5 Things Retailers Should Know about the Shift to EMV Card Technology

EMV conversions go into overdrive as the merchant liability shift deadline approaches

The U.S. conversion from mag-stripe credit cards to EMV chip-and-pin cards* is picking up speed as we get closer to an important deadline for merchants.

Those who fail to make the switch will leave their customers more vulnerable to fraud and will incur an increased liability when fraud occurs. Here are five important things to know about the EMV technology changeover.

1. The Deadline

Each of the four major credit card issuers in the U.S., VISA, MasterCard, American Express and Discover, have established October 1, 2015 as the deadline when the liability for credit card fraud shifts to the merchant if they do not have an EMV payment system in place.[1]

Retailers and others are looking to upgrade their point of sale (POS) systems to prepare for the deadline. The conversion target for ATMs and automated fuel dispensers (AFD) comes one or two years later.

Dates when the fraud liability shifts to the merchant if EMV systems are not in place:

- October 1, 2015 – Visa, MC, Amex, Discover
- October 1, 2017 – Deadline for automated fuel dispensers (AFD) to comply.
- October 1, 2016 – MasterCard liability will shift in the U.S. for ATMs.
- October 1, 2017 – VISA liability will shift in the U.S. for ATMs.

2. How the 'liability shift' affects me

After the Oct. 1, 2015, deadline, the liability for *card-present fraud* will shift to whichever party is the least EMV-compliant when a fraudulent transaction happens.

Card-present fraud occurs when a credit or debit card is used to make an unauthorized transaction in a face-to-face setting, such as a grocery store checkout lane. It may involve the use of a stolen card or a duplicated card made using a card number and magnetic stripe information.[2]

If a fraudulent card is used at a merchant that has not upgraded their equipment to work with the chip technology, the merchant will be liable for the cost of the fraud.

If the transaction acquirer/processor hasn't offered an EMV-capable solution to merchants, or the card issuer has not issued EMV-capable cards to its cardholders, they would be liable rather than the merchant.

The EMV conversion policy[2] of the major card issuers:

VISA - The party that is the cause of a contact chip transaction not occurring will be financially liable for any resulting card-present counterfeit fraud losses.

MasterCard - If at least 95% of MasterCard transactions originate from EMV-compliant POS terminals, the merchant is relieved of 100% of account data compromise penalties. MasterCard liability hierarchy takes effect.

American Express - Will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.

Discover - Will institute a Fraud Liability Shift policy in the form of a risk-based payments hierarchy that benefits the entity that leverages the highest level of available payments security.

"The EMV chip-and-pin card liability shift is upon us. Merchants should take steps now to convert their POS technology to protect their customers and not incur serious potential fraud liabilities.

3. The consequences of not meeting the deadline

The switch to EMV is voluntary, but failing to do so exposes the business to fraud liability and the loss of customers who prefer to transact business with the more secure technology.

After the October 1, 2015 deadline, if a merchant is still using mag-stripe technology and the customer presents a chip card, the merchant is liable for the cost of any fraud.

Credit card fraud in the United States is expected to exceed $10 billion in 2015.[3] Merchants don't want to be on the hook for a share of those costs.

If a merchant has upgraded their technology to the EMV standard then the liability shifts elsewhere.[3]

- The bank will bear the cost if they haven't issued the customer a Chip and PIN card
- The credit card company is liable if the merchant and the customer both use EMV/Chip and PIN technology and fraud occurs.

Starting the transition now is critical. Manufacturers of POS equipment could run low on inventory as the deadline approaches, software compatibility issues might surface and IT consultants could be booked up.

Visa projects that 47 percent of the merchant card reading terminals in the U.S. will be upgraded to EMV chip technology by the end of 2015. Full implementation may take a couple of years based on the experience of other countries.

4. How to get ready for EMV cards

For merchants and professionals who accept credit cards, the switch to EMV involves adding new in-store POS and office technology to accept the cards and learning how to use it.

- Merchants will need to order new credit card terminals and obtain software updates from their POS system provider. They should schedule installation with their IT and POS system providers as soon as possible.

  The price for a new reader varies from $30 for an EMV reader that plugs into mobile devices, up to $600 per terminal depending on features and the vendor.[4] Merchants may want to consult their IT provider about what will work best for them.

- Employees may require training on procedures for handling the new cards and policies for accepting old, non-EMV cards.

  Customers will insert their cards into a slot in the EMV card reader and hold them in place while the reader communicates with the chip on the card. Then they can enter their PIN or sign for the transaction.

- The new EMV cards and readers will be backwards compatible. Readers will be equipped to accept mag-stripe cards and chip cards will also have magnetic stripes to enable their use in existing card readers.

eMazzanti Technologies, a NYC area IT consultant and MSP, offers EMV credit card technology upgrade services to retail merchants, doctors, attorneys, contractors and other businesses that accept credit cards.

eMazzanti will also install and manage your Internet connection, PCI compliance, wireless networks and all of your retail technology connecting all of your stores.

Most of the changes for EMV conversion are covered for eMazzanti Technologies customers with existing eCare agreements (eCare is eMazzanti's branded managed services). eCare keeps stores up to date and operating with the latest technology, improving their customer experience.

With an extensive customer base, eMazzanti is able to leverage vendors to provide clients with superior support. Small retailers that delay, or who are without a good technology partner to advise them, may be left behind.

5. Making the most of EMV

In spite of the costs to upgrade equipment, merchants should focus on the positives of EMV conversion. There is a great opportunity to improve the customer experience by using the latest advancements in technology.

Positives of switching to EMV technology:

- Converting to EMV will protect your customers from fraud.
- Switching prior to the deadline will shield your business from liability for card fraud at your establishment.

- Over time, customers will learn to expect EMV terminals at stores, restaurants and other places of business. They'll come to know that using EMV cards is more secure.
- Since most EMV terminals also accept mobile payments, you'll be able to accommodate NFC-based payment systems.

A secure business environment creates an atmosphere of confidence and growth. The EMV deadline creates an opportunity to generate increased customer confidence in your business and preference for your brand, if your customers know about your use of the technology.

Merchants may want to consider promoting their EMV status. Here are a few ideas to help you get the word out:

- Design an "EMV Cards Accepted Here" logo to use as a window and register sticker. Ask your bank if they supply them.
- Print a security tag line like "EMV Protected Card Data" on receipts, invoices, quotes and email signatures.
- Post about your EMV compliance on social media.
- Create a press release about your EMV upgrade and other outstanding data security technology and policies.

Data security technology is an investment. You can increase your ROI beyond reducing credit card theft by using your EMV upgrade as a business asset to attract customers and increase revenues.

An improved customer experience with a corresponding increase in sales and a reduction of theft will more than justify the effort and expense to comply with the EMV deadline. Those merchants that are prepared will most likely see the biggest positive effect on their bottom line.

*EMV stands for Europay, MasterCard and Visa, a global standard for the compatibility of chip cards and POS terminals designed to accept the cards and authenticate credit and debit card transactions. In the midst of frequent large-scale data breaches and the resulting increase of counterfeit card fraud, U.S. card issuers are implementing the EMV technology to protect their customers and to minimize their losses from fraud. A chip card is a credit card with embedded microelectronics designed to reduce the risk of loss to cardholders and merchants from fraud. During the coming months, banks will be replacing credit and debit cards with chip cards to help increase security for customer's accounts.

[1]Source: VeriFone Systems, Inc., http://lp.verifone.com/media/2146788/emv_key_dates_chart_021213.pdf

[2]Source: CreditCards.com Glossary, http://www.creditcards.com/glossary/term-cardpresent-fraud.php

[3]Source: Missing the EMV Liability Shift Bears a Huge Cost, http://www.paymentssource.com/news/paythink/missing-the-emv-liability-shift-bears-a-huge-cost-3018661-1.html

[4]Source: The EMV Card Deadline Is Coming. Here's How to Prepare Your Business, http://www.entrepreneur.com/article/247485