

WHEN MUST EMV BE ADOPTED?

EMV functionality is not required or mandated. However, the Fraud Liability Shift takes place October 1, 2015. After October 1, 2015, the liability for card-present fraud will shift to whichever party is the least EMV-compliant in a fraudulent transaction. The party that is the cause of a chip transaction not being conducted will be held financially liable for any resulting card-present counterfeit fraud losses.



The Liability Shift applies to counterfeit cards, not lost or stolen cards.

When considering the ROI for EMV it is important to understand what the Liability Shift, which takes place October 1, 2015, really means to your organization.

EMV's main purpose is to provide mechanisms to authenticate and validate cards, preventing thieves from duplicating or counterfeiting cards. EMV is not the silver bullet for all fraud and does not add protection from hackers. An EMV card does not safeguard the PAN information contained on it; that will still be up to the Merchant's secure encryption and tokenization platform in combination with the encrypted EMV devices utilized in the merchant's environment. On-line, call center, and other card-not-present transactions will continue to process as they do today.

A cost/benefit analysis of EMV should include the fraud that currently occurs in your card present environment. Consider the chargeback losses that can be attributed to card fraud and estimate what those levels of card fraud will be after the liability shift begins. If card present fraud is minimal today, then it may not be worth going through the expense of an EMV upgrade immediately.