EMV Chip Security

Are you EMV ready? Is your data safe & secure?

October 2015 – the date US based credit acquirers and processors are required to be EMV (Europay, MasterCard, Visa) compliant. Although it is not mandated for merchants and processors at this time, this date will come at a cost for those who have not adopted this more secure and efficient technology. Merchants and processors who do not adopt the new EMV standards over the current outdated magnetic strip cards by October 2015 will assume liability for fraudulent transactions, resulting in a direct hit to the bottom line – ouch!

What does this mean?

EMV is the new standard for payment processing. Restaurants, retailers, SMBs, and any other businesses that have a POS (Point of Sale) system are required to upgrade their system to accept cards with an EMV chip embedded in them. The reason for this upgrade requirement is simple – SECURITY! The US is one of the last to still use magnetic strips. A majority of other counties have migrated to EMV chip technology already.

What are the benefits of EMV?

EMV (also referred to as chip-and-PIN, chip-and-signature, or simply chip technology) is an advancement in technology and part of a global strategy to combat fraud and protect sensitive data in both card-present and card-not-present (CNP) environments. Data on a magnetic strip is static and consequently, data from the magnetic strip can be easily copied, enabling criminals to reproduce counterfeit cards for use in both the retail and CNP environments.

EMV allows dynamic authentication capabilities, providing POS systems the ability to verify the cards legitimacy, value and clone validations.

"Retailers incur $580.5 Million in debit card fraud losses and spend $6.47 Billion annually on credit and debit card fraud prevention annually." (*Payments Journal, Feb. 2012*)

EMV	Swipe
A cardholder inserts an EMV chip card into a reader or taps the card in the case of a contactless transaction.	A cardholder swipes a magnetic stripe card at a terminal.
The POS terminal identifies what payment brand's application is on the card.	Static Track 1 and/or Track 2 data is captured
The terminal selects the appropriate EMV application and uses a data set associated with each payment brand to enforce the brand's application requirements.	An authorization request is made
The card and terminal follow an EMV-specified protocol process to conduct a dialog that allows each of them to execute their respective risk management processes.	The transaction is sent to an acquirer, then routed to the appropriate payment brand or network, and finally delivered to an issuer for authentication and authorization.

(Source: www.emvco.com)

Upgrade

Credit Card and debit card fraud resulted in losses amounting to $11.27 billion during 2012. Card issuers and merchants incurred 63% and 37% of those losses, respectively, with the following transactional breakdown:

- **During 2012 credit card and debit card gross fraud losses accounted for roughly 5.22₵ per $100 in total volume, up from 5.07₵ per $100 in 2011**

- **In 2012, US accounted for 47.3% of the worldwide payment card fraud losses but generated only 23.5% of total volume**

(SOURCE: NILSON REPORT, AUGUST 2013)

ESSINTIAL
ENTERPRISE SOLUTIONS

Why should I move to EMV?

October 2015 is the date that triggers a shift in liability from card issuers to card processors, and to merchants as well.

Merchants that do not accept EMV cards by October 2015 will have to absorb the cost of a fraudulent charge. With already thin margins, this could substantially impact the bottom line.

How do I upgrade, and fast?

Essintial works with our customers to understand each unique set of requirements, formulate a strategy and develop an implementation plan while keeping you involved every step of the way. Once all pre-install milestones have been achieved, we go to work. We handle everything from installation and scheduling to device exchange and device destruction. Essintial will provide a certificate of destruction to certify the disposal of your old equipment. We know that every customer is different and will work with you on developing a solution to fit your needs.

PCI Compliance

Essintial adheres to PCI requirements for physical data destruction and has partnered with Smith Recycling and Armor Metal Company to ensure physical destruction takes place within all DOD guidelines and is environmentally friendly.

Chain of Custody

Devices that are sent to Essintial's depot are delivered in secure, tamper proof packages to ensure they arrive unmodified. We take security very seriously, and this level of security provides our customers with peace of mind.

The device is logged, diagnosed, repaired and returned. If the device is faulty or the package has been damaged, Essintial will dispose it in a secure manner in compliance with DOD guidelines.

How can Essintial Help?

Most customers that come to Essintial looking for help do not have the resources or the technical field staff in place for a large scale deployment. We will work with you to understand your cost, quality, implementation requirements and deployment strategy. We will formulate a plan based on your needs and propose a solution that will enhance your overall objective. Our success is achieved by our partnership with our customers and we take pride in our ability to communicate and problem solve. No one can predict when an issue might arise, but if one does, we have the mitigation strategy and contingency plan already in place.

To learn more about EMV Chip Technology and how Essintial can help you get started, visit www.essintial.com or call at 1-800-384-7000 and speak to a customer service representative.