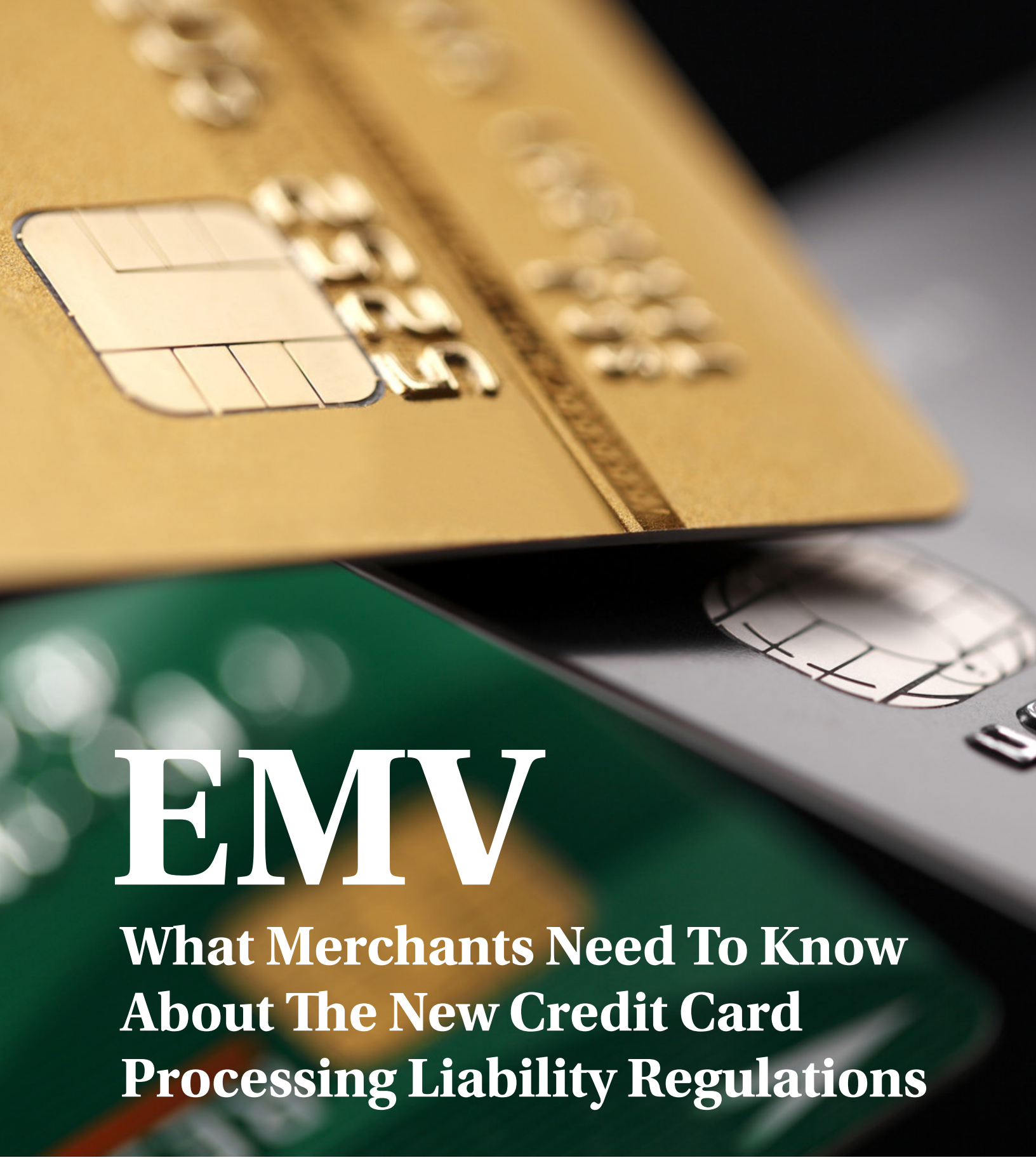

EMV

What Merchants Need To Know About The New Credit Card Processing Liability Regulations

MPX
MERCHANTPRO EXPRESS

How To Be Compliant
Post-October 1 EMV Deadline

Share This

Meet EMV

EMV, which stands for Europay, MasterCard, and Visa, is a type of credit and debit card with an embedded microchip that holds concealed information in the form of a code.

With every purchase made, the microchip produces a different code, so none is used more than once. This is unlike credit and debit cards that have a magnetic stripe on the back, which allows the same data to be transferred for every payment. The microchip is visible on the front left side of the card, above the card number. Instead of swiping an EMV card, another type of terminal is required, into which the card is inserted while its information is deciphered. EMV cards possess both the microchip and magnetic stripe, so if a retailer has not yet switched to EMV technology, a purchase can still be made with an EMV card.

EMVCo—a consortium of credit companies that manages, maintains and enhances EMV specifications for payment systems—developed this technology in order to make credit and debit card data less vulnerable to counterfeit card fraud, an issue in many countries.

Leading payment systems industry newsletter The Nilson Report states that at the end of 2012, $11.27 billion was lost worldwide due to card fraud.[1] As a result of EMV's unique coding technique, stealing someone's card information, unless a card is actually taken out of its owner's possession, is much more difficult. Additionally, although EMV's name only refers to three credit card companies—with Europay having since merged with MasterCard—other companies associated with EMV include Discover, American Express, JCB and UnionPay. Since many well-known companies have adopted EMV technology, the cards are easy to access, especially now that it's after October 1st. In fact, many consumers received EMV cards from their issuing banks before the October 2015 deadline.

EMV is available internationally and is growing in usage each year.

More than 80 countries have embraced this payment method. According to Mercator Advisory Group—a leading global advisory and analytical firm to the payments and banking industries—as of January 2014, several countries have seen a decline in fraudulent activities involving counterfeit cards, including the United Kingdom and Australia.[2] EMVCo also released the amount of EMV transactions made in-person as of late 2014: 80% of transactions in Africa and the Middle East were made with EMV cards, as well as 85.41% in Canada, Latin America and the Caribbean. The percentage reached new heights in Europe Zone 1—Ireland, Monaco, Holland, Luxembourg, Denmark, Belgium, Germany and France—with 96.60%. However, in comparison, the United States only reached 0.12%.[3] That may begin to change now that the October 2015 liability shift has taken place.

Share This

It's After October 1st. Now What?

New credit card processing regulations are officially in effect in the United States. Merchants are now responsible for any fraudulent card activities carried out in their place of business.

Previously, if a person's credit or debit card was used by somebody else, the issuing bank was liable; businesses where these purchases were made were usually not required to refund the card owner. This new liability shift moved the accountability away from issuing banks and onto retailers. However, the policy is only applicable if a business chooses not to utilize EMV-enabled point of sale (POS) systems and the card in question is EMV-enabled.

So, if both the merchant and consumer possess EMV-enabled products, the responsibility would fall back into the hands of the issuing bank. Furthermore, the liability shift involves store cards as well; a merchant, such as Macy's, is now responsible for any card-present fraudulent transactions that occur with non-EMV Macy's store cards.

Therefore, if customers have not already received new store cards, they probably will soon. Lastly, in a situation where a business is using EMV terminals and a fraudulent transaction occurs with a non-EMV card, the issuing bank would be liable once again. Responsibility does not just pertain to retailers, but with more people obtaining EMV credit or debit cards, businesses appear to be at a heightened risk compared to issuing banks.

The switch to EMV technology is not required.

That is, retailers will not be punished if they do not switch to this system. There are not any direct legal issues or fines they will face.

Since EMV use is on the rise in the United States, retailers are more likely than ever to be liable for actions not involving their core business.

The Aite Group—an independent advisory and research firm focused on business, technology and regulatory issues and their impact on the financial services industry—expects the number of EMV consumers to increase, specifically in the United States. **A June 2014 prediction forecasts that 70% of all credit cards and 41% of all debit cards in the marketplace will have an EMV microchip by the time this year concludes.**[4]

Share This

Keep in Mind...

EMV products are receiving even more attention in the merchant services industry since the October 1st deadline.

More and more countries are seeing a tremendous improvement in counterfeit card fraud prevention. Still, there is a possibility a card can be stolen. The EMV microchip cannot stop a fraudulent transaction that is conducted online; it only affects card-present payments. Unfortunately, online fraud is also increasing internationally.

The EMV microchip cannot stop a fraudulent transaction that is conducted online.

It only affects card-present payments.

Global payment technology solutions company First Data Corporation analyzed a study done in the United Kingdom between 2000, one year before their EMV move, and 2010, in which the percentage of losses from fraud is measured. The results indicate counterfeit card fraud decreased from 34% of total losses from fraud to 13%, whereas card-not-present fraud increased from 23% to 62%.[5] With EMV clearly tackling the counterfeit card fraud issue for card-present transactions, a move from this type of fraud to card-not-present fraud may continue to increase. With that said, EMV cards also have a 16-digit number on the front as well as a three-digit code similar to magnetic stripe-only credit and debit cards. If that information gets into the wrong hands, the possibility of theft still exists.

Additionally, the transition to EMV did not happen overnight. Not every merchant and consumer had EMV-enabled products by October 2, 2015. This is going to be a process, which may be creating a bit of confusion and frustration right now, because someone who has just received an EMV card may be unhappy if the stores he or she shops at has not made the switch since the microchip cannot be used without an EMV-enabled POS system. Additionally, purchasing EMV products is going to be expensive for merchants. On October 16, 2014, global banking and payments technologies provider FIS' Payments Leader trade publication referred to a Javelin Strategy and Research study predicting EMV-enabled POS systems will cost approximately $6.75 billion dollars alone in the United States.[6] According to merchant services provider MerchantPro Express, one EMV terminal starts at $388, meaning that if one merchant purchases five terminals, the cost will be about $2,000. However, retailers should remember that with every consumer who converts to EMV cards and every case of counterfeit card fraud that occurs at their place of business, the greater the chance the business could lose money as a result of the liability shift. The question remains:

Are merchants willing to take that risk? Or should they spend the money in order to avoid responsibility and keep up with the new standard?

To Switch or Not to Switch?

As aforementioned, one of the challenges for merchants making the switch to EMV technology is the cost, though there are some key benefits.

With the collaboration of both businesses and consumers, the country can reduce counterfeit card fraud occurrences. According to Payments Source, the United States will spend about $10 billion in liability costs by the end of 2015 due to counterfeit card fraud as well as lost or stolen cards.[7] These staggering numbers indicate that a business failing to adopt EMV technology may ultimately suffer in the long run.

Having one card-present payment method for a business can be a benefit as well. Retailers may prefer to be as consistent as possible with their payment methods. So, as consumers continue to adopt EMV cards, the amount of credit and debit card swipes will most likely fizzle out, making the preferred card payment transaction EMV-enabled. Not to mention that consumers who want to utilize the microchip on their EMV cards would appreciate retailers who purchase EMV terminals because that would help them avoid using the magnetic stripe. If most consumers have EMV cards, but merchants do not have the right terminals for properly using those cards, protecting credit and debit card information will still be just as tough as before, because card-present payments are made the same way.

Furthermore, since the EMV liability shift has come as a surprise to many, business owners should not hesitate to educate themselves more on the subject and figure out what is the best move for their business. One way to accomplish this is to attend EMVCo seminars, which take place all around the world. More information can be found on the company website: **emvco.com**. Another way is to contact a merchant services company, such as MerchantPro Express, that can offer consultation, provide detailed information in terms of what EMV terminals are available, and explain what makes them different from other terminals. A merchant can also learn terminal prices and purchase them from a merchant services company.

Plus, older terminals will not be available eventually. As MerchantPro Express points out, a merchant who is looking to buy new terminals in the future will probably end up getting EMV-enabled terminals anyway. First Data Corporation also suggests working with a merchant services provider in order to create an effective schedule that will oversee a retailer's EMV transfer timeline.[8] In an ever-changing world of technology, staying up-to-date on major advancements and managing transitional periods are essential components to being successful.

The United States will spend about $10 billion in liability costs by the end of 2015 due to counterfeit card fraud as well as lost or stolen cards.

PAYMENTS SOURCE, 2014

Stay Tuned...

EMV's presence, particularly in the United States, will continue to expand. Another liability shift will transpire October 1, 2017. This time, it concerns automated fuel dispensers. However, the same rules apply. The businesses who fail to purchase EMV terminals will be accountable for any fraudulent transactions made with an EMV card at one of their automated fuel dispensers. And even though the liability shift is two years away, it appears as though retailers are not wasting any time. An August 2015 report by payment systems manufacturer and supplier Gilbarco Veeder-Root found that orders for EMV-enabled automated fuel dispensers have skyrocketed in recent months, specifically this past June.9 Since EMV cards are available in the Unites States, companies who know that they will inevitably make the switch at some point or another are adapting to the imminent liability shift early.

EMV technology may be new to some, especially merchants in the United States, but the technology has been making headlines in other parts of the world, including Europe, Asia, and Australia, for years.

Although there are some initial challenges to the new standard, there is also confirmation of a significant counterfeit card fraud decline in other countries after making the switch to EMV technology. As more time progresses, consumers are said to be abandoning their old, swiping ways and turning to EMV cards to help better protect them.

Merchants should not only be aware of what exactly the new regulations are, but they should continue to find out more about EMV terminals in order to effectively determine when or if they should do away with their current credit and debit card processing terminals. **Reliable merchant services companies such as MPX** can help teach merchants about the benefits of EMV products and better inform them to properly decide their next move. ■

SOURCES & REFERENCES

1. Nilson Report, "Global Card Fraud" (Chart). August 2013.
2. Mercator Advisory Group, "EMV Adoption and its Impact on Fraud Management Worldwide." January 2014.
3. EMVCo, "Worldwide EMV Deployment Statistics." 2014.
4. The Aite Group, "Seventy Percent of U.S. Credit Cards to be EMV Enabled by the End of 2015." June 10, 2014.
5. First Data Corporation, Dom Morea, "EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions." 2011.
6. Payments Leader, "Will Retailers be Ready for EMV by Oct 2015?" October 16, 2014.
7. Payments Source, Dick Mitchell, "Missing the EMV Liability Shift Bears a Huge Cost." August 4, 2014.
8. First Data Corporation, "What Merchants Need to Know About EMV." 2012.
9. Gilbarco Veeder-Root, "Major Retailers Acting Ahead of EMV Compliance Deadline with Dispenser Marketing Upgrades." August 4, 2015.

SUBSCRIBE For more information on topics in this eBook, visit **news.merchantproexpress.com**