MasterCard Advisors™

EMV FOR U.S. ACQUIRERS: SEVEN GUIDING PRINCIPLES FOR EMV READINESS

BY PHILLIP MILLER, GUY BERG, JEFF STROUD, AND STEVEN PAESE

Acquirer EMV[1] enablement is a critical first step to full chip migration in the U.S. In April 2013, MasterCard, Visa, American Express, and Discover will require that acquirers, service providers, and sub-processors have the capability to process any EMV point of sale (POS) transaction, both contact and contactless. To be fully compliant means that acquirers must adhere to payment network rules and complete approvals, including network approvals and testing procedures, in order to begin processing and passing additional authorization messaging for EMV transactions.

+70% OF TERMINALS ARE PROJECTED TO BE EMV EQUIPPED PRIOR TO THE LIABILITY SHIFT IN 2015[2]. WILL YOU BE READY?

EXECUTIVE SUMMARY

The acquirer readiness date is now less than a year away and is a vital first step for retailers to begin deploying EMV terminals and advancing EMV migration within the United States. Currently, acquirers are rapidly preparing to complete compliance and approvals to meet this important deadline. However, completing the approval process is only the "tip of the pyramid" of what they need to accomplish to be operationally ready to efficiently and effectively support EMV in the U.S.

This white paper is designed to provide high-level guidance for acquirers to support EMV implementation in the U.S. It is not meant to replace well-documented EMV implementation requirements previously established. Highlighted in this paper are "Seven Guiding Principles for EMV Readiness" based on challenges, opportunities, and learnings gained from EMV migration in other markets.

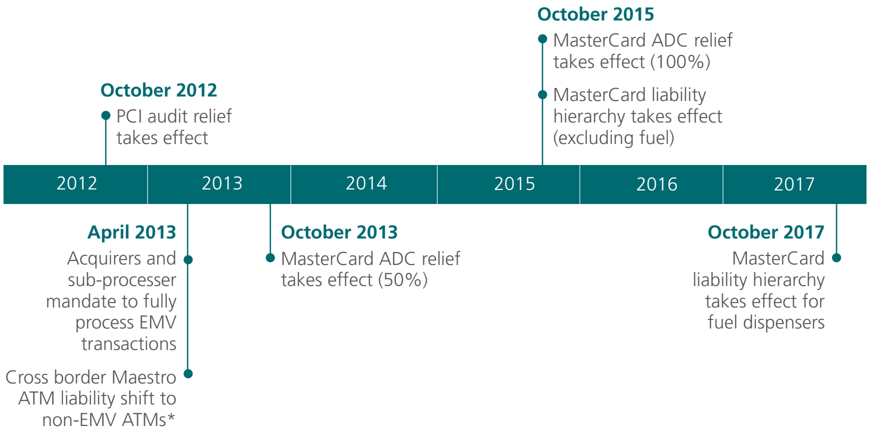
Completing the approval process is only the "tip of the pyramid" of what acquirers need to accomplish to be operationally ready to efficiently and effectively support EMV in the U.S.

THE LIABILITY SHIFT AND MIGRATION INCENTIVES

The April 2013 acquirer readiness date is the first step in preparation for MasterCard's liability shift, which takes effect October 1, 2015. This liability shift directly affects acquirers and issuers as it pertains to counterfeit fraud. *This means that the party, either the issuer or merchant, who does not support EMV, assumes liability for counterfeit card transactions.* In addition, MasterCard supports a liability shift for lost, stolen, and never received or issued (NRI) cards to the party that does not support PIN as a cardholder verification method. If neither party supports PIN, only the counterfeit liability shift rules apply. The liability shift does not apply to Automated Fuel Dispensers (AFDs) until October 1, 2017.

This means that the party, either the issuer or merchant, who does not support EMV, assumes liability for counterfeit card transactions.

FIGURE 1: MASTERCARD EMV LIABILITY SHIFT


October 2015
MasterCard ADC relief takes effect (100%)
MasterCard liability hierarchy takes effect (excluding fuel)
October 2012
PCI audit relief takes effect
2012
2013
2014
2015
2016
2017
April 2013
Acquirers and sub-processer mandate to fully process EMV transactions
Cross border Maestro ATM liability shift to non-EMV ATMs*
October 2013
MasterCard ADC relief takes effect (50%)
October 2017
MasterCard liability hierarchy takes effect for fuel dispensers

**Previously announced*

Beyond the liability shift, MasterCard is offering additional incentives to merchants to encourage rapid EMV adoption. These incentives include enhancements to the Payment Card Industry (PCI) compliance validation requirements for Level 1 and 2 Merchants and Account Data Compromise (ADC) program operational reimbursement and fraud recovery calculations. To be eligible, merchants must deploy hybrid EMV terminals (support of both contact and contactless interfaces).

PCI audit relief is applicable if 75 percent or more of the merchant transactions are captured at hybrid EMV terminals, effective October 2012. Even if the majority of transactions are from magnetic stripe-only cards, if they are performed at hybrid EMV terminals the relief is applicable.

The ADC relief reduces Operational Reimbursement (OR) and Fraud Recovery (FR) exposure in the event of a data compromise, up to 50 percent starting October 2013. Relief from OR and FR exposure increases to as much as 100 percent by October 2015 if at least 95 percent of merchant transactions are captured at hybrid EMV terminals that support both contact and contactless EMV.

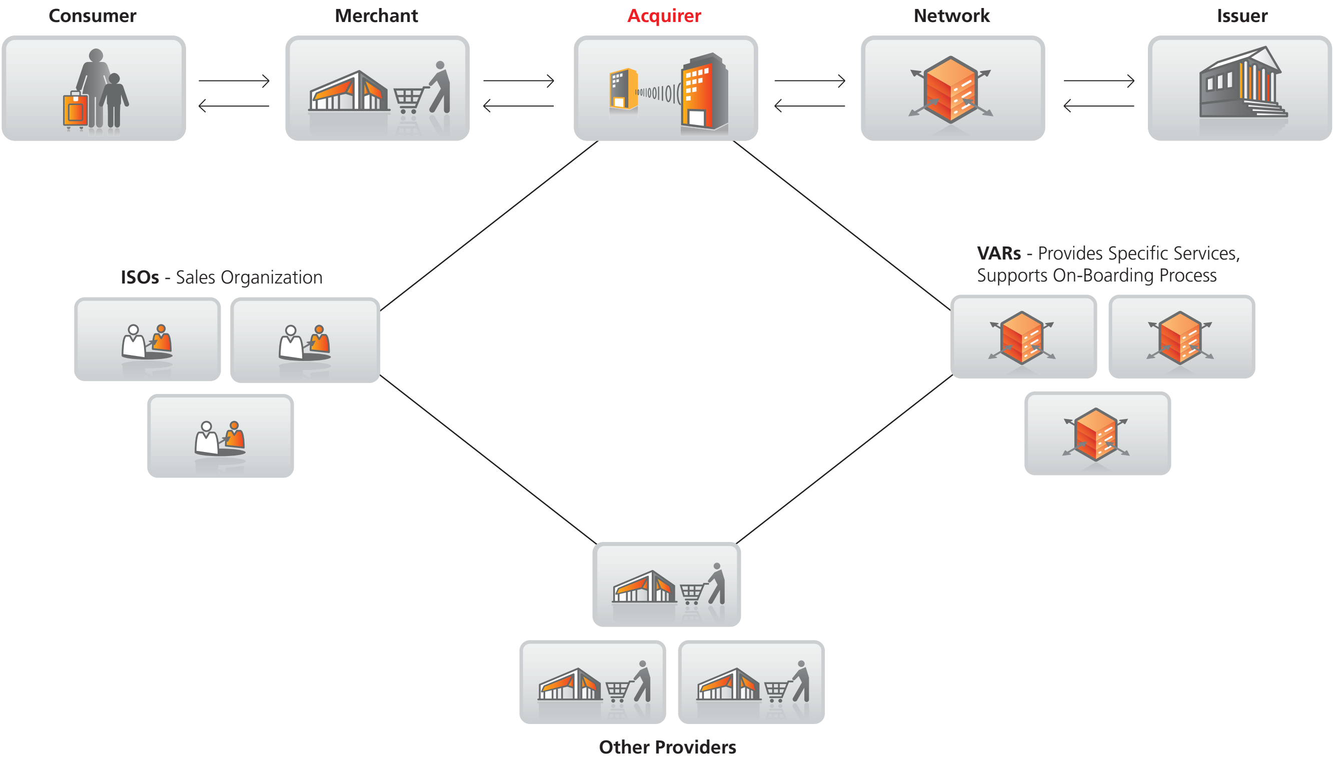
The combination of the liability shift and PCI and ADC relief provides merchants with significant incentive to begin implementing EMV terminals and should spur demand for acquirers to meet their needs.

The combination of the liability shift and PCI and ADC relief provides merchants with significant incentive to begin implementing EMV terminals and should spur demand for acquirers to meet their needs.

TURN CHALLENGES INTO OPPORTUNITIES

Acquirers are uniquely positioned to foster migration to the new EMV ecosystem. Very simply, for the enhanced functionality and security features of EMV to be realized, both cards and terminals must be deployed. But before the terminals can be deployed, acquirers need to be ready to implement EMV support.

FIGURE 2: PAYMENTS ECOSYSTEM—ACQUIRERS ARE THE CENTRAL LINCHPIN IN EMV MIGRATION


Consumer
Merchant
Acquirer
Network
Issuer
ISOs - Sales Organization
VARs - Provides Specific Services, Supports On-Boarding Process
Other Providers

Deployment of EMV will be challenging, but there are potential benefits to the migration initiative. Developing strong EMV core competencies will differentiate acquirers and can provide an opportunity to gain share through enhanced service offerings, high-quality EMV migration support, and supporting new mobile Near Field Communication (NFC) acceptance as well as value-added service opportunities. Minimizing EMV deployment investment may decrease the ability to meet a surge in demand for EMV terminals and cost-effectively support terminals on an ongoing basis. This may ultimately diminish acquirers' ability to meet customer needs and lead to potential lost business.

Retailers will need to carefully weigh the risks and rewards associated with their decision to migrate to EMV early or deploy later. A rapid move to EMV can reduce the risk of counterfeit, lost, stolen, and NRI fraud as well as provide PCI and ADC relief. If EMV deployment is delayed, retailers installing EMV-capable terminals later in the cycle could potentially incur increased fraud losses and even become a target for fraudulent transactions, thereby increasing their counterfeit fraud losses even more.

EMV PARADIGM SHIFT AND OPERATIONS IMPACT

EMV Paradigm Shift

To fully appreciate the potential impact of EMV on acquirers' operations, it is important to understand the fundamental shift in payment forms and terminals and the impact of offline authentication and authorization options. Today all magnetic stripe cards are encoded with the same basic information; the terminal simply captures this information and passes it on for authentication and authorization.

EMV radically changes this interaction between the payment form and the terminal in a manner that significantly increases the role and sophistication of the terminal application. The current change in the U.S. payment infrastructure can be comparable to the shift in the music industry from analog to digital; substantial changes will facilitate further innovation.

EMV leverages the secure chip memory and intelligent processor to enable the definition of different card authentication and cardholder verification methods, as well as other risk parameters, set by the issuer. The data and the processing functions presented to the terminal may vary by issuer. The core EMV logic in the terminal is designed to get its operating instructions for each transaction from the card and then begin card authentication and transaction processing. With increased two-way interaction between the payment form and the terminal, there is a corresponding need for increased testing prior to terminal deployment, which ultimately requires greater knowledge for both pre-deployment testing and post-deployment troubleshooting.

The core EMV logic in the terminal is designed to get its operating instructions for each transaction from the card and then begin card authentication and transaction processing.

EMV Operations Impact

EMV is continuing to evolve and is designed to enable implementation of stronger security over time. Examples of changes to EMV will include different key lengths and different cryptographic algorithms in the future. It can be expected that there will eventually be more frequent terminal application and EMV configuration updates or, at a minimum, the need to load new keys to the EMV terminals. For this reason, investments in terminal management systems with remote download capabilities for application version upgrades and EMV offline authentication key updates may prove invaluable. These cost-effective investments can also be leveraged to improve overall terminal support efficiencies, merchant fraud analysis, and even opportunities to add new services and improve overall customer satisfaction.

Given the nature of the changes involved in EMV, building contact and contactless core competencies can represent an opportunity to bring significant value to your customers. Merchants will need assistance in understanding and integrating EMV acceptance into their daily operations. Anything from operations training to integration consulting and even mobile NFC marketing program implementation opportunities will appear for those acquirers that are interested in leveraging this industry shift for business growth.

Given the nature of the changes involved in EMV, building contact and contactless core competencies can represent an opportunity to bring significant value to your customers. Merchants will need assistance in understanding and integrating EMV acceptance into their daily operations.

The first step for acquirers will be to achieve network compliance prior to the requirement dates. Beyond network approval, there are two other important steps to complete to minimally meet the requirements to deploy EMV terminals at merchant locations:

- **Identify terminals with the appropriate EMVCo[3] approvals.** A terminal must complete testing approval by EMVCo before it can be deployed in the market; however, this is not the only testing that will be required.
- **Confirm that payment network-specific application logic is loaded onto the terminals.** This logic, required beyond the base EMV logic, must be tested and approved by each of the payment networks.

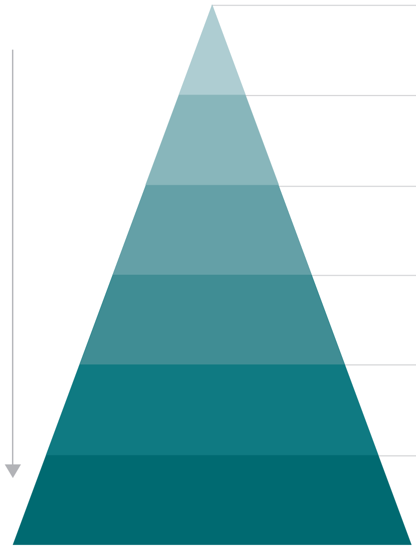
EXAMINING THE ENTIRE PYRAMID: THE TIP IS ONLY A STARTING POINT

EMV compliance and approvals are often viewed as the only steps required by acquirers to prepare for EMV migration. However, they represent the absolute minimum requirements and should be considered only the "tip of the pyramid" of business imperatives that can maximize EMV deployment success.

Most importantly, the business shift to support EMV must have a longer-term vision in mind even under the current readiness timelines.

FIGURE 3: ACQUIRED READINESS QUESTIONS

The Shift To Support EMV Must Have A Longer Term Strategy In Mind



Certifications/ Approvals - How do you get approved? When should you be approved?

Support - What are you doing to be prepared? Have your resources recieved sufficient EMV training to effectively implement EMV support?

Terminals - How many terminal combinations and terminal models will you need to approve? How will you implement new terminal key management functions?

Applications - Are you implementing EMV logic into proprietary terminal applications?

On-Boarding - Are you prepared to support the on-boarding of merchants that want to intergrate the EMV logic into their POS systems?

Partners - How are your partners in the value chain, like ISOs and VARs becoming prepared for EMV migration?

SEVEN GUIDING PRINCIPLES FOR EMV READINESS

There are seven guiding principles that MasterCard Advisors has compiled for initial acquirer EMV readiness.

1. EMV Payment Network Approvals

Consolidate all known network requirements and plan for flexibility to meet future requirements with minimal recertification efforts.

Each payment network requires terminals to be tested and approved prior to deployment. The purpose of this testing is to ensure that implementation of any applications, specifically the payment application, in the merchant environment does not adversely impact the EMV functionality (kernel) previously approved by EMVCo. Acquirers should have all their EMV terminals approved by all payment networks prior to terminal deployment. Deploying without payment network approval may result in interoperability issues requiring terminal software upgrades and redeployment.

In Canada, terminals were initially approved for only one payment network and later had to be re-launched when they were ready to support other payment network approvals. Because of this redeployment, several acquirers had to go through multiple, not to mention timely and costly, terminal certification iterations.

In Canada, terminals were initially approved for only one payment network and later had to be re-launched when they were ready to support other payment network approvals. Because of this redeployment, several acquirers had to go through multiple, not to mention timely and costly, terminal certification iterations.

2. EMV Terminal Selection

Select EMV terminals with the right capabilities and approvals to meet your customers' needs.

EMV is an option-based specification. Some of these options that terminals may or may not support include Offline Data Authentication (ODA) and PIN support. Payment networks will often specify which EMV options are required and which ones may be optionally supported in a market. Acquirers and merchants will need to decide which of these options they want to support. They will also need to determine the type of environment within the terminal at which they will be deployed. To help acquirers and merchants determine which terminal meets their needs, terminal vendors have Implementation Conformance Statements (ICS) that indicate which EMV features are supported by each terminal.

Acquirers and merchants should make every attempt to select the most recently approved terminals. In addition, merchants implementing contactless payments will need to obtain terminals supporting MasterCard's *PayPass 3.0* specification.

3. Terminal Management

Invest in automated POS management systems to remotely implement terminal updates.

EMV terminals require more frequent updates to software and EMV-specific parameters than do traditional terminals. Centralized terminal management software to update terminals remotely is worth the initial investment to prepare for continued EMV maintenance requirements and enhancements, particularly as innovation continues in the market. In markets like Mexico and Canada, not having terminal application management systems led to time-consuming and costly in-person manual updates to terminals.

While smaller markets may be able to implement in this inefficient manner, the U.S. market characteristics and demand for customer responsiveness will make in-person and manual updates difficult to sustain over time. Considering the emergence and development of e-tablets and mobile phones into the acceptance market space, terminals may soon need to support frequent updates to remain competitive both with alternative POS devices and the demand for new functionality.

EMV terminals require more frequent updates to software and EMV-specific parameters than do traditional terminals. Centralized terminal management software to update terminals remotely is worth the initial investment to prepare for continued EMV maintenance requirements and enhancements, particularly as innovation continues in the market.

4. EMV Key Management

Add trained support/resources for key management even if not used immediately.

Key management should be a central part of any acquirer's implementation planning. Cryptographic keys play a vital role in offline card/device authentication, as well as offline PIN support. These keys require periodic updates and deletions.

Offline authentication can play a vital role when retailers or acquirers experience communication downtime. Implementing terminals without offline card authentication support and without a key management support strategy can lead to substantial support costs that could ultimately require terminal redeployment at a later date.

5. EMV Testing and Test Tools

Additional testing should be completed on top of specified payment networks' approval tests: Test Everything!

Prior to deploying EMV terminals, it is essential to complete multiple stages of testing for each terminal brand model and configuration that is deployed. The first stage of testing or approval is EMVCo Level 1 and Level 2 testing. These are the hardware interface (Level 1) and EMV kernel or software (Level 2) approvals that the terminal vendors should have received before you purchased the terminals.

The next level of testing is payment network level testing. Each payment network has defined a specific set of tests that must be passed before the network will approve the terminal for support of its EMV chips.

The next level of testing is payment network level testing. Each payment network has defined a specific set of tests that must be passed before the network will approve the terminal for support of its EMV chips.

There is another level of "best practices" testing that is not required but can have a significant impact on the cost and overall EMV migration success. Some of these best practices include reversal processing and exceptions, such as a card being removed prior to transaction completion for a contact transaction.

6. EMV Merchant On-Boarding Process

Implement tools where possible to reduce the time and technical expertise required.

The EMV deployment process will vary by type of customer. Many merchant customers will simply require a new "standalone" terminal with EMV functionality supported. Other larger or niche retailers will have unique payment processing needs that require integrating the EMV kernel and payment network logic into their highly customized point of sale (POS) and point of interaction (POI) systems.

Both the retailer and the acquirer must have a deep understanding of EMV terminal and card interaction as well as messaging requirements. This presents both a challenge and an opportunity for acquirers to play a vital role in merchant education. Having the ability to test customers' specific EMV implementation requirements can lead to either a much deeper relationship or one that is strained, depending upon the ability to respond to these support needs.

Meeting the challenge to support "integrated merchants" represents an opportunity to demonstrate greater customer service while reducing the resource time and cost of supporting the on-boarding process. On-boarding an integrated merchant requires the ability to receive frequent test transactions throughout the development cycle, perform detailed data analysis of the EMV data passed in the transactions, and rapidly respond. Delayed responses have a direct impact on a merchant's EMV integration timeline. By investing in on-boarding test tools, messaging can be rapidly analyzed and the results presented in more simplistic terms, which decreases reliance on EMV and transaction messaging experts.

An acquirer in Canada took a step back prior to EMV migration to reexamine their needs, and eventually they completely reengineered their systems. While EMV does not require a complete system rebuild, it gave this acquirer the chance to take a look at their systems infrastructure. Now they are able to provide more features in the terminal, which offers greater value to their customers and a better sales story for expanding share.

7. Post-Deployment Monitoring

Monitor performance data to identify change requirements early and provide enhanced customer service.

The objective of post-deployment monitoring is to identify problem areas such as system issues and exception processing challenges early in the implementation process and capture data for benefit analysis. Another reason to incorporate monitoring is to observe chip utilization rates and magstripe fallback volumes to alert customers about potential abuses. This can increase customer satisfaction, produce service revenue opportunities, and provide valuable data to build business cases for merchants that have not yet migrated to EMV.

The objective of post-deployment monitoring is to identify problem areas such as system issues and exception processing challenges early in the implementation process and capture data for benefit analysis. Another reason to incorporate monitoring is to observe chip utilization rates and magstripe fallback volumes to alert customers about potential abuses.

OTHER EMV CONSIDERATIONS

In addition to the seven guiding principles, there are other considerations around EMV that acquirers will need to think about when rolling out EMV terminals.

Kernel Lifecycle

Acquirers and merchants need to be aware that the EMVCo Letter of Approval (LOA) for a terminal is valid for a three-year period. MasterCard requires terminals to have a valid LOA when M-TIP (M/Chip Terminal Integration Process) testing is performed.

If acquirers or merchants plan on purchasing EMV terminals, and deploying them with the EMV functionality disabled prior to performing the MasterCard approval processes, they must ensure that the approval processes will be performed before the LOA expires.

Once a terminal has gone through the MasterCard approval process, acquirers and merchants can continue to deploy these devices into the field, even after the LOA on the terminal has expired.

Only terminal vendors may submit terminals to EMVCo to receive an LOA. Terminal vendors may resubmit a terminal to EMVCo to renew the LOA, provided the terminal is able to pass current EMVCo testing requirements.

EMV Fraud Detection Capabilities

Implementing EMV provides the ability to focus on "bad" magstripe transactions. While EMV deters counterfeit, lost, stolen, and NRI fraud if PIN verification is used, the magstripe will still be a viable form factor for the near future. And since fraud could still occur during this time, acquirers need to be able to help merchants detect and prevent it.

Being able to "analyze the data" to enhance and develop new fraud logic, especially as the U.S. migrates to EMV, mobile, and beyond, will be critical. One example of EMV-specific fraud logic might be automatic rule creation.

Durbin Impact on EMV

Many participants across the industry are still working to evaluate the final impact of the Durbin Amendment and the requirement to support at least two unaffiliated networks on debit cards. This process becomes more complex with EMV cards because of the payment network-specific implementation dynamics of the chip application and the issuer risk management settings.

Some networks do not have support for EMV while other payment networks have over 15 years invested in EMV technology and field experience. When acquirers and merchants implement EMV for debit cards, it will be important to clearly understand their options and the ramifications of sending transactions through unaffiliated networks.

Some networks do not have support for EMV while other payment networks have over 15 years invested in EMV technology and field experience. When acquirers and merchants implement EMV for debit cards, it will be important to clearly understand their options and the ramifications of sending transactions through unaffiliated networks.

EMV/Mobile Linkage

As acquirers implement contactless EMV, they may also want to build NFC technology infrastructure to enhance the consumer experience for price checks, promotions, and much more. Current forecasts indicate that mobile contactless will have a substantial impact on the overall consumer experience as well as future sources of revenue.

EMV for Online and Card Not Present Usage

In markets like the UK, dynamic authentication used in Chip Authentication Program (CAP) readers is combined with SecureCode to combat online fraud and to authenticate users of online banking services.

EMV dynamic authentication security is also built into mobile contactless, which enables MasterCard to transfer CAP technology to the mobile handset and eliminate the need for a special CAP reader. CAP technology in the mobile phone can then be implemented to support e-commerce transactions and begin to combat fraud in the online and Card Not Present (CNP) environments. In a future online shopping scenario, consumers may be able to tap their NFC phone against their NFC computer to create a “Phone Present” transaction... time will tell.

CONCLUSION

Developing an EMV business case is complex, but all acquirers need to be in the process of developing EMV capabilities. EMV implementation will change the nature of terminal deployment and management as well as customer on-boarding processes moving forward.

Acquirers should leverage lessons learned in other markets while also building new tools to manage terminal software updates and reduce operational costs. Do not underestimate the resources that will be needed for EMV migration efforts; establish timelines for implementation and monitor deployment resource constraints.

Planning is everything; plan for the future today. The longer an acquirer delays EMV migration, the greater the risk to their business and to their customers. There are experienced companies in the U.S., like MasterCard, that can maximize an acquirer's EMV investment.

Contact MasterCard now as we are ready to help with EMV network approvals and also provide consulting services through MC Advisors' subject matter experts.

ENDNOTES

[1] EMV (Europay, MasterCard and Visa) is a global, interoperable standard for secure chip payments.

[2] Mercator Advisory Group, *The State of EMV Adoption: A Global Update*, January 2012.

[3] EMVco governs the EMV standard.

AUTHORS

Phillip M. Miller Global Head of the Acquiring Knowledge Center
Phillip_Miller@mastercard.com

Guy Berg Senior Managing Consultant and EMV Subject Matter Expert
Guy_Berg@mastercard.com

Jeff Stroud Senior Managing Consultant and EMV Subject Matter Expert
Jeff_Stroud@mastercard.com

Steven Paese MasterCard Advisors Consultant
Steven_Paese@mastercard.com

FURTHER MASTERCARD ACQUIRER SPECIFICATION SUPPORT INFORMATION

For questions regarding MasterCard specifications, please contact MasterCard Worldwide: USPOI@mastercard.com

Chris Benedict Senior Business Leader, Expert Sales
Chris_Benedict@mastercard.com

For questions regarding EMV implementation for acquirers and the "Seven Guiding Principles for EMV Readiness," please contact MasterCard Advisors:

Phillip Miller Global Head, Acquiring Knowledge Center
Phillip_Miller@mastercard.com

For additional insights, please visit www.mastercardadvisors.com and insights.mastercard.com.

Insights and recommendations are based on proprietary and third-party research, as well as MasterCard's analysis and opinions, and are presented for your information only.

ADVANCING INSIGHTS ADVANCING COMMERCE.