“EMV” stands for Europay, MasterCard and Visa, the original developers of chip card standards. Chip card technology increases the security of card-present transactions by requiring communication between a computer microchip embedded in the card and a chip reader contained within a chip-enabled terminal. Chip card technology seeks to eliminate card-present counterfeit fraud.

When the chip card and chip-enabled terminal interact, a set of contacts engage and power is provided to a microprocessor within the card’s chip. A dynamic authentication occurs during each chip transaction, validating that the card is legitimate. This process is the enhanced security provided by chip technology.

A chip transaction can only occur when a chip card is used with a chip-enabled terminal.

Performing a chip card transaction at the point-of-sale in a contact interaction:

1. Insert card.
   Instead of swiping, the card is inserted into the terminal, chip first, face up.

2. Leave the card in the terminal.
   The card must remain in the terminal during the entire transaction.

3. Customer signs receipt or enters PIN.
   The customer will either enter their PIN to complete the transaction or sign the receipt.

4. Remove Their card.
   When the purchase is complete, the card must be removed from the terminal and handed back to the customer.

Performing a chip card transaction at the point-of-sale in a contactless interaction:
In order for a chip to work in a contactless interaction, both the card and the terminal must possess near-field communication (NFC). When the NFC card’s chip is brought within two inches (5 cm) of the NFC-capable terminal (tapped) it transmits the account information.

What happens if a chip card is swiped, not inserted, into a chip-enabled terminal?
The terminal will prompt the user to instead insert the card so that the chip can be read. The terminal will not allow a swiped chip card transaction to process unless it determines that there is an issue with the chip after it is inserted.
Participation in chip card technology does include some expenses for both card issuers and merchants. Issuers will need to invest money in issuing the costlier chip cards to their cardholders, and merchants will need to invest in the more sophisticated chip-enabled terminals. Since chip technology aims to prevent the use of counterfeit cards and protect card-present transactions, a consumer using a chip card at a chip-enabled terminal should result in a completely legitimate transaction.

The liability shift is the result of decisions made by the card brands (e.g., Visa, MasterCard). Chip card technology is expected to enhance payment security, and the liability shift is “designed to encourage EMV chip card issuance and acceptance”.

The card brands have stipulated that, **AS OF OCTOBER 1, 2015, ANY MERCHANT NOT USING A CHIP-ENABLED TERMINAL WILL BECOME RESPONSIBLE FOR SOME COUNTERFEIT CARD FRAUD.**

**October 1, 2015**

It is in each merchant’s best interest to begin using chip-enabled terminals and training customer-facing staff on the processes involving chip cards.

**What can you do to prepare for EMV?**

- Use a chip-enabled terminal and terminal application.
- Train customer-facing staff on processes involving chip cards.

<table>
<thead>
<tr>
<th>VERIFONE</th>
<th>INGENICO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminal</strong></td>
<td><strong>Terminal</strong></td>
</tr>
<tr>
<td>Countertop Option</td>
<td>Countertop Option</td>
</tr>
<tr>
<td>VX 520 DC SC contact/contactless</td>
<td>VX 680</td>
</tr>
<tr>
<td>Wireless Option</td>
<td>Wireless Option</td>
</tr>
<tr>
<td>VX 680</td>
<td>iWL255</td>
</tr>
</tbody>
</table>

FIS™ understands the complexity of EMV/chip card technology, and we are here to help you prepare for this important advancement in the payments industry. Contact us today at 800.552.5828, option 5, to learn more about the simple solutions we have available.