W. Capra
CONSULTING GROUP

221 NORTH LASALLE ST. | CHICAGO, IL 60601 | 312-873-3300 | INFO@WCAPRA.COM

EMV: The Journey Begins October 1st

An Examination of the History, Impact, Best Practices, Pitfalls of EMV Implementations, and What Merchants Need to Know Post Liability Shift

October 1, 2015

Introduction

At this point, you may be familiar with EMV. You may know what it means for your business and the implications that you face for not meeting the October 1, 2015 liability shift. What you may not know is how EMV became a focus for US merchants, what the most efficient EMV implementation methods are, or how outside forces may influence the future of EMV.

This paper examines EMV from its origin to provide a more complete context around the US implementation so that you can begin to identify the challenges, best practices, and potential pitfalls of implementing EMV.

History

The Beginning

Europay, MasterCard, and Visa formed EMVCo in 1999 in an effort to combat card fraud. Since then, EMVCo has grown in scope of participants, now including American Express, Discover, JCB, and UnionPay. From the beginning, the goal of EMVCo has been to facilitate the interoperability of payments between chip cards, payment terminals and the pertinent acquirers. The group also oversees the testing and certification procedures for the adherence of payment terminals and chip cards to EMV specifications. Today, EMVCo remains responsible for creating and maintaining these specifications. It is important to note that EMVCo does not issue products or enforce EMV compliance in the marketplace. Rather, EMVCo focuses solely on maintaining the worldwide EMV payment standard.

Global Adoption

Though not managed by EMVCo until 1999, the first EMV specification (v 2.0) was created in 1995. EMVCo released their most recent specification (v 4.3) in 2011[1]. In that sixteen-year span, every major global region, with the exception of the United States, transitioned to EMV.

Financial institutions and card brands worldwide relied on fraud liability shifts to incentivize and accelerate EMV adoption. An EMV liability shift occurs when the financial accountability for in-store counterfeit and Lost and Stolen fraud shifts to the party that is least secure. Liability may fall upon the merchant that cannot accept chip card transactions or the issuer that has not yet made chip cards available to consumers.

The financial incentives for issuers (reduction in counterfeit fraud losses) and the associated penalties for merchants (increase in fraud costs) helped drive adoption of the EMV standard across the global payment ecosystem. Figure 1 displays the liability shift deadlines and Q4 2014 adoption rates.

You can see from the chart that a liability shift, even one that occurred years ago, does not mean that every region has accomplished full EMV acceptance. A variety of factors have prevented 100% EMV penetration in these post-liability shift regions. Chip and terminal supplier readiness, relationships between card brands, merchants, acquirers, and issuing banks, and even geography all dictate the speed at which a region can implement EMV.

	Europe Zone 1	Europe Zone 2	Canada, Latin American, and the Caribbean	Africa and the Middle East	Asia Pacific	Canada	The United States
MasterCard Liability Shift Date	Jan, 2005	Jan, 2005	Jan, 2005	Jan, 2006	Jan, 2006	Mar-11	October, 2015
2014 Adoption Rates							
% of Cards EMV	83.50%	40.40%	59.50%	50.50%	25.40%	95.00%	7.30%
# of EMV Cards	833M	153M	544M	116M	1.68B	90M	101M
% of Transactions EMV	96.60%	58%	85.40%	80%	27%	N/A	0.12%
Months Post Liability Shift	129	129	129	117	117	54	0
Exceptions			Brazil - March, 2008 Colombia - October, 2008 Venezuela - July, 2009 Canada - March, 2011	South Africa - Jan, 2005	Australia - April, 2013		

Figure 1 – Global EMV Liability Shift Dates and Adoption Rates [2] [3] [4] [5] [6]

[1] EMVCo.
[2] MasterCard Chargeback Guide, October 3rd 2010
[3] EMVCo EMV Worldwide Adoption, Q4 2014
[4] MasterCard Press Release: "MasterCard Canada Extends Timeline for Chip Migration" September 24th, 2010
[5] MasterCard - The US Chip Migration Feb 13, 2014
[6] Financial Post - Canada's Credit Card War is Shifting to New Battleground

The Impacts of EMV

Major markets that have implemented EMV have benefitted from a decrease in counterfeit card fraud. Figure 2 highlights the impact of EMV implementation on card fraud in the UK and Canada. Those that have also upgraded cardholder verification methods (CVMs) have seen a sharp reduction in lost and stolen card fraud. It is important to note that total fraud has not decreased; it has shifted in two major ways.

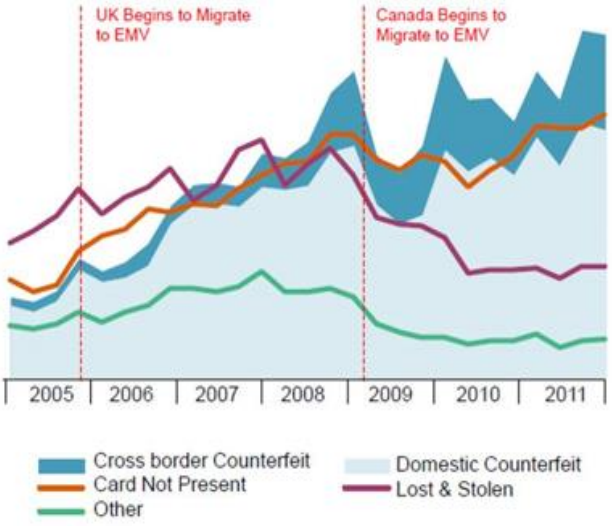

Figure 2 – UK and Canadian Payment Card Fraud [7]

Fraud Migrates Channels

First, fraud has migrated to new channels. While Card Present (CP) fraud has decreased in markets where EMV has seen greater penetration, Card Not Present (CNP) fraud rates have risen. Between the 2006 UK liability shift and 2012, the UK saw CNP fraud rates rise roughly 20% (£200M to £240M), with the year 2008 having the highest level of CNP fraud (£360M). During the same period, counterfeit card fraud decreased roughly 45% (£120M to £60M).[8]

Fraud Migrates Countries

Fraud has also migrated to new countries. Canadian counterfeit card fraud rates decreased roughly 68% from 2008 to 2014[9]. Since these regions implemented EMV, fraudsters have increasingly aimed for US merchants. If the US sees similar benefits to implementing EMV that other regions have seen, US merchants can expect to significantly reduce the amount they spend on cross-border counterfeit and CP fraud.

EMV Positioning

Before the major US data breaches began in 2013, the discussion on EMV acceptance in the US had already begun. The first indication that EMV was coming to the United States was Visa's 2011 announcement of the October 2015 liability shift date. Other card brands followed and maintained that EMV acceptance will be required in order to avoid the fraud liability shift.

The EMF

EMV's imminence spurred EMV stakeholders to establish the EMV Migration Forum (EMF) in order to foster cooperation and address EMV adoption issues that require cross-industry collaboration. The EMF currently has more than 140 members[10], including payment brands, financial institutions, industry suppliers, processors, and merchants.

US Uncertainty and the Aftermath of Major Breaches

Even after the liability shift date was established, many merchants speculated – and card brands hinted – that the date for the liability shift may be postponed. However, major data breaches at Target and Home Depot (amongst others) ignited conversations about the protection of consumer data and the additional steps that merchants can take to prevent future breaches. This focus on fraud prevention resulted in the card brands upholding October 2015 as the liability shift date.

[7] MasterCard Analysis 2012
[8] FICO European Fraud Infographic
[9] Candaian Bankers Association – Credit Card Fraud and Interac Debit Card Statistics
[10] EMV Connection

US Implementation Challenges

EMV implementation has posed a unique set of challenges to the US payments ecosystem. The greatest obstacles to implementing an EMV-compliant solution in the US have been the complexity of implementation, impacts to existing suppliers, federal regulations, costs, a return on investment that is difficult to identify, and a new customer and employee experience at the point of sale.

US Debit Complexity

The complexity of the debit environment in the US posed a tremendous challenge to acquirers, issuers, payment networks, and merchants preparing for EMV. Whereas most other countries work with only one or two debit networks, the US payments ecosystem consists of sixteen unique debit networks. Integration with the networks was further complicated due to the Durbin Amendment, which mandated merchants have the ability to route transactions to at least two independent PIN debit networks. While the measure aimed to protect merchants – increasing competition among debit networks and reducing the fees that merchants pay banks and credit unions – the debate over interpretation of the measure, along with a prolonged period of establishing a technical solution to support the measure, delayed the US EMV solution. This delay impacted merchants' ability to start planning and designing a solution.

The Effect of Debit on US Timelines

The creation of the US Common Debit AID in the fall of 2014 finally accomplished the necessary debit routing requirements to support the Durbin mandates. By this time, however, the US payments ecosystem had just over twelve months to implement EMV debit before the October 2015 liability shift, a process that merchants in other regions were given four to five years to implement. This effectively created a US specific implementation of what is supposed to be a global standard.

Project Timing

As with any major IT project, implementing EMV is disruptive to everyday business operations. However, EMV projects are unique in that they require a significant time and knowledge investment, as well as realignment of company resources across multiple departments beyond IT (learning and development, treasury, store operations, and more). Each industry has its own business considerations that impact its EMV implementation, including speed of service, retail channels, and fraud levels, among others. No two EMV implementations are the same. Merchant readiness will dictate how long the EMV implementation process will take and which tasks will be required. At a minimum, most merchants will need to perform a payment architecture review, create EMV business requirements, develop an EMV training curriculum, and extensively test and certify their new solution. It is crucial that merchants work with their vendors to ensure that the functional requirements of the system are all in alignment for EMV. Depending on merchant size and complexity, EMV implementations can last up to 2 years.

Procurement and Working with External Vendors

In some cases, merchants have engaged the appropriate parties to implement EMV, but their suppliers are not yet ready to deliver the hardware or functionality. Some retailers work with technology vendors or processors whose services do not yet comply with EMVCo standards. Technology vendors that are EMV-compliant still may struggle in fulfilling orders for large merchants, as the merchant requires a new terminal for each point of sale location. Some merchants may have installed EMV-compliant hardware, but have yet to enable their terminals because of resource constraints associated with the upcoming October liability shift.

Cost

Implementing EMV is not just complex; it's a costly undertaking. EMV-capable customer terminals cost, on average, $500. This figure does not include installation costs, which may be significant. Large retailers can expect to spend tens of millions of dollars on a hardware changeover alone, as each physical payment location requires an upgraded EMV terminal. The installation of these terminals will only ensure that the merchant has hardware capable of processing EMV payments. Enabling EMV functionality in a production environment requires the retailer to invest further material funds into software, development, certification testing, and deployment.

Impact on Fraud

EMV ROI

The EMV system, while complex and costly, is still not a cure-all solution. EMV does nothing to protect against CNP fraud. As noted above, fraudsters will migrate to CNP channels with the introduction of EMV to the US market. CNP fraud will continue to increase independently of EMV as eCommerce volume grows. Due to this expected migration of fraud, the return on investment for implementing EMV is difficult for issuers and merchants to quantify.

Chip and PIN vs. Chip and Signature

With regards to CP fraud prevention, EMV implementation in the US may not prove as successful as it has in other countries. This is primarily due to the fact that most retailers will accept chip-and-signature cards, which many consider to be a less secure CVM than chip-and-PIN. Issuers' preference for chip-and-signature is tied to the belief that chip-and-PIN adds friction to the customer experience and requires infrastructure upgrades to authenticate PIN. Despite the challenges that exist, the payment networks have upheld the October 2015 liability shift. To protect themselves from financial liability for fraudulent in-store transactions, US merchants must overcome the challenges to implement and deploy an EMV-enabled solution.

Best Practices

Planning your EMV rollout is a time and resource intensive task that directly impacts your bottom line. What is typically viewed as an IT project is anything but, as EMV will affect your store operations, treasury/accounting, compliance/risk management, and store support. W. Capra has developed the best practices below from implementing EMV with multiple Fortune 500 organizations.

Implementation Planning

In the planning phase, you should make a clear decision on encryption and tokenization usage alongside EMV. Then, as you plan your EMV rollout, you should focus on creating strong requirements, accounting for all EMV elements and processes, to avoid rework. Develop your processes and standards with a mind toward accommodating both ongoing and new system certification requirements. As you develop your requirements, you should understand your total risk tolerance and develop response plans accordingly.

Staffing and Third Party Vendors

Since you will work with third party vendors to implement EMV, it is important to practice strong vendor management and host regularly scheduled cross-vendor meetings. Ensure that there is clear ownership of cross-functional risks that exist within the project.

Though third parties offer EMV-essential services, it remains important to verify that your existing payments team has the knowledge required for EMV at all levels (technology, equipment, processing, business operations, and external linkages). If this is not the case, you should adjust your staffing to meet the learning needs and future EMV maintenance needs that the project will require. In addition, ensure that you provide your support team with sufficient training to understand technical EMV issues.

Consumer Experience

The transition to EMV is a cumbersome process for both merchants and consumers. Prepare to address consumer-facing issues and establish an effective communication strategy. Before the EMV upgrade, you should focus on training store personnel to respond to questions around chip cards. You should also train staff to respond appropriately to various cardholder situations—premature card removal, incorrect "dipping" of the card, and CVM options for your store.
Following the upgrade, you should focus on improving the customer experience. Make sure EMV functionality seamlessly integrates with your current loyalty experience for both EMV and existing mag stripe payments. To ensure employees and consumers are comfortable with the EMV experience, you should update new employee training, provide staff with a reference guide, and create a feedback mechanism for store personnel to communicate training needs to managers.

Analytics

As a merchant, you should position yourself to gain a view into the issues that arise in your deployment and the influence of outside market forces. This will allow you to anticipate problems and incorporate solutions in your payments strategy. The most effective response to mitigating EMV pitfalls is to ensure that the foundation of your company is flexible and adaptive. That way, as the need for change inevitably arises, you can respond in an agile manner.

Implementation Pitfalls

Along with the challenges mentioned above, several pitfalls may emerge upon the US deployment of EMV.

Certification

Access to certification queues will remain limited through 2016. Plan your certification strategy accordingly. The use of dedicated testing and certification tools, along with detailed documentation, will minimize time spent testing and certifying your EMV solution.

Brand Management

EMV is a concept that is largely misunderstood by the general public. If you will not make the October 1st deadline, your brand will be subject to increased public scrutiny about security. As a retailer, you should focus on crafting a message to consumers about why you are not meeting the date, what that means for your customers, and the other security measures that you utilize to protect cardholder data.

Pilot Testing

As with any major IT project, you will encounter hurdles as you begin your EMV rollout. Use your pilot test to observe any impacts to the cardholder experience, including time in lane increases and technical issues that require help desk support. Use this time to test and further refine your support and troubleshooting model in preparation for a large-scale rollout.

Final Thoughts

EMV implementation is complex, and can sometimes seem overwhelming. By following W. Capra's best practices, and by establishing positive relationships with your payments partners, you can position yourself as a leader in fraud mitigation by implementing a flexible and comprehensive fraud prevention system. Though many hurdles lie before EMV deployment, it is important to remember that you are not alone in the struggle to implement EMV.

About W. Capra

W. Capra Consulting Group is a professional services organization focused on identifying, leading, integrating and delivering technology, payment, security, and loyalty solutions to a broad range of major established retail firms and emerging businesses. We have a passion for our business and for seeing our clients succeed.

If you have additional questions regarding EMV and its implications, please contact Clint Cady, Director of Payments.
ccady@wcapra.com, 312-873-3300