The New Pawn in Payment Security

The Industry:

In October 2015, the much-discussed Payment Networks' Liability Shift associated with EuroPay, MasterCard, and Visa (EMV) is due to take effect in the United States.

It's a major milestone for financial companies (meaning banks and credit unions), credit card issuers, retailers, and more. There is a great deal of information, and a ton of misinformation regarding the US EMV migration roadmap as presented by Payment Networks, EMVco, LCG and many other institutions. Shedding some light on the realities involved is helpful for everyone concerned.

To date, Europe, Canada, Latin America, and the Asia/Pacific region are all well on their way with migrating from the legacy magstripe standard to EMV chip card technology. The U.S., the world's single largest user of payment cards, has just started this process. However, the potential impacts of being the last bastion of magstripe technology is forcing U.S. financial entities to take the idea seriously.

The main driver behind the EMV migration is card-related financial fraud. Despite the best efforts of global law enforcement agencies, global losses have risen steadily, increasing pressure to find a global solution. Annual costs of card fraud in the U.S. alone are estimated at $8.6 billion per year. Experts believe that figure will rise to $10 billion or higher by 2015, especially if the U.S. does not make significant progress with chip card adoption. The rising cost of fraud is accompanied by a concurrent rise in mobile payments. In 2010, the total gross dollar volume of mobile payments in the U.S. alone was $16 billion; some experts expect this volume to rise to $214 billion by 2015. If ever there was a time to ensure compliance with a global chip-compatibility strategy that reduces fraud, it's now.

This is especially true in light of the fact that many countries are now considering banning traditional magnetic stripe cards, a technology standard in use for over 40 years. It's estimated that 40% of the world's cards and 70% of its terminals deployed outside the U.S. are today using the EMV standard. Visa, a prime mover in the US migration to EMV, states that the pace of EMV-adoption is accelerating globally, estimating that right now, 62% of transactions conducted across international borders involve a chip-enabled card used at a chip-enabled terminal. Currently, our government is content to let the financial industry set its own course- but that hands-off approach may not last long.

One key component in the EMV discussion is its accompanying liability shift. This liability shift means that those issuers and merchants using non-EMV compliant devices that choose to accept transactions made with EMV-compliant cards assume liability for any and all transactions that are found to be fraudulent. MasterCard defines the liability shift this way: The party, either the issuer or merchant, who does not support EMV, assumes liability for counterfeit card transactions. Understand that by issuer, the card companies do not mean themselves; the term refers instead to banks, credit unions, and any other financial institution issuing credit or debit cards.

Liability is an emotionally charged word with potentially huge and disturbing ramifications. Still, the threat of assumed liability does not mean that entities involved in card-based transactions must move toward EMV compliance immediately. What it does mean is that issuers, acquirers, merchants, and others must start planning their course of action.

For most, some EMV-related implementation is essential, so planning must begin soon, if it's not underway already. Funding that implementation of EMV-compliant cards and devices represents a major expense item.

Courtesy of Javelin Strategy & Research, here's a big picture look at potential costs involved in achieving EMV compliance in the U.S.:

Item	Volume	Estimated Cost to Replace
POS Devices	15,000,000	$6,750,000,000
ATM's	360,00	$500,000,000
Credit/Debit Cards	1,126,800,000	$1,400,000,000
TOTAL:	1,142,160,000	$8,650,000,000

No matter how you slice it, $8.65 billion is a big number, however, there is a positive aspect to this. Earlier in this post, I pointed out that by 2015 it is estimated that the annual cost in this country for card-related fraud is $10 billion. If companies commit to the $8.65 billion spend in 2014, then fraud-related costs for 2015 could drop exponentially. With improved EMV-compliant technologies and continued reduction in the frequency of fraud thanks to intensified law enforcement efforts, improvements should continue, adding up to a positive ROI.

There are other advantages worth noting: Many of the ATM manufacturers have already changed over to EMV-compliant technology, reducing costs on this front. Chip-enabled cards, while initially more expensive to produce, have a longer shelf life than magnetic stripe cards, as well as being capable of 'flash-updating,' lowering their costs over time. VISA offers merchants who make the conversion an incentive package, relieving some of the financial burdens on that side. Adoption of EMV-compliant cards and devices is seen by many as a step toward wider adoption of mobile payment methods. So where do we stand today?

According to EMVCo, 1.55 billion EMV cards- accounting for 41% of the total payment cards in circulation worldwide- have been issued as of Q2 2012. It also reports that 18.7 million EMV-compliant POS devices- accounting for 71% of the total number- were installed in Q1 2011.

This chart, courtesy of EMVco, provides a quick glance at how far along adoption is in other countries:

Worldwide EMV Chip Card Deployment and Adoption*

	2013		2014	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Canada, Latin America, and the Carribbean	471M	54.2%	544M	59.5%
Asia Pacific	942M	17.4%	1,676M	25.4%
Africa & the Middle East	77M	38.9%	116M	50.5%
Europe Zone 1	794M	81.6%	833M	83.5%
Europe Zone 2	84M	24.4%	153M	40.4%
United States	-	-	101M	7.3%

*Figures reported in Q4 2013 and Q4 2014, respectively, and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.

LCG, Inc:

If you are currently not engaged in an EMV conversation with someone within your payment ecosystem such as your POS provider, your Software Gateway Provider, CC Processor or your Merchant Bank, you are extremely late to the game.

Breaches and Fines are inevitable. Preparing for a breach and executing on industry standards for PCI and EMV compliance will substantially reduce the costs associated to these fines when that day comes. Willful non-compliance will be the position many companies will be in when this liability shift takes place in October. You don't have to be an industry expert to know that companies who have taken a stance to do nothing towards producing a more secure platform to process your credit card information will see the full recourse of this liability shift from the Merchant Banks in the event of any breach or even a minor fraudulent charge.

For anyone who has been part of a breach you know this first hand. The Merchant Banking Company that regularly checks in to ensure your processing is going smoothly is now sitting at the same side of the table as the FBI and the PCI audit team. The same company that you have paid thousands of dollars for processing fees for many years will be the same company that you are negotiating with on how large your fine will be. There is no love loss here if you have little to know evidence showing your implementation or roadmap to compliancy.

And the end result is always the same… After a grueling 12-24 month process of Forensic PCI audits, QSA and third party investigations, PCI deficiency reviews, countless lawyer meetings and much, much, more.. Your Merchant Bank is going to sit in front of the executive team and hand them one more additional bill that will be substantial compared to the money already spent on the resources needed to work through this breach.

These are all hard costs associated to a breach. This does not consider damages to your brand, in house resource allocation and the impact to day to day production and operations. These costs often out way the cost of the actual fine.

It won't happen in October or even by December but the start of 2016 will showcase some prominent companies in your community getting hit with substantial fines from the merchant banks that will ultimately put them out of business. As a business owner, if you wait for this type of press to get your attention, you will likely be a part of the press sooner then later. It doesn't take a massive breach or thousands of stolen cards. It's as simple as an employee writing down a few card numbers on a receipt because the POS wasn't working for a few minutes.

The small and mid-market companies will continue to be the top targets for fraud due to the current statistics associated to these companies having less money to spend on better security and more resources to put better policies and procedures in place to help mitigate breaches.

~ IT Security Advisors Group, A Division of LCG, Inc.