Resources and Guidance for EMV Implementation in a C-Store Environment

December 21, 2017

Version 1.0

CONEXXUS
solve forward

Document Summary

This document provides links into educational information and frequently asked questions regarding EMV implementations in the U.S.

Contributors

Alan Thiemann, Conexxus
Allie Russell, Conexxus
Bradford Loewy, Dover Fueling
Brian Russell, Verifone
Clerley Silveira, Verifone
Chuck Young, Impact 21
Don Emery, CHS
Gabe Olives, Impact 21
Greg Jones, World Pay
Jake Hoxha, Excentus
Jeff Minard, Toshiba GCS
Kara Gunderson, CITGO
Kim Seufer, Conexxus
Konstantin Dolgushin, Petrosoft
Linda Toth, Conexxus
Manju Aradhya, First Data
Maren Jackson, NCR
Matt Cogburn, Pilot Travel Centers
Mike Lindberg, CHS
Ron Hilmes, Chevron
Sharon Scace, WEX Inc.
Steve Reischman, Heartland

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
December 21, 2017	1.0	Linda Toth, Conexxus	- Final release version
November 7, 2017	0.15	Sharon A. Scace, WEX Linda Toth, Conexxus	- Updates from committee approval review: reword of loyalty section, receipt modification and copyright changes for non-member distribution.
October 24, 2017	0.14	Linda Toth, Conexxus	- Updates after committee review - Reordered resources within a section in reverse chronological order - Corrected formatting issues with headers
October 24, 2017	0.13	Linda Toth, Conexxus Alan Thiemann, Conexxus	Updates after legal review
October 10, 2017	0.12	Linda Toth, Conexxus Sharon A. Scace, WEX Kim Seufer, Conexxus	- Updates from committee review - Additional formatting - Updated kernel section - Updated contributors list
October 6, 2017	0.11	Linda Toth, Conexxus Sharon A. Scace, WEX	- Additional formatting - Updated from committee review - Updated fleet, manual entry, and loyalty sections - Added additional resources
August 29, 2017	0.10	Linda Toth, Conexxus Sharon A. Scace, WEX	- Additional formatting, arranging and wordsmithing of content as a result of committee review - Accepted prior changes to have a clean version to work with and review - Additional resources for petroleum—FAQ and Webinar.
August 23, 2017	0.9	Linda Toth, Conexxus	Formatting, arranging and wordsmithing of content
May 31, 2017	0.8	Sharon A. Scace, WEX	Revisions post meeting
May 9, 2017	0.7	Sharon A. Scace, WEX	Revisions during meeting
May 8, 2017	0.6	Sharon A. Scace, WEX Inc.	Revisions

April 18, 2017	0.5	Sharon A. Scace, WEX Inc.	Revisions
February 14, 2017	0.4	Chuck Young, Impact 21	Revisions
January 16, 2017	0.1	Sharon A. Scace, WEX Inc, Chair RFTC	Initial Version

Copyright Statement

This document may be furnished to others, along with derivative works that comment on or otherwise explain it or assist in its implementation that cite or refer to the standard, specification, protocol or guideline, in whole or in part. All other uses must be pre-approved in writing by Conexxus. Moreover, this document may not be modified in any way, including removal of the copyright notice or references to Conexxus. Translations of this document into languages other than English shall continue to reflect the Conexxus copyright notice.

The limited permissions granted above are perpetual and will not be revoked by Conexxus, Inc. or its successors or assigns.

Disclaimers

Conexxus makes no warranty, express or implied, about, nor does it assume any legal liability or responsibility for, the accuracy, completeness, or usefulness of any information, product, or process described in these materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any encumbrances resulting from third party intellectual property rights (IPR), it cannot guarantee that such IPR does not exist now or in the future. Conexxus further notifies all users of this standard that their individual method of implementation may result in infringement of the IPR of others. Accordingly, each user is encouraged to carefully review its implementation of this standard and obtain appropriate licenses where needed.

Table of Contents

1 Introduction

This white paper is intended to assist members of the petroleum and convenience industry to find information related to EMV. Three primary sources are the following organizations:

- Conexxus
- Secure Technology Alliance (formerly known as the Smart Card Alliance)
- US Payments Forum (formerly known as the EMV Migration Forum)

While many EMV resources exist, the resource links included in this document were found to be the most helpful and relevant to merchants in the petroleum and convenience industry. This document is organized as follows:

- EMV Basics: This is the section providing basic information and answers to commonly asked questions regarding EMV.
- Up Front Decisions: There are many decisions that must be made in advance of EMV implementation. This section covers some of these common areas (e.g., debit routing, contactless, optimizing transactions, fallback, manual entry).
- Cardholder Data Considerations: This is the section that clarifies the role EMV plays in protecting cardholder data.
- Testing and Certification: This is the section providing basic information regarding testing and certification of an EMV implementation.
- Ongoing Care and Maintenance: There are some processes that require ongoing management. This section covers some of those areas (e.g., chargebacks, kernel maintenance).
- Other considerations for topics that may be applicable to your particular business including:
    - ATMs;
    - Unattended payment terminals;
    - Tips and gratuities if you also have a restaurant or provide other services where tipping is allowed; and
    - Processing card not present transactions (i.e., you accept phone or online transactions).
- Additional resources available.

2 EMV Basics

2.1 Where can I find basic information about EMV?

The following resources are a good place to start for general EMV information:

EMV Frequently Asked Questions (FAQs)
Secure Technology Alliance developed these FAQs to provide answers to commonly asked questions regarding EMV.

Petroleum Industry: EMV FAQs
A more specific petroleum industry FAQ is also available from the U.S. Payments Forum.

Glossary of Standardized Terminology
This EMV Migration Forum glossary, published in 2014, defines acronyms and vocabulary commonly used to describe EMV chip cards and how they are processed.

Contact Chip Card Online Authentication
This EMV Migration Forum animated presentation is a non-technical overview of how an EMV transaction is secured using “cryptograms.”

Road to EMV on the Forecourt Webinar Slide Deck
This 2015 power point presentation from a Conexxus webinar provides an overview of EMV for outdoor terminals.

The 411 of EMV Webinar Slide Deck
This 2014 power point presentation from a Conexxus webinar provides an overview of the basics of EMV, what the liability shift means, and how to prepare.

Merchant Considerations for U.S. Chip Migration
This 2014 recording of an EMV Migration Forum webinar, held in partnership with the National Retail Federation, provides guidance to educate merchants on the global use of chip cards, the status of the U.S. migration, considerations for making the decision to accept chip payments, and tools to begin project planning for chip card acceptance implementation. While it is not specific to the petroleum industry, it does provide a good overview on chip cards.

EMV Workshop for VARs, ISVs and ISOs "Why EMV Now in the US"
This 2014 one-day event included 6 workshops. This link specifically refers to the "Why EMV Now in the US" workshop. The recording and PowerPoint provides an overview of the drivers for the U.S. migration to EMV.

A Guide to EMV Chip Technology
This 2014 EMVCo white paper provides good introductory information with helpful graphics. While it is not specific to the petroleum industry, it does describe what EMV is, how EMV is processed, and why payments are transitioning to EMV.

Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?
This 2013 Smart Card Alliance white paper discusses why merchants should adopt EMV. It provides a basic understanding of how EMV works, including both graphics and written explanations of the process.

The EMV Ecosystem: An Interactive Experience for the Payments Community
This 2013 interactive PowerPoint presentation from Smart Card Alliance provides an overview of the full EMV ecosystem, with participants who play roles in EMV issuance, acceptance and transaction processes.

2.2 Where can I find more advanced information about EMV?

For a deeper dive into EMV, these resources are available:

Accepting EMV Chip Payments at the Fuel Pump
This September 2017 webinar was a joint presentation by Conexxus and the US Payments Forum to help explain the complexities of the migration to chip technology at the pump in advance of the payments networks' October 2020 fraud liability shift.

The 411 of EMV after October 1, 2015
This 2016 recording of a Conexxus webinar addresses a overview of EMV, the myths about EMV, and breaks it all down for what it means for a petroleum/convenience merchant.

Cardholder Verification Methods (CVM)
This 2015 video recording by EMV Migration Forum reviews EMV Cardholder Verification Method (e.g., PIN, signature, no CVM) concepts, implementation and impact on issuers, ATM owners, merchants, and cardholders.

EMV 101 Webinar

This 2014 recording of an EMV Migration Forum webinar provides a primer on EMV chip payments. It is a comprehensive overview of EMV chip payments, including the EMV transaction flow and options for card authentication, cardholder verification, and transaction authorization. Note that this webinar predates Faster EMV processing.

EMV Workshop for VARs, ISVs and ISOs "EMV 101"

This 2014 one-day event included 6 workshops. This link specifically refers to the "EMV 101" workshop. The recording and PowerPoint provides an introduction to EMV for both technical and non-technical audiences on development considerations, implementation best practices, and testing.

EMV Workshop for VARs, ISVs and ISOs "Implementation Best Practice and Considerations"

This 2014 one-day event included 6 workshops. This link specifically refers to the "Implementation Best Practice and Considerations" workshop. The recording and PowerPoint is not specific to the petroleum industry but it provides a high-level project overview.

Video Workshop: How EMV Changes Payment

This series of videos, recorded in 2013, provides in-depth information about various aspects of EMV. Because these are older videos, some information may be outdated (e.g., liability shift dates, faster EMV processing). These videos in particular were found to have useful information on the following specific topics:

- Fundamentals of EMV Payments This video provides an in-depth overview of the EMV payment process. It includes details of risk management, online/offline authentications and CVM, with a detailed walk through of an EMV transaction flow. This video is very technical and is useful for someone who wants to understand what is happening "under the covers."
- Changes at the Point of Sale This video discusses EMV implementation options and considerations for card and mobile payments acceptance, including hardware, software, and transaction messaging support. Note that the liability shift dates presented are incorrect.
- EMV Testing and Certification This video provides an overview of the end-to-end testing and certification process required for EMV acceptance and outlines how it differs from the current magnetic stripe process. Note that this session does not cover UAT (merchant testing), which is an area that can be a stumbling block.

EMV Best Practices Web Resource

The EMV Migration Forum developed this searchable web resource to provide easy-to-find answers on commonly asked questions about best practices for implementing EMV chip technology. Note that many of the results from this search tool will point to resources listed in this guide.

2.3 Are there petroleum specific resources?

There is a Petroleum Frequently Asked Questions document on the U. S. Payments Forum website.

There is a September 2017 webinar, Accepting EMV Chip Payments at the Fuel Pump, that was jointly produced by Conexxus and U. S. Payments Forum to address the complexities of the migration to chip technology at the pump in advance of the payments networks' October 2020 fraud liability shift.

2.4 How will my loyalty program work?

Where loyalty credentials can be presented in an EMV transaction will depend on the EMV solution that is implemented:

- Full (standard) EMV; or
- Faster EMV (e.g., Quick Chip, M/Chip Fast).

In a full EMV solution, the payment card is in the reader during the entire authorization process. Depending on the implementation, loyalty may need to be processed before payment authorization.

In a faster EMV solution, loyalty can be presented before or after payment is presented.

2.5 How will fleet cards process?

There is ongoing work between Conexxus, the U.S. Payments Forum, and IFSF to address fleet cards. Documentation for this effort can be found in the member only section of the Conexxus website.

Fleet card companies use proprietary specifications for prompting and purchase restrictions with mag-stripe cards, utilizing track data which may be considered sensitive. Merchants have requested that EMV fleet cards take advantage of EMV capabilities to standardize prompting and purchase restrictions without having to use track data equivalent tags. The new specification, under development at Conexxus, has a tag specified to hold prompting information and a tag to hold purchase restriction information. These tags provide flexibility to the fleet card issuer for specifying prompts and data restrictions, while standardizing how the tags are interpreted across all cards using the tags. In addition, using these new tags instead of track equivalent data tags removes the concern that POS systems may not have access to needed data under generic point-to-point encryption environments.

2.6 How can I help train my customers?

GoChipCard.com

This website was developed by the EMV Migration Forum and the Payments Security Task Force for consumers, merchants, and issuers. Merchants and issuers are encouraged to use the website content when developing communications with customers, cardholders, and employees. The site provides easy-to-use and downloadable resources, including training FAQ, a merchant infographic, and recommendations on communications best practices.

Communications Best Practices Guide

This guide covers communications points for the issuer and merchant to use with the customer.

2.7 Will my receipts change?

Your acquirer will provide specific receipt requirements. This section explains some of the lines that may be added to the receipt. Values involved in an EMV transaction are transported and identified by a "tag," which is simply an identification for each piece of data. Below are some of the common values (and their associated tags) that may be required on the receipt. Not all the values are required by every acquiring processor; in fact, the least common denominator is often just the Application Identifier (AID). Note that Hexadecimal digits are 0-9, A, B, C, D, E, and F.

- ***AID***: Application Identifier is specified in EMV tag 9F06. The AID identifies the EMV application used to process the EMV transaction. The AID must be present on both the card and the terminal in order for the application to be used to process the EMV transaction. Some cards have multiple AIDs on the card (e.g., Brand Global AID and U.S. Common AID[1] (CAID) both are on U.S. Debit cards). At a high level, the AID controls how the transaction is processed. For example, a "brand global" AID may not prompt for a PIN, while a "U.S. Common" AID will usually prompt for a PIN. The value can be alphanumeric characters
- ***Application Name***: This information is specified in EMV tag 9F12. In addition to the AID, many acquirers specify the receipt contain the application name as well. The value comes from the chip on the card and is determined by the issuer.
- ***ARC***: Application Response Code is specified in EMV tag 8A. Generally, an approved transaction will have a "00" value shown. ARC values shown in a

[1] Each brand has a Common AID (CAID)

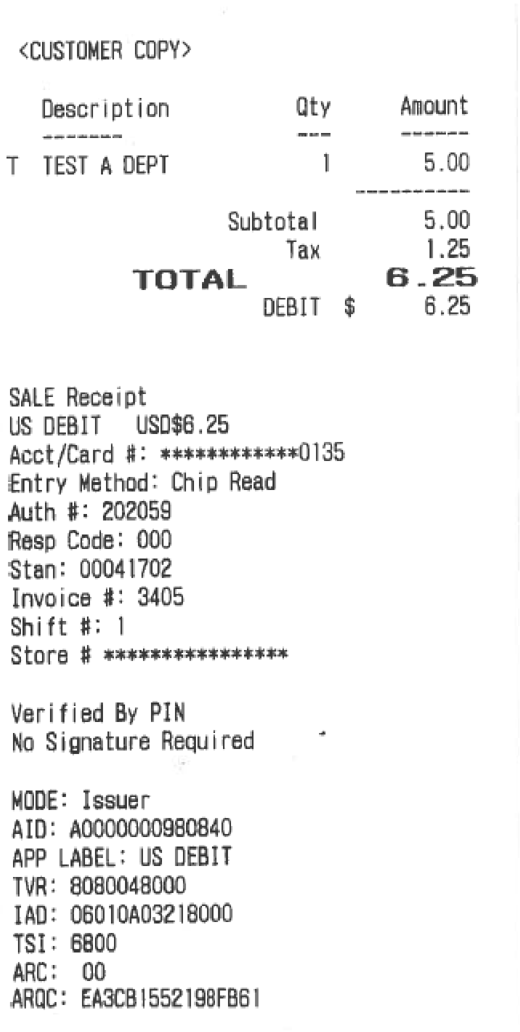
declined receipt can be used to determine why a transaction may have been declined.

- ***TVR***: Terminal Verification Results is specified in EMV tag 95. This value will be shown as 10 hexadecimal digits (e.g., 8000088000). The value is a bitmap described in the EMVCo Specification, which represents the results of the EMV portion of the transaction[2]. Generally, unless a transaction is declined, the value is simply informative in nature. For instance, the TVR value 8000088000 indicates that:
  - offline data authentication was not performed
  - a PIN was prompted for but not entered.
  - the transaction exceeded the floor limit.
- ***ARQC or ARPC or AC:*** Application Request Cryptogram or Application Response Cryptogram or Application Cryptogram is specified in EMV tag 9F26. This value contains a cryptographic "signature" that allows the EMV card and the EMV card issuer to validate that the card is a genuine (not fraudulent) EMV card. The value is 16 hexadecimal digits. Its value cannot be verified by the merchant or a consumer. Only the chip on the card or the issuer of the card can validate its value. Even though it is a cryptogram, and looks "secret," the data is not considered sensitive in any PCI relevant manner.
- ***TSI***: Transaction Status Information is specified in EMV tag 9B. This status is a hexadecimal string representing a bit map describing the transaction status as reported by the terminal. Interpretation of this value requires an understanding of hexadecimal numbers, bitmaps, and access to the EMVCo EMV specs. Generally, unless a transaction is declined, the value is simply informative in nature.

Many acquiring processors require that additional values be included on the receipt when a transaction is declined. This data can be useful for troubleshooting reasons for transaction failures.

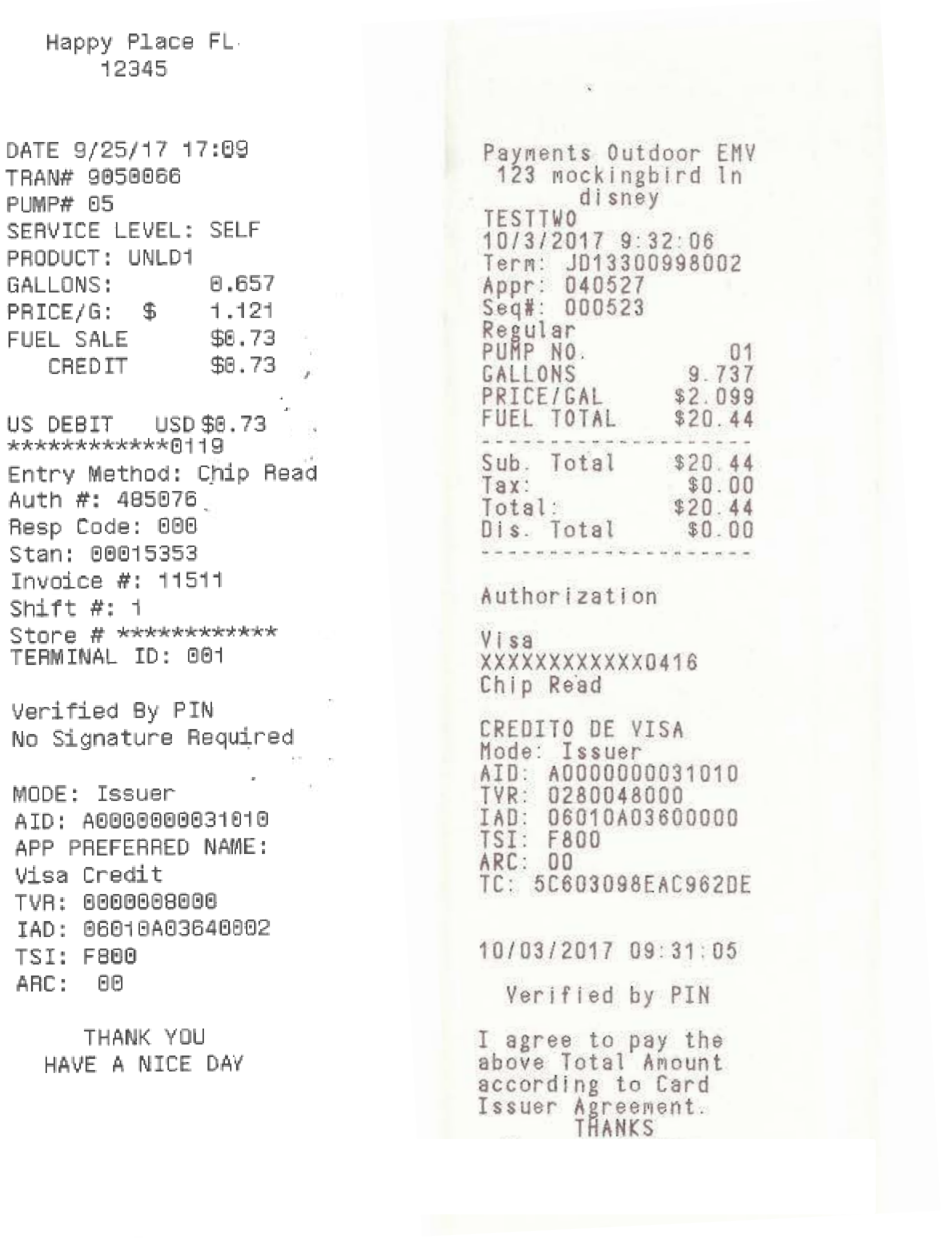
Following are example receipts. Note that receipts may not include all of the EMV elements. Check with your vendors and/or processors regarding their specific requirements.

[2] Interpretation of this value requires an understanding of hexadecimal numbers, bitmaps, and access to the EMVCo EMV Specification. There are online TVR decoders, for example: https://tvr-decoder.appspot.com/t/decode/95/EMV/8000088000.



```
<CUSTOMER COPY>

   Description          Qty     Amount
   --------             ---     ------
T  TEST A DEPT            1       5.00
                               ----------
                   Subtotal       5.00
                        Tax       1.25
          TOTAL                   6.25
                      DEBIT  $    6.25


SALE Receipt
US DEBIT   USD$6.25
Acct/Card #: ************0135
Entry Method: Chip Read
Auth #: 202059
Resp Code: 000
Stan: 00041702
Invoice #: 3405
Shift #: 1
Store # ****************

Verified By PIN
No Signature Required

MODE: Issuer
AID: A0000000980840
APP LABEL: US DEBIT
TVR: 8080048000
IAD: 06010A03218000
TSI: 6800
ARC:  00
ARQC: EA3CB1552198FB61
```

Figure 1: Inside Receipt Example



```
   Happy Place FL
       12345


DATE 9/25/17 17:09
TRAN# 9050066
PUMP# 05
SERVICE LEVEL: SELF
PRODUCT: UNLD1
GALLONS:         0.657
PRICE/G:  $      1.121
FUEL SALE        $0.73
   CREDIT        $0.73

US DEBIT   USD $0.73
*************0119
Entry Method: Chip Read
Auth #: 485076
Resp Code: 000
Stan: 00015353
Invoice #: 11511
Shift #: 1
Store # *************
TERMINAL ID: 001

Verified By PIN
No Signature Required

MODE: Issuer
AID: A0000000031010
APP PREFERRED NAME:
Visa Credit
TVR: 0000008000
IAD: 06010A03640002
TSI: F800
ARC:  00

      THANK YOU
   HAVE A NICE DAY
```

```
Payments Outdoor EMV
 123 mockingbird ln
       disney
TESTTWO
10/3/2017 9:32:06
Term: JD13300998002
Appr: 040527
Seq#: 000523
Regular
PUMP NO.            01
GALLONS          9.737
PRICE/GAL       $2.099
FUEL TOTAL      $20.44
--------------------
Sub. Total      $20.44
Tax:             $0.00
Total:          $20.44
Dis. Total       $0.00
--------------------

Authorization

Visa
XXXXXXXXXXXX0416
Chip Read

CREDITO DE VISA
Mode: Issuer
AID: A0000000031010
TVR: 0280048000
IAD: 06010A03600000
TSI: F800
ARC: 00
TC: 5C603098EAC962DE


10/03/2017 09:31:05

  Verified by PIN

I agree to pay the
above Total Amount
according to Card
Issuer Agreement.
       THANKS
```

Figure 2: Outside Receipt Examples

3 Up Front Decisions

There are many decisions that must be made in advance of EMV implementation. The resources in this section may help you with making some of those up-front decisions.

3.1 Debit Considerations

To support debit EMV processing, considerations need to be given to prompting, routing, and PIN entry requirements. The following resources are available to help in understanding the choices when it comes to debit processing.

Implementing EMV in the U.S.: How the U.S. Common Debit AIDs Facilitate Debit Transaction Routing and Ensure Durbin Compliance

The Durbin amendment requires that merchants have the ability to choose between at least two unaffiliated networks when routing debit transactions. This US Payment Forum video recording, updated in 2017, provides an overview of the U.S. Common Debit AIDs and how they facilitate debit transaction routing and ensure Durbin compliance. It provides good historical information and background on prompting.

PIN Bypass in the U.S. Market

This US Payments Forum white paper, updated in 2017, provides an overview and considers the impact of implementing PIN Entry Bypass, which can be used to allow cardholders to opt out of PIN entry on a PIN-preferring EMV card. It also discusses alternative processes that allow selection of cardholder verification methods.

U.S. Debit EMV Technical Proposal

This 2015 EMV Migration Forum white paper takes a more in-depth look at EMV debit and defines recommendations for a debit technical framework for the U.S. payments industry.

3.2 Contactless EMV Implementations

Contactless EMV may be implemented separately from Contact EMV. The following resources provide information about contactless EMV:

Contactless EMV Payments: Merchant Opportunities

This 2016 Smart Card Alliance webinar discusses the opportunities that contactless EMV payments offer to merchants. It provides good background information, as well as information on adoption rates in other countries, transaction security, and consumer and merchant experiences. Note: In the U.S., NFC-capable terminals are primarily deployed inside at the present time and there will be an additional cost to deploy outdoor terminals.

Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers

This 2016 Smart Card Alliance white paper and infographic provides a look at contactless payments, gives an overview of contactless EMV in the current U.S. payments environment, and summarizes the benefits of adoption.

EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments
This 2015 Smart Card Alliance white paper discusses chip migration in the US market and provides an in-depth explanation of how EMV and NFC are companion technologies and clarifies how they work together. Note: some stats may be outdated, but the information in general is still valid.

3.3 Merchandising at the Pump

While the EMV Specification does not preclude selling merchandise (e.g., carwash, motor oil) at the pump, in an EMV transaction flow the initial card insertion may not be able to accommodate the sale of merchandise. In 2017, dispenser and POS vendors have typically coordinated the timing of a car wash offer into the initial cryptogram. Other merchandise offers are not typically available before a customer begins fueling. Due to current EMV Specification requirements, sale of merchandise will likely be done in a separate transaction, and in the case of Faster EMV, will probably require a second card insertion.

3.4 Optimizing Transactions

Because EMV chip cards are inserted into the terminal, often for a period of time, consumer perception is that EMV transaction processing is slow as compared to traditional mag-stripe card processing. As a result, merchants may want to consider ways to optimize the transaction for a better customer experience.

Support for “Faster EMV” (i.e., optimized online-only EMV processing) was announced independently by four of the card brands in 2016 under various names (e.g., Quick Chip). Now an integral part of the EMV landscape, this variation allows for a better customer experience by shortening the time of interaction between the card and the terminal. There are also a smaller number of test transactions to be completed for Faster EMV, so certification timelines may be shorter. Merchants may want to consider “Faster EMV” for new implementations. The following resource provides information on Faster EMV, as well as other ways to optimize transactions:

Optimizing Transaction Speed at the POS
This 2017 U.S. Payments Forum white paper discusses approaches and potential impacts to help speed up EMV transactions. It presents information in three areas: “Faster EMV” solutions, contactless/Near Field Communication (NFC) transactions, and other EMV checkout optimization practices.

3.5 Minimum EMV Requirements

Each payment network in the U.S. has minimum card and terminal requirements for EMV transaction processing. This resource may be helpful:

Minimum EMV Chip Card and Terminal Requirements – U.S.

This 2016 U.S. Payments Forum matrix summarizes the minimum card and terminal EMV requirements, as well as required cardholder verification methods at the terminals for individual payment networks in the U.S. (American Express, Armed Forces Financial Network (AFFN), China Union Pay, Discover, Jeanie, Mastercard, NYCE, PULSE, SHAZAM, STAR and Visa). Note that, for petroleum, the requirements for inside terminals are not the same as outside terminals.

3.6 Fallback to Magnetic Stripe

Fall back to magnetic stripe (not related to traditional fallback/store and forward) may happen if the chip in an EMV card cannot be read. This kind of fallback may impact merchant liability and/or interchange rates. The following resource is available for further information:

EMV Implementation Guidance: Fallback Transactions

This 2015 EMV Migration Forum guide outlines potential causes of fallback transactions and actions that can be taken to address the problem.

3.7 Manual Entry

Manual entry has historically been used as a backup method to enter payment information when a magnetic-stripe card cannot be read. Some payment card brands have announced that when EMV is operational, manual entry no longer needs to be supported. Before turning off manual entry, a merchant should refer to its operating agreements, consult with its vendors/processors and consider the following:

- Some card types may still require manual entry, particularly if they are not EMV capable (e.g., fleet, EBT) and some POS systems do not have the ability to turn off manual entry by card type;
- Sites that allow post-pay fuel transactions may wish to retain manual entry for the case where the chip and the magnetic-stripe both fail and the customer has no other payment method; and
- Some certifications may still require manual entry.

3.8 Communications Disruption

A decision on how (if) to process EMV transactions when communications are disrupted will need to be made. You should discuss your options with your vendors and/or acquirer. The following resource may provide helpful information:

Merchant Processing during Communications Disruption

This 2016 EMV Migration Forum white paper discusses best practices for merchants processing EMV chip transactions to follow when communications are disrupted resulting in the site not being able to obtain an authorization. It defines three processing options: EMV offline authorization; deferred authorization of an EMV card transaction; and force post of an EMV card transaction. This discussion includes the definition, authorization and/or clearing, and known liability concerns for each method. Also note that while calling for authorization (also called voice authorization) is not formally discussed, it may still be available.

4 Cardholder Data Considerations

EMV provides additional mechanisms for validating the cardholder, as well as validating the card itself. EMV does not replace any of the existing security measures that are required to protect cardholder data, including the PCI standards. EMV does not encrypt cardholder data. Existing security measures, including encryption and tokenization, are still applicable to EMV card processing. These are complementary technologies and should be considered in addition to EMV. The following resources are available for further information:

Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization
This 2014 Smart Card Alliance white paper describes the role of EMV, in addition to two other technologies, encryption and tokenization, for securing the payments infrastructure and preventing payment fraud. It discusses authentication methods in EMV and the importance of fraud management. It has a comprehensive overview of encryption and tokenization methods, standards, and merchant value.

EMV Workshop for VARs, ISVs and ISOs "Payment Security Standards"
This 2014 one-day event included 6 workshops. This link specifically refers to the "Payment Security Standards." The recording and PowerPoint is focused on how cardholders, merchants, and banks share trust in a payment transaction process and how standards bodies help create that framework of trust. This is slightly dated but provides an overview of the complexity behind the scenes.

PCI DSS Applicability in an EMV Environment
This 2010 PCI Security Standards Council white paper lays out how the capabilities of EMV enhance, but do not replace, the Payment Card Industry Data Security Standards. It provides details on why PCI DSS is still necessary, and why EMV is not the complete solution.

5 Testing and Certification of an Implementation

Testing and certification of an EMV solution must be performed before deployment begins. This ensures that the solution can process EMV (and other) transactions correctly and minimizes the possibility of problems in the field. You will need to work with your vendors and acquirer/processor to devise a test plan that is suitable for your needs. The following resources are also available:

EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community

This 2016 white paper by the EMV Migration Forum Testing and Certification Working Committee describes the current processes required to test EMV chip transactions with American Express, Discover, Mastercard, and Visa. The white paper provides a clear approach to acquirer host and EMV chip terminal testing and certification and includes examples of use cases that identify when testing or retesting is required for EMV chip and contactless terminals, when retesting is recommended as a best practice, and when only standard internal testing is advised. It also covers the testing and certification requirements for faster EMV implementations.

EMV Workshop for VARs, ISVs and ISOs "Testing Best Practices"

This 2014 one-day event included 6 workshops. This link specifically refers to the "Testing Best Practices." There is a recording and PowerPoint presentation which focuses on the terminal integration testing. This may be handled by a solution provider. Note that this does not discuss "Faster EMV" since it was introduced after the workshop.

6 Ongoing Considerations

6.1 Chargebacks

Once an EMV solution is implemented, ongoing chargebacks may be a concern. You should develop a plan to review and resolve chargebacks. The following resources may be helpful:

EMV Chargeback Best Practices

This 2017 US Payments Forum white paper and webinar discuss the appropriate treatment, mitigation, and best practices for both counterfeit and lost/stolen chip liability shift chargebacks occurring after the liability shift dates for contact chip cards used in attended transactions.

6.2 EMV Kernels

EMV kernels are an integral part of the terminal and payment application that enables EMV functionality. Kernels are broken out by two levels: level 1 kernels control the physical reading of the chip card; level 2 kernels manage the transaction from card insertion though verification. Kernels are tested and certified according to an EMVCo certification process. In petroleum applications, it is very likely that the terminals outside use a different EMV kernel than the terminals inside the store. Kernels may need to be updated to understand and interact with newer chips or processing features.

You can think of a kernel upgrade as similar to having to upgrade your PC Operating System to be able to get the latest version of an application to work. The difference is that an EMV kernel actually has an expiration date set in advance. It is important to make sure you are not operating with EMV kernels that have expired. Kernel expiration dates may be extended, particularly if no new functionality is introduced or additional updates aren't needed. When discussing the EMV kernel with your providers make sure it is clear when it expires and how it can be updated. Also, you should determine if your kernel can be updated remotely or is a site visit required, and whether new hardware will be required.

7 Other Considerations

7.1 ATMs

If your site includes an ATM, the following resources provide information for understanding the impact of EMV on ATMs:

Implementing EMV at the ATM

This 2015 EMV Migration Forum white paper provides an educational resource for stakeholders responsible for the implementation of EMV at the ATM in the U.S.

Implementing EMV at the ATM Webinar

This 2015 EMV Migration Forum webinar recording provides a non-technical review of the critical components of the EMV implementation process at ATMs. It includes basic requirements, fundamental concepts, as well as planning recommendations and best practices.

National ATM Council

The National ATM Council ("NAC") is a not-for-profit trade association that supports the business interests of ATM owners, operators, and suppliers.

7.2 Unattended Payment Terminals (Non-AFD)

If your site includes unattended payment terminals not related to an automated fuel dispenser (AFD) (e.g., car wash, vacuum, air hose), you must take into account that the EMV liability shift for these terminals went into effect on October 1, 2015. Care should be taken to include these terminals in your EMV migration and implementation plan.

7.3 Tips and Gratuities

If your business includes the application of tips and gratuities (e.g., a restaurant), the following resources may be helpful:

Managing Card-Based Tip and Gratuity Payments for EMV Chip
This 2017 EMV Migration Forum white paper provides information on how to best manage transactions which include tips and gratuities as the U.S. migrates to chip, and what options restaurant owners and other merchants in travel and entertainment can pursue. This document is intended to provide a high-level overview and reviews the three ways in which tips and gratuities may be processed in a an EMV chip environment.

National Restaurant Association
The National Restaurant Association ("NRA") is a foodservice trade association that supports restaurant owners and operators.

7.4 Card Not Present

Online or payments via telephone are CNP (card not present) transactions. These transactions cannot take advantage of the added security of a chip card and may see increased fraud activity as EMV solutions are rolled out. If your business accepts CNP transactions, the following resources provide information and potential ways to mitigate CNP fraud:

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud
This 2016 EMV Migration Forum white paper, which includes graphics and statistics, provides an educational resource on the existing best practices for authentication methods and fraud tools to secure the card-not-present (CNP) channel.

Card-Not-Present Fraud: A Primer on Trends and Transaction Authentication Processes
This 2014 Smart Card Alliance white paper discusses the impact of and need to address card-not-present fraud in conjunction with migration to EMV in the U.S.

8 Additional Resources

These resources may also be helpful:

Merchant Advisory Group

This organization provides good information in the members only section of their website.

EMVCo

EMVCo is responsible for developing and maintaining the EMV technical specifications and related testing processes. Released versions of these specifications can be downloaded from the website. In addition, the website offers general information and bulletins regarding the specifications and new work items. Note: Specification documents are very technical in nature.

EMV Connection

This website, maintained by Secure Technology Alliance, provides information and educational resources on EMV and is the source of many links found in this document.