, not upgrading your EMV compliance will cost you more than actually doing the upgrade. IN many cases, depending on your product and the industry of course, with just one liable chargeback where you lose the product, the money you should have collected, as well as refunding the rightful cardholder, you may have easily been able to justify the equipment upgrades.

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

Let's reiterate our point on liability:. TODAY, if the card is present, the issuing bank for that card is generally responsible for any counterfeit losses. However, on October 1, 2015, that changes. Then, in card present transaction, the company responsible for the EMV information has to take on counterfeit losses.

What's important for banks: If the bank issues a non-EMV card, the responsibility's on them. But, if the card had an EMV chip and the provider did not process the transaction, then they may be responsible for counterfeit losses.
What's important for merchants: Legally, the provider can pass responsibility for losses onto the merchant if their equipment isn't capable of processing EMV transactions.

CHARGEBACKS – CARD NOT PRESENT TRANSACTIONS

What about Card Not Present Transactions for E-Commerce Companies? How does this relate to the whole EMV discussion?

Just because the EMV chargeback liability shift pertains to card present transactions only, this does not mean the card-not-present (CNP) transactions are safe from fraud. CNP fraud cases currently account for 16% of all US card fraud today. In 2013, that accounted for $5.3 billion! And in 2017, US consumers are projected to spend $430 billion online.

If you have an e-commerce arm of your business, CNP fraud used to be a huge deal. Card issuers would simply charge back the losses to you. But today, those are all wiped out because of the 3D secure protocol programs they offer.

While the EMV chargeback liability shift only pertains to card present transactions, there is evidence that card-not-present fraud will rise once the EMV transition happens, as fraudsters find it harder to do their schemes with EMV and look to new avenues for their thievery.

Take for example what happened in Canada in 2008, when they rolled out chip-based cards nationwide. According to this data, Canada cut card fraud costs 55% from $195.1 million to $88.7 million in 2013. That sounds pretty good on the surface. But then domestic card-not-present fraud increased 133% from $102.1 million in 2008 to $238.4 million in 2013! Just because you do not have to worry about the EMV chargeback liability shift for your CNP transactions, you must still remain diligent about credit card security.

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

But what about merchants that have both Card Present and Card Not Present business? One solution for Card Present may not address Card Not Present transactions, and vice versa. Working with a provider like Solupay who specializes in putting together a complete "hybrid" solution for these types of merchants from our broad portfolio of products will be necessary to ensure you are addressing the security in all your transactions.

EMV AND SECURITY

Here is how EMV makes transactions more secure: Today, the data stored on cards never changes. So if a criminal steals it, it's easy to copy the data and sell or use it. With EMV cards, however, every time a transaction happens, the chip creates a unique code that never gets used again – ever! Because hackers use duplication when they actually steal your data, this makes EMV quite powerful. They could steal the transaction code, but since it's unique, using the code repeatedly simply results in the card's use being denied.

What also makes EMV cards hard to counterfeit is the actual physical media. A magnetic strip base card is easy to copy, while to make a plastic card with a chip on it, and then to copy its data, takes far more sophisticated equipment. Basically, EMV technology will not prevent data breaches, but it makes fraud and theft much more difficult. But is it enough?

We reported earlier that ABI Research has forecasted 575 million U.S. payment cards will feature EMV by 2015, and Global EMV card shipments are expected to total more than 3 billion by 2019. In the end, it will eventually be the preferred method to accept credit cards. But it is only one arm in what we have termed "The Trifecta of Card Security."

THE TRIFECTA IN SUMMARY

1. Tokenization protects the storage of cards
2. EMV fixes the card using a programmable chip
3. P2PE protects the transmission and acceptance of cards.

EMV combined with point to point encryption and tokenization will put your business in the most secure position as possible in conjunction with the other published PCI best practice recommendations. Here is how :

Tokenization allows merchants to store tokens for each transaction, and use that token instead of the original card data.

SOLUPAY
PAYMENT SOLUTIONS. **SIMPLIFIED.**

Point-to-point encryption (P2PE), sometimes referred to as end-to-end encryption (E2EE), is the ideal state in which credit card numbers and other sensitive information is encrypted from the point of entry (card swipe) to the other end (the issuing bank).

Take for example, the now infamous Target and Home Depot Data Breaches. Just installing EMV in your place of business does not improve the level of security as it pertains to the kinds of breaches that occurred at these two retail giants.Those incidents could have been prevented even without EMV had the merchant installed P2PE (point to point) encryption technology. This is where the card data located either on the magnetic stripe or the EMV chip is encrypted on the credit card terminal immediately when it is scanned, and stays encrypted until it reaches the payment processor or payment gateway. So if the credit card data is breached, it is useless to the culprit. (Yes, without P2PE even EMV data can be breached.)

CONCLUSION

In the end, EMV is coming to the U.S., and it will eventually be the preferred method to accept credit cards. EMV combined with point to point encryption and tokenization will put your business in the most secure position as possible in conjunction with the other published PCI best practice recommendations.

Solupay is arming merchants with the ability to accept contactless payments with the multiple different terminal types that have EMV and other contactless credit card readers. Solupay maintains devices that support cardholder-initiated, contactless, NFC, PIN-based debit and traditional magnetic stripe transactions. This allows merchants to offer their customers the choice, convenience and security to initiate and complete their transaction, while maintaining control of their card during the entire process. Solupay can help you with all of these considerations..

Are you ready for the EMV revolution?