EMV Migration Forum

Payments Security Task Force (PST)

U.S. Market – The Big Picture

EMV Migration Forum/Payments Security Task Force
April 2015

About the EMV Migration Forum and the Payments Security Task Force

The EMV Migration Forum is a cross-industry body focused on supporting the implementation steps required for global and regional payment networks, issuers, processors, merchants and consumers to help ensure a successful introduction of more secure EMV chip technology in the U.S. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV chip technology in the U.S.

For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/

Announced in March 2014, **the Payments Security Task Force** is a cross-industry group focused on driving executive level discussion that will enhance payment system security. The Task Force comprises a diverse group of participants in the U.S. electronic payments industry including payment networks, banks of various sizes, credit unions, acquirers, retailers, industry trade groups, and point-of-sale device manufacturers.

EMV® Migration Forum

Introduction: *US Market – The Big Picture*

Welcome to the U.S. EMV Value-Added Reseller Qualification Program's educational webcast series, brought to you by the Payments Security Taskforce and EMV Migration Forum.

This is a brief on U.S. Market – The Big Picture, presented by Stuart Miller of FIME.

Note: This webcast is one in a series of webcasts which will provide U.S. value added resellers, independent software vendors and merchant organizations with understanding of the U.S. market for EMV migrations, U.S. debit deployment, development preparation, lessons learned and testing considerations to assist with EMV chip migrations.

EMV® Migration Forum

Why should I support EMV migration at all? Why is EMV chip necessary? Why now?

- EMV migration is not just about security but also about migrating to a global standard that not only offers better security, but is the baseline for new payment products and solutions like mobile payments.
- The U.S. is the last major market to broadly adopt EMV. Recent breaches are testimony to the increased security threat that the U.S. payments industry is facing and EMV is a critical step to further secure the payments industry.
- Key reasons:
  - Security & fraud
  - Future innovation
  - Global standard and interoperability
  - Customers and merchant experience fewer fraud events
  - U.S. travelers experience fewer acceptance problems when traveling internationally

EMV® Migration Forum

What is the liability shift? How does it work? How does it differ by payment network? Why/how does it impact you or your clients? Is migrating to chip required?

- Liability shifts are being introduced by different payment networks to encourage accelerated adoption of chip technology in the U.S., thus making paying safer.
- October 1, 2015, the major U.S. payment networks plan to implement fraud liability shifts impacting who is responsible for counterfeit chip card transactions and/or lost or stolen chip card transactions at the retail point-of-sale. The details of the liability shifts for each payment network may vary.
- As of that date, liability for those transactions will shift to the merchant in certain cases if the merchant has not implemented EMV chip-enabled devices and applications to process EMV chip payment transactions.
- Liability shifts for ATM and automated fuel dispensers will take place at later dates, depending on the particular payment network.
- The counterfeit liability shift works by shifting responsibility for certain fraud transactions from the party that invested in EMV technology and to the party that did not.
- The EMV Migration Forum will publish a white paper soon, “Understanding the 2015 U.S. Fraud Liability Shifts,” which will summarize each payment network’s liability shift requirements. The white paper will be available on the EMV Migration Forum Knowledge Center webpage.

EMV® Migration Forum

If deploying an EMV solution in the U.S., what are the key considerations for the U.S. market? How are these different from other countries (e.g., Canada, Europe)?

- The U.S. market is different from other EMV markets due to its large size and fragmentation, regulatory requirements, and legacy infrastructure.
- Start planning for EMV migration immediately, if you have not already started. There is a substantial EMV learning curve.
- U.S. regulation requires that an issuer provide at least two unaffiliated network routing choices to the merchant for U.S. issued debit cards. This requires an EMV solution for the U.S. Refer to The EMV Migration Forum white paper "U.S. Debit EMV Technical Proposal" available on the EMV Migration Forum website. Also refer to the debit webcast for more details.
- Legacy systems may need significant change to accommodate EMV rather than an incremental upgrade.
- The pace of change of the U.S. EMV migration appears to be comparably faster than in other countries. This may result in the need to manage many projects in parallel. Consider the implementation challenge for each merchant may be different, depending on the merchant's system configuration.
- Evaluate whether a 'semi-integrated' solution can be used instead of a fully integrated solution. Not all merchants require a fully integrated solution and it can speed up the merchant migration.
- The EMV Migration Forum hosted a Value Added Reseller Training Day in September 2014. The recorded sessions and presentations are available on the EMV Migration Forum website.

EMV® Migration Forum

How does EMV help prevent fraud?

- The main reason for fraud reduction is preventing the re-use of cardholder data, typically in counterfeit cards and online fraud. The main types of theft of cardholder data are:
  - Theft from systems that store cardholder data
  - From the visible data embossed on the card
  - From the card magnetic stripe
- EMV creates a unique cryptogram for each transaction. Cardholder data is difficult to extract from card-present EMV transactions and difficult to re-use for in-person fraudulent transactions.

What is the outlook for fraud over the next 2 years? What is this 'multi-layered' approach? What is my current exposure to fraud and can this look different over time?

- Global migration statistics suggest the value of EMV technology is in reducing counterfeit fraud. Countries like UK, Canada and Mexico have migrated to EMV and have experienced a counterfeit fraud reduction in the range of 50-80%.
- A multi-layered approach extends cardholder data protection using a combination of EMV chip cards tokenization and encryption:
  - Tokens are derivations of the cardholder data that are difficult to re-use, such as Acquirer Tokens and Issuer Tokens.
  - Industry standards, such as the PCI Data Security Standard, call for encryption to protect data at rest and any time card data is transmitted over a public network.
  - Encryption can be initiated at the beginning of a transaction to protect data from being compromised inside a merchant environment by malware or other means.
- Experience of other countries suggests that, when EMV is implemented, criminals seek to attack less secure, non-EMV merchants.

Aren't there other technologies (e.g., mobile / Apple Pay) that are better/cheaper?

Should I prioritize mobile (NFC contactless) over EMV (contact chip)? How does Apple Pay leverage chip technology; what are the technological commonalities?

- EMV is the foundation for a more dynamic and secure payments infrastructure. It is not just about cards; some NFC-based mobile wallets, notably Apple Pay, are utilizing EMV security features today.
- Merchants should consider leveraging the opportunity to enable both contact and contactless chip technology, given the hardware will be present. We encourage merchants to complete contactless certification at the same time as contact chip.
- Apple Pay uses compatible technology, NFC technology, which supports EMV standards and is a global standard. Given the same payments technology, Apple Pay and EMV can be implemented at the same time.

How does migrating to EMV vary by major industry vertical/segment (e.g., retail, restaurants, gasoline, quick serve)?

- Industry verticals have different acceptance requirements due to their specific environments.
- The requirements of verticals vary considerably; some options suit specific environments better than others:
  - Retail may prefer terminals that are stand-alone, and are semi-integrated or fully integrated according to their size and environment.
  - Portable wireless terminals may be useful in remote and restaurant environments.
- Each vertical may require or suggest particular types of transactions be supported:
  - Pre-authorization may be necessary at a hotel for check in
  - Deferred authorizations may be needed when host connections are unavailable
- Cardholder amount entry or confirmation may be necessary
- Refer to the payment network requirements for details on particular transaction types and EMVCo best practices document on "Recommendations for EMV Processing for Industry-Specific Transaction Types."
- The EMV Development Preparation webcast will also provide more details.

Will magnetic stripe still be supported in the U.S.? For how long is this expected to continue? Will the U.S. be 100% chip on chip by October?

- The U.S. will not achieve 100% migration of chip cards and chip terminals by October 2015.
- The percentage of chip on chip transactions will increase mostly in the early stages of the migration as points of high-density transactions migrate.
- Points of lower density transactions will take longer as a larger number of systems need to be migrated.
- Magnetic stripe will continue to be supported for the foreseeable future and it continues to be supported in every market that migrated to EMV. Each payment network will need to decide when it will "retire" magnetic stripes.

EMV® Migration Forum

How do the PCI Security Standards Council and EMVCo work together?

- The PCI Security Standards Council and EMVCo have different perspectives and scope of influence, but both seek to make the payments industry more safe and secure. They collaborate for that purpose when feasible.
- EMVCo focuses on common standards across participating payment networks which enable the payments industry to operate on a common cardholder device and terminal technology.
- The PCI Security Standards Council focusses on security practices for protecting payment account data.

U.S. Market—The Big Picture

- EMV chip has strong security features proven to reduce counterfeit card fraud at card-present retail environments.
- The PCI Data Security Standard (PCI DSS) provides other complementary levels of security necessary when the account data reaches the merchant's system. Rather than focusing on a specific category of fraud, PCI DSS seeks to protect account data everywhere within the payment ecosystem, thus limiting the availability of this data to fraudsters. When used together, EMV chip and PCI DSS can reduce fraud and enhance the security of the payments ecosystem.

Consult with your acquirer and payment network for more details on their EMV implementation requirements.

FIME
Stuart Miller
Stuart.Miller@fime.com

EMV® Migration Forum

Payments Security Task Force (PST)

WWW.EMV-CONNECTION.COM