Understanding the EMV Conversion  
Is Your Business Ready?

The EMV Conversion takes effective October 2015, that is the deadline for all merchants who accept credit cards in a **CARD PRESENT (FACE TO FACE)** environment will be required to convert to EMV enabled terminals for credit card processing.

EMV stands for Europay, MasterCard and Visa, a global standard that ensures chip-based payment cards (also known as smart cards) and smart pay terminals are compatible around the world. Static magnetic stripe cards will be replaced by these EMV chip cards, which will contain new technology to further validate the payment being made.

**The Reason for the Shift**

The dynamic elements of this new chip technology are capable of more sophisticated security which will make account data harder to steal. When the microprocessor embedded chip connects with an EMV enabled terminal, the smart card technology provides for another form of card identification for the transaction. This will reduce the risk of counterfeit and lost or stolen cards being used at ATM’s or retail points of sale.

EMV cards may be new to the United States but they are in wide use globally. There are over 2 billion chip cards in circulation in over 80 countries world-wide. Chip cards have become popular due to the increased security protection they offer compared to traditional magnetic stripe cards.

**What this Means for Merchants**

Businesses need to be aware of the liability shift scheduled to go into effect on October 1, 2015, which is a date determined by the credit card associations. That means, if by this date a business accepts and processes a counterfeit transaction on a non-EMV enabled terminal, the liability is the on the business, not the card issuer.

*Information provided by the card networks, at this time, applies to retail merchants in card present environments. The deadline for businesses with automated fuel dispenser technology is October 2017 and deadlines for other industries are to be announced. You can count on East Commerce Solutions, CAP COM’s chosen partner for merchant services, to provide the most accurate information and cost effective solutions to meet these mandated requirements and protect businesses.*

**Merchants Who Don’t Make the Transition**

Payments can still be made with a chip card on non-EMV terminals, however, if the purchase is fraudulent, the business will be liable for the cost of the transaction.

**Making Payments with EMV Terminals**

Instead of swiping, the customer will insert the card into the terminal, chip first, face up. The card must remain in the terminal during the entire transaction. As prompted, depending on the requirements of the card distributor, the customer will sign the receipt or enter their PIN to complete the transaction. When the purchase is complete, the customer will remove the card.
It's important to understand the cardholder must insert the card and this dipping process takes longer than the traditional swiping method. The terminal prompts for next steps and several seconds pass for each part of the transaction process.

Can I still accept magnetic stripe cards with an EMV enabled terminal?
Yes. The new EMV enabled terminals are designed to accept EMV chip cards and magnetic stripe cards to help during the transition to EMV. With a new EMV enabled terminal you won’t need two terminals for both types of payment cards.

What if I decide not to upgrade to a new EMV enabled terminal?
The Payment Card Networks have announced that on October 1st, 2015*, counterfeit fraud liability, which has traditionally been losses incurred by the card issuer, will be assumed by any merchant customer that does not have EMV enabled equipment capable of detecting the fraudulent card. This means, by the date, if your business accepts and processes a counterfeit card transaction on a non-EMV terminal, the liability for that fraudulent transaction is yours, not incurred by the card issuers.

Card-Not-Present Transactions
*While not affected by the liability shift of EMV*, it is important that merchants still take precaution against fraud in card-not-present situations such as internet and over-the-phone purchases. When accepting a card-not-present payment, merchants can authorize the legitimacy of a card by making sure all the card information is present and valid such as address, expiration date, and the card security codes located on the front or back of the card. The payment card networks provide verification services to help confirm this information.

Other signs of a potential card-not-present fraudulent transaction are first time shoppers, purchasing very large orders, orders that include several of the same item, rush or overnight shipping requests, shipping to an international address, orders involving high value items, multiple transactions on one card in a short amount of time, multiple transactions on one card with one billing address but multiple shipping addresses, and multiple card payments from the same IP address. *Merchants can refer to the payment card network websites for additional tools, guides and services on security and fraud prevention.

How You Can Prepare Your Business
CAP COM's Merchant Services Program, offered through East Commerce Solutions, can get your business ready for the EMV transition. We will replace your terminal with a low-cost solution that doesn’t require up-front costs or long-term lease commitments.

Having an EMV compliant terminal ensures that the business owner is complying with the new mandates required to protect themselves against liability for fraudulent transactions.