Some Frequently Asked Questions

Q: Why is this EMV conversion such a big deal?

A: Credit card fraud can be reduced by 90% with the implementation of EMV throughout the U.S.

Q: What happened on October 1, 2015?

A: On October 1, retailers will still be able to process bankcards as usual, but there will be a liability shift. The in-store counterfeit fraud liability shift for merchants will ONLY affect liability in the following situation: A fraudulent EMV bankcard is used in a traditional magnetic stripe-only terminal, and there is a chargeback on that fraudulent EMV card. In only that case, would the retailer be liable. In all other liability situations (card-not-present transactions, lost and stolen fraud, and non-EMV card), the liability remains on the bankcard issuer.

Q: What is the liability shift?

A: If a fraudulent EMV bankcard is used in a traditional magnetic stripe-only terminal, and there is a chargeback on that fraudulent EMV card, then the liability shifts to the retailer. In only that case, would the retailer be liable. The liability rules after October 1, 2015 are as follows:

Counterfeit Scenario	Card type	Pin pad type	Financial Liability
1	Mag stripe	Mag stripe terminal	Card Issuer
2	Mag stripe	EMV enabled terminal	Card Issuer
3*	EMV card	Mag stripe terminal	Merchant
4	EMV card	EMV enabled terminal	Card issuer

***This is the only liability shift change.**

Q: Can I still accept bankcards after October 1, 2015?

A: Yes, you can continue to accept bankcards.

Q: What if my pin pads are not EMV-ready?

A: You can process bankcards the same way as you did before, except that there is a liability shift if you accept a fraudulent EMV card.

Q: Why is it taking so long to get EMV implemented?

A: The card brands (VISA, MasterCard, AMEX, and Discover) did not anticipate the significant changes needed by the processor, pin pad manufacturer, and POS software vendor. Epicor could not start our coding work until we had the changes and requirements from both the processors and the pin pad manufacturers. The processor and pin pad manufacturers are still discovering new issues.

In addition, the implementation of EMV for Eagle customers, who process with over 30 different debit keys and four major processors, is very complex and will required a secure update of your debit keys to EMV-ready debit keys and uploading the EMV firmware. Because of this complexity, Epicor will help to manage the conversion so retailers are not without pin pads.

Q: Where can I learn more about EMV?

A: Retailers should visit **www.epicor.com/emv**. On this site, retailers will find detail on EMV and the process for implementing it in their business.

Q: Is there a different process if I purchased third-party pin pads?

A: Yes, there will be a fee from Epicor and/or another party to securely change the debit key and allow EMV to be loaded onto your third party pin pads.