DCRS solutions

RETAIL • HOSPITALITY • RESTAURANT

Delivering Certified Results & Satisfaction

What you need to know about EMV

Date 12.27.15,

Updated 10.3.16

Since October 2015, when the chargeback liability shifted to the Merchant, for any transaction that used a counterfeit mag-stripe (from a card with a chip), on a mag-stripe/non-chip terminal, a new scam has developed, for what some are calling "Chargeback fraud."

- Customer using a Chip Card disputes a very large transaction used on a non-EMV device (mag-stripe only, non-chip terminal)
- Customer then fraudulently disputes that "very large transaction" by reporting the Chip Card lost or stolen, avoiding liability for the charge
- Although Card Company/Bank "shuts down" the Card, this type of customer sacrifices the inconvenience of waiting for a new card, for not being responsible for the large transaction
- Similar instances, for even small transactions, are being reported
- Video of that Customer using the Chip Card as proof of use, is not being accepted as evidence to dispute a chargeback, by Card Companies/Banks
- **In these scenarios, Merchants still using non-EMV devices are being saddled with Chargebacks, losing no matter, and some are being targeted**

With so many inquiries regarding the acceptance of EMV in Restaurants and Stores, DCRS has gathered what we feel is accurate information on EMV, and to become educated on EMV, before making any decision.

The Europay MasterCard Visa (EMV) is a standard for using chip-based payment cards. EMV applies to everyone in the chain: Merchant, Card Reader at POS, Payment Gateway, Payment Processor, and Card-issuing Bank. Migrating payment systems in the U.S. to the EMV standard will take a long time and will offer fewer security benefits to Merchants.

EMV helps prevents the use of Counterfeit Cards (making it harder to clone cards and use them to make fraudulent transactions—**that is why the Card Brands, MasterCard and Visa, want this to happen**).

EMV does not prevent Cardholder Data from being stolen (**that is the objective of Point-to-Point Encryption, or P2PE**). One of the biggest obstacles of EMV adoption in the U.S. is cost: This is estimate at 35 Billion dollars, to fix a 12 Billion dollar problem.

This is also not about the Merchant having a card reader at POS can read a chip-based card, as all others in the payment chain must be able to accommodate the same: **The Payment Gateway, the Payment Processor, and the Card-issuing Bank all must also be able to accommodate the EMV standard**. Card-issuing banks will need to spend tens of millions to upgrade their networks and internal systems if they want to be ready for PIN credit transactions.

And there is still uncertainty about “Chip & PIN” versus “Chip & Signature”. MasterCard and Visa have left the decision to the Card-issuing banks in the U.S. to decide which route they want to take. Some feel “Chip & Signature” will ultimately prevail. Some doubts remain over the willingness of Merchants accept the costs associated with supporting EMV.

So with all this indecision in the industry, what we do know is:

- Readers must accommodate reading a Card with a Chip
- Whether it is “Chip & PIN” or “Chip & Signature” remains to be determined
- The Payment Gateway must be certified to accommodate the EMV standard
- The Payment Processor must be certified to accommodate the EMV standard
- The Card-issuing Bank must be certified to accommodate the EMV standard

An ideal source for ***accurate information around the EMV initiative***, and its impact on Restaurateurs in particular, has come from a National Restaurant Association webinar, found at:

http://www.restaurant.org/Events-Networking/Events/Webinars/EMV-and-Restaurants-What-You-Need-to-Know

The key points to understand (for now) are:

- ***EMV is NOT PCI-DSS related***

- EMV “liability shift” exposure can be considered by some as less consequential when applied to certain typical restaurant transaction volumes and check averages. The Merchant’s liability currently applies only to any transaction that used a counterfeit mag stripe (from a card with a chip), on a mag stripe/non-chip terminal, after October 2015.

EMV requires external readers—generally not supplied by a POS provider such as Oracle Hospitality (formerly MICROS)—but rather the Payment Processor. The primary reason is due to the “control” surrounding chain of custody, tamper protection, and the specific encryption key injection, ***essentially requiring direct procurement between the end user and the Payment Processor vendor*** (i.e. Customers secure certified, injected readers directly from the Payment Processor chosen; reader recommendation comes from the Payment Processor providing the solution).

Payment Processors understand that such a change represents a large commitment, and once committed, a Merchant is unlikely to change Processors.

Table Service presents even more challenges, as that requires a change in basic operations, from the traditional authorize/tip/adjust/batch methods, to one whereby the total amount—including the tip—must be rendered while the EMV enabled card is in the reader with the guest present, for the duration of the transaction.

Ideally, a portable EMV device (PATT—Pay at the Table) would also be integrated in the POS system via a “non-network” link such a Bluetooth or serial (for *Point to Point Encryption*—P2PE), passing only the amount and token information. Additional device functionality for *Near Field Communications* (NFC, as in ApplePay, GoogleWallet, etc.) must also be considered, as mobile payments will most likely become increasingly popular.

Oracle Hospitality (MICROS) was involved with EMV in Europe since introduction of this technology. Currently supported MICROS workstation will function in this environment, based on appropriately integrated Payment Processors. Most Payment Processors are seeking to provide viable P2PE/EMV/NFC/PATT solutions to integrate to most MICROS systems.

DCRS encourages any Restaurant or Retail store to compute and consider their potential liability against the investment costs and operational changes that are required to satisfy EMV acceptance, before making any decision.

Because EMV is simply a liability shift and not a mandate, merchants should first determine if the cost to upgrade to EMV is justified.

Merchants who regularly experience charge backs or fraudulent card use may want to upgrade to EMV sooner, while those that don’t have in-store fraud or disputed transaction issues may be better served to wait until their next POS upgrade to move to EMV – if at all.

Finally, before investing solely in EMV, Merchants should also consider other payment functionalities that include *Point to Point Encryption* (at a minimum)*,* and if applicable, *Near Field Communications* (for mobile payments), and *Pay at the Table* (for Table Service operators), as noted earlier.

Many EMV solutions <u>do include</u> *Point to Point Encryption (P2PE),* which <u>helps prevent</u> Cardholder Data from being stolen, and helps to reduce the Merchant’s ‘in-scope’ responsibility for PCI compliance.

<u>Statement from Qualified Security Assessors QSA):</u>

Encrypted cardholder data (stored or transmitted) being out of scope is based on whether or not that data meets the following definition.

“It is possible that encrypted data may potentially be out of scope for a particular entity if, and only if, it is validated (for example, by a QSA or ISA) that the entity in possession of the encrypted data does not have access to the clear text cardholder data or the encryption process, nor do they have the ability to decrypt the encrypted data.”