Heartland

Help your customers navigate EMV planning and implementation

The launch of EMV in the U.S. is underway, with the impending liability shift set for October 2015. This means that liability is going to shift to the party using the least secure technology, which could be the merchant. Your customers will be looking to you to provide the guidance they need to protect their business.

Following are some questions to ask your customers to help start the discussion for EMV implementation planning, as well as the background and information you need to put the questions in context.

Are you in a business susceptible to counterfeit fraud? Do you sell anything high dollar or easily transferrable that can be resold?

Existing fraud exposure alone is probably not sufficient to warrant the investment in new technology, but as fraudsters catch on, they will target businesses without EMV.

Do you operate in a location that is conducive to fraud, such as a tourist destination?

Small merchants will become targets in geographic areas prone to fraud, since large retailers will be the first to invest in EMV.

How much time and effort is it for you to deal with a chargeback today? How much does each chargeback cost you?

Merchants who implement EMV will have fewer disputes related to counterfeit and potentially lost/stolen fraud reason codes. Merchants who do not may see an increase in chargebacks as they become liable for fraud, which they are not today (in general).

Will your customers prefer paying with EMV? Will your competitors support EMV?

Because of the advantages to card issuers, EMV marketing to consumers will ramp up as issuance increases. Merchants will want customers to feel their data is secure.

Do you support Apple Pay or other mobile payments today? Are mobile wallets relevant for your environment or desired by your customers?

Apple Pay and other mobile payment technologies also leverage EMV technology, so an upgrade plan should take into account devices that support dual contact and contactless interfaces.

RSPA

What kind of device configurations does your environment require (e.g., unattended kiosks, table service/no PIN)? Counter service? Interest in Pay-at-the-Table?

The merchant environment will drive how the device/software should be configured for cardholder verification methods (CVMs), such as "no PIN." Merchants looking to invest in Pay-at-the-Table have many additional considerations, including impacts to waitstaff workflows. These configurations can also govern how tips are handled, so the merchant needs a thorough understanding of the impact.

Are you concerned about all of the data breaches in the news the last few years? Did you know that 60 percent of businesses that get breached go out of business within a year?

If you are Heartland Secure, then you automatically get the industry's only free comprehensive breach warranty. Additionally, Visa has modified their *Global Compromise Account Recovery* program to provide safe harbor for merchants who process more than 95 percent of their card-present transactions through EMV devices, in the event of a data breach.

Are you using devices that encrypt magnetic stripe or manually entered card data? Are you storing card data for mail/fax orders, loyalty or recurring billing?

EMV guarantees that a card is genuine, but E3™ technology and tokenization protect card data—magstripe or chip—in motion and at rest. Heartland Secure delivers all three technologies for the highest level of data security.

Do you sell through online channels as well? Are you increasing your security measures to account for the migration of fraud due to EMV?

Data from other countries proves that EMV will eventually drive an increase in online purchase fraud. "Omnichannel" merchants need to carefully reassess their e-commerce strategies and consider implementing advanced fraud protection measures and programs that may be offered by their e-commerce service providers, such as predictive rules engines and data tokenization.

Are you a Level 2 or higher merchant (over 1 million transactions per year) or do you hope to grow to be one?

Visa's Technology Innovation Program provides relief from PCI compliance validation reporting for these large merchants when 75 percent of their transactions originate from a dual-interface EMV chip-enabled device.

RSPA