CRS El Paso
2208 TEXAS AVE
EL PASO, TX 79901
P 915.544.1402 F 915.231.6288
NCR Aloha
Authorized Hospitality Solutions Provider

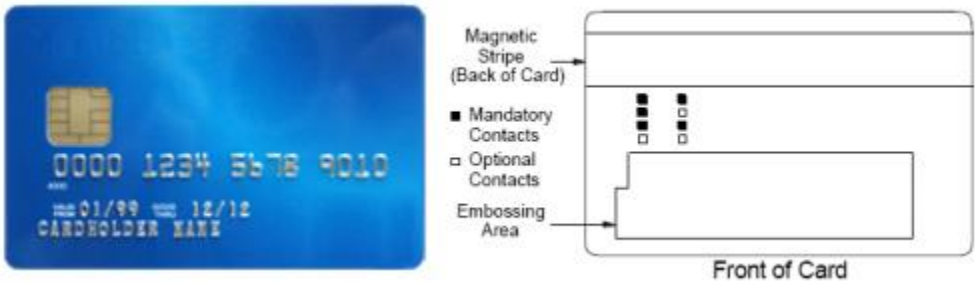
IMPORTANT THINGS TO KNOW ABOUT EMV

- **October 1, 2015 is the date that liability shift occurs (this date is a risk and liability shift NOT a mandate.**
- **NO FINES will be associated with failure to implement EMV on that date.**
- **After that date, liability shifts to the party that is the least EMV-compliant in a fraudulent transaction.**
- **"Magnetic strip" cards will still be in circulation for some time.**
- **EMV will not prevent data breaches from occurring, but will make it harder for criminals to profit from stolen data.**

What is EMV?

"EMV® is a global standard for credit and debit payment cards based on chip card technology" taking its name from the card schemes Europay, MasterCard, and Visa - the original card schemes that developed it. The standard covers the processing of credit and debit card payments using a card that contains a microprocessor chip. A chip card used in payment transactions is usually a card with a magstripe at the back plus a chip in front which is a self-contained microprocessor.

A chip card can be,
- Contact only
- Contactless only
- Dual-interface, i.e. contact and contactless



Cards used in EMV transactions are basically MSR cards with a chip, which is a self-contained computer.

How does EMV chip technology work?

Your EMV-enabled device will communicate with the chip inside the customer's smart card to determine whether or not the card is authentic. Generally, the terminal will prompt the customer to sign or enter a PIN to validate their identity. This process enhances the authentication of both the card and cardholder, effectively reducing the possibility that your business will accept a counterfeit card or be held liable for a fraud-related chargeback.

Why is the United States migrating to EMV?

Issuers around the world are including chips in bank cards and merchants are moving to EMV-compliant terminals to increase security and reduce fraud resulting from counterfeit, lost and stolen cards.

What makes EMV different than the traditional magnetic stripe card payment?

Simply put, EMV (also referred to as chip-and-PIN, chip-and-signature, chip-and-choice, or generally as chip technology) is the most recent advancement in a global initiative to combat fraud and protect sensitive payment data in the card-present environment. A cardholder's confidential data is more secure on a chip-enabled payment card than on a magnetic stripe (magstripe) card, as the former supports dynamic authentication, while the latter does not (the data is static). Consequently, data from a traditional magstripe card can be easily copied (skimmed) with a simple and inexpensive card reading device – enabling criminals to reproduce counterfeit cards for use in both the retail and the CNP environment. Chip (EMV) technology is effective in combating counterfeit fraud with its dynamic authentication capabilities (dynamic values existing within the chip itself that, when verified by the point-of-sale device, ensure the authenticity of the card).

What other incentives are there to accept chip cards?

In addition to the reduction of fraud and related chargebacks, there are other cost savings associated with EMV acceptance. The payment brands are doing their part to ensure that chip-bearing customers can pay at chip-enabled businesses. For example, Visa and MasterCard have issued upcoming rules and guidelines for processors and merchants to support EMV chip technology. Visa is introducing their Technology Innovation Program (TIP) to the U.S. region, which waives an annual PCI-DSS audit if 75 percent of the merchant's Visa transactions are processed through a dual contactless and contact EMV certified device. MasterCard is introducing their PCI-DSS Compliance Validation Exemption Program to the U.S. region, which also waives the annual PCI-DSS audit if 75 percent of the merchants' MasterCard transactions are processed through a dual contactless and contact EMV certified device.

Another Visa and MasterCard ruling is the liability shift. Once this goes into effect, merchants who have not made the investment in chip-enabled technology may be held financially liable for card-present fraud that could have been prevented with the use of a chip-enabled POS system.

How am I impacted by the liability shift?

With the liability shift, if a chip card is presented to a merchant that has not adopted a terminal that is certified for chip card acceptance, liability for counterfeit fraud may shift to the merchant's acquirer – who may then pass this fee back to the merchant. The liability shift encourages chip adoption since any chip-on-chip transaction (chip card read by a chip certified terminal) provides the dynamic authentication data that helps to better protect all parties. In addition, if a counterfeit magnetic stripe card is presented at a chip certified terminal, the liability for the counterfeit fraud will be the responsibility of the card issuer.

Am I required to support EMV?

No, you are not required to support EMV in the U.S. region at this time. However, one item that you need to consider is that even if your organization hasn't been targeted by high levels of card present fraud in the past, you may be putting yourself at risk in the future, as fraud will migrate to the weakest technology (magnetic stripe) Therefore, you may want to ensure that all your terminals are chip capable and that your payment processing application can support chip card acceptance.

PCI DSS Applicability in an EMV Environment

EMV must be considered in the context of the current transaction-processing environment where the confidentiality of cardholder data from EMV transactions, along with sensitive authentication data from non-EMV transactions, remains fundamental to ensuring the integrity of the payment system.

While EMV can substantially reduce fraud in card-present transactions, it does not automatically satisfy PCI DSS requirements for the protection of cardholder and sensitive authentication data.

Within this context of current EMV deployments, the need to protect the confidentiality of cardholder and sensitive authentication data as prescribed by PCI DSS is still a critical part of the industry's overall effort to prevent that data being used for fraudulent transactions in other environments.

In the future, should EMV become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence, the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly.

Today EMV and the PCI DSS, as well as the PA-DSS and PTS standards, are complementary and form important layers in providing a holistic approach to the objectives of reducing overall fraud and securing cardholder data in the payment industry. In those markets which have migrated or are in the process of migrating to EMV, payment industry stakeholders should use EMV and PCI DSS together to reduce fraud and increase security.

Does NCR and Cash Register Systems of El Paso have a solution for my Aloha System?

The payment landscape is currently undergoing massive disruption from the EMV liability shift, data security breaches that continue to occur and the mobile wallets entering the market.

EMV is important, but we also want to make sure that you understand that it is just one component of the payment security. Your biggest priority should be focused on protecting your restaurant from all data security-related threats.

Our approach is to help you bridge the gap between all of the payment trends that are impacting your business and give you exactly what you need – the ability to be more secure, take mobile payments and accept EMV payments.

NCR Connected Payments is an NCR-created cloud-based platform that enables our customers to implement point-to-point encryption, EMV and mobile wallet capabilities all in one solution. It is currently in use in more than 17,000 NCR Retail customer locations today.

Connected Payments will be available later this year. In the meantime, we would like to do a free assessment of your existing technology system to help make sure that you are ready for its availability and prepared for EMV acceptance.

The minimum Aloha Point of Sale software version required for EMV acceptance is 12.3.

Please contact us for any questions, concerns or to schedule an appointment for the free assessment of your system.

Cash Register Systems of El Paso, 2208 Texas Ave, El Paso, TX 79901
Phone (915) 544-1402 Fax (915) 231-6288 email support@crsep.com