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

March 11, 2021

Version 1.3

CONEXXUS
solve forward

Document Summary

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

Contributors

Alan Thiemann, Conexxus
Allie Russell, Conexxus
Bradford Loewy, NCR
Brian Russell, Verifone
Clerley Silveira, Conexxus
Chuck Young, Impact 21
Don Emery, CHS
Gabe Olives, Impact 21
Greg Jones, FIS
Jake Hoxha, 7-Eleven
Jeff Minard, Toshiba GCS
Kara Gunderson, CITGO
Kim Seufer, Conexxus
Konstantin Dolgushin, Petrosoft
Linda Toth, Conexxus
Manju Aradhya, Fiserv
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
March 11, 2021	1.3	Kim Seufer, Conexxus	- Final Release
February 9, 2021	Draft 1.3	Linda Toth, Conexxus	- Updates from SQA review: Define PAN at first usage, Added Conexxus webinar from December, Corrected typo.
November 21, 2020	Draft 1.3	Alan Thiemann, Conexxus	- Legal Review
October 26, 2020	Draft 1.3	Kim Seufer, Conexxus	- Updated based on comments from Mike Lindberg, CHS
September 15, 2020	Draft 1.3	Kim Seufer, Conexxus	- Updated with new resources
April 28, 2020	1.2	Kim Seufer, Conexxus	- Final Release
April 20, 2020	Draft 1.2	Kim Seufer, Conexxus	- Updated based on comments from the Public Comment period
March 19, 2020	Draft 1.2	Kim Seufer, Conexxus	- Updated based on comments from RFT vote
February 18, 2020	Draft 1.2	Alan Thiemann, Conexxus Kim Seufer, Conexxus	- Legal Review
January 2, 2020	Draft 1.2	Kim Seufer, Conexxus Sharon Scace, WEX	- Updated for V1.2
September 26, 2019	1.1	Kim Seufer, Conexxus	- Updated based on comments from Public Comment Period
August 15, 2019	1.1	Kim Seufer, Conexxus Sharon A. Scace, WEX	- Updated for V1.1
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

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, even if such liability was disclosed to Conexxus or was foreseeable. Although Conexxus uses commercially reasonable best efforts to ensure this work product is free of any encumbrances from third-party intellectual property rights (IPR), it cannot guarantee that such IPR does not exist now or in the future. Conexxus further notifies each user of this standard that its individual method of implementation may result in infringement of the IPR of others. Accordingly, each user is encouraged to seek legal advice from competent counsel to carefully review its implementation of this standard and obtain appropriate licenses where needed.

Table of Contents

1 Introduction

1.1 New in Version 1.3

This is the fourth version of this white paper. The new or updated entries include *NEW* or *UPDATE* at the start to help you find those quickly if you have been using Version 1.2:

- Roadmap to EMV;
- Debunking EMV Myths;
- EMV: A Focus on 3rd Party Retrofit Kits
- Contactless Operating Mode Requirements Clarifications;
- U.S. Automated Fuel Dispenser Chip Fallback Transaction Process Best Practices;
- Options for Reducing Level 3 EMV Certification Time for Retailer Systems Using Electronic Payment Servers;
- EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community;
- EMV 3-D Secure;
- #213 EMV: Ready or Not?;
- #230 EMV Upgrades Made Easier; and
- #242 Protect Card Payments at the Gas Pump.

1.2 Overview

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.

To understand the status of EMV deployment within the convenience and retailing fueling industry, please refer to the Conexxus EMV Surveys.

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, published in 2017, is also available from the U.S. Payments Forum.

Glossary of Standardized Terminology
This U.S. Payments 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 U.S. Payments 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 U.S. Payments 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 provide an overview of the drivers for the U.S. migration to EMV.

[A Guide to EMV Chip Technology]
This 2011 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.

__NEW__ [Roadmap to EMV]
This infographic outlines the steps and considerations to implementing EMV

__NEW__ [Debunking EMV Myths]
This March 2019 guide from the U.S. Payments Forum provides accurate information for all stakeholders communicating about contact and contactless chip technology, including card issuers, retailers and the media.

2.2 Where can I find more advanced information about EMV?

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

The 411 of EMV after October 1, 2015
This 2016 recording of a Conexxus webinar addresses an 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 the U.S. Payments 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 a U.S. Payments 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 provide 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 U.S Payments 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 are four resources to get you started:

- An EMV 101 for Gas Stations and Convenience Store Retailers page on the Conexxus website.
- A Petroleum Frequently Asked Questions document can be found on the U. S. Payments Forum website.
- A September 2017 webinar, titled 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.
- Moving Toward Outdoor EMV
  Published in August 2018, this webinar reviews what the liability shift is and how it affects you, what equipment you will need to invest in, what hardware, software and other upgrades are required, as well as installation and other considerations you will need to take into account.
- ***NEW*** EMV: A Focus on 3rd Party Retrofit Kits
  Recorded in December 2020, this webinar focuses on 3rd party retrofit kits for EMV enablement at Automated Fuel Dispensers (AFDs). An overview of the EMV liability roadmap, an update on transactions currently being processed as EMV at the AFDs and the case for adding contactless payment acceptance when doing EMV upgrades is presented. In addition, the options (along with their pros and cons) for upgrading to EMV at the AFDs, as well as ways to pay for those upgrades are explored.

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.
By comparison, 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 the 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 primary account number (PAN) and 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 Conexxus specification 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 U.S. Payments 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 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.

---

[1] Each major card brand (e.g., Visa, Mastercard) has a Common AID (CAID).

[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.

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

<CUSTOMER COPY>

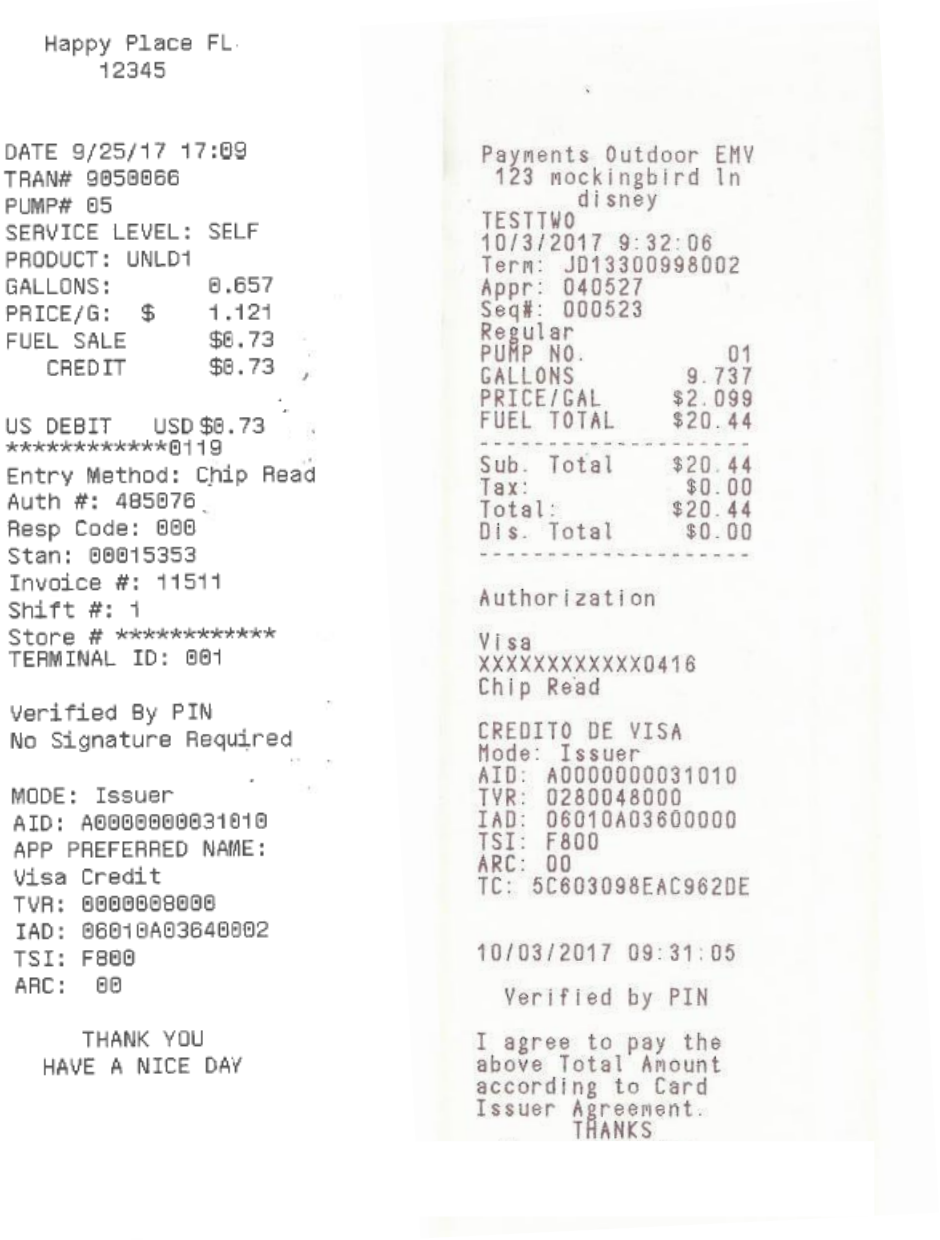
	Description	Qty	Amount
T	TEST A DEPT	1	5.00
	Subtotal		5.00
	Tax		1.25
	TOTAL		**6.25**
	DEBIT $		6.25

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

2.7.1 EMV Receipt Best Practices

EMV Receipt Best Practices

Published in June 2017 by the U.S. Payments Forum, this resource aims to clarify applicable recommendations and requirements regarding data elements most commonly found on printed receipts for chip-on-chip transactions, and focuses on EMV-related items.

Signature Best Practices

Published by the U.S. Payments Forum, this resource concerns the storage and capture of signatures at physical point-of-sale (POS) locations only, where goods and/or services are purchased at that location.

2.8 Troubleshooting

Merchant and Issuer Error Data Collection Forms

These forms can be used to assist issuers, issuer processors, merchants, acquirers, and acquiring processors with gathering information in a consistent way with sufficient details to help determine the source of the error. These forms can be used to identify data needed for troubleshooting and to communicate the data among payment processing partners. As described in the forms, a merchant is advised to work with its acquirers and an issuer advised to work with its processors on any transaction issues.

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, passed as part of the Dodd-Frank financial review law in 2010, requires that merchants be given 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

Published by the U.S. Payments Forum in February 2019, this document describes PIN Entry Bypass, as defined in Book 4 of the EMV specification. PIN Entry Bypass is used to allow cardholders to opt out of PIN entry, with a transaction indicator informing the issuer that the PIN was bypassed on a PIN-preferring card. The white paper discusses the transaction flow and the impact on issuers, merchants, and cardholders. The white paper also discusses alternative processes that may be deployed which allow selection of cardholder verification methods – merchant cardholder verification selection and issuer

preference for and cardholder selection of cardholder verification method. Merchant and issuer considerations are described for these alternative approaches.

U.S. Debit EMV Technical Proposal

Updated by the U.S. Payments Forum in July 2018, this document describes a technical framework developed to address the fundamental challenges faced by the U.S. debit payments industry: how to implement EMV for debit cards with the flexibility to meet current compliance guidelines established by the Federal Reserve Board and identify some flexible procedures should rules change over time. The solution provides an approach for the debit card processing scenarios in use today, so that debit industry organizations can continue chip implementation with confidence. In July 2018, clarifications were added to address consumer application selection.

3.2 Contactless EMV Implementations

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

NEW Contactless Operating Mode Requirements Clarifications

This U.S. Payments Forum white paper, published in February 2020, provides a resource to help merchants, issuers, and acquirers understand the contactless operating mode rules set by each of the payment networks.

The white paper provides:

- An overview of contactless EMV and contactless MSD technologies; and
- Tables with a summary of each payment network's current contactless requirements for issuing contactless cards and devices and accepting contactless payments.

Contactless POS Experience Best Practices Webinar

This webinar, hosted by the U.S. Payments Forum in October 2019, discusses best practices for consumer communications at the POS; consumer transaction prompting and flow, and cashier training.

Consumer Experience at the Contactless Point-of-Sale,

Published by the U.S. Payments Forum in June 2019, this document discusses common contactless POS challenges and best practices including:

- Communicating to consumers that a merchant accepts contactless payments through clear and consistent signage;
- Prompting consumers when and where to tap during the transaction;

- Familiarizing cashiers with how to properly execute a contactless transaction based on the merchant's implementation and to help consumers as they make transactions; and
- Creating a seamless consumer transaction flow with clear communication that a consumer's card was read and whether the transaction was approved or declined.

U.S. Payments Forum Contactless Resources: Implementation Considerations and Clarifications

Published by the U.S. Payments Forum, this document provides recently-published resources that provide guidance when implementing contactless payments in the U.S. learned from a contactless survey conducted among Forum members.

Mobile and Contactless Payments Requirements and Interactions

Published in February 2018 by the U.S. Payments Forum, the document describe how mobile and contactless payments requirements are collected from mobile/contactless payments ecosystem stakeholders. The intent is to garner cross-industry understanding of mobile and contactless payments requirements and best practices and encourage standardization to meet common requirements. The white paper uses a broad definition of "mobile and contactless payments" to mean all non-contact payment approaches that facilitate convenient, fast, and secure payment transactions for consumers. The scope is, however, limited to mobile payments with POS interactions (in-app or mobile-based browser payment are in scope if they are used at the POS); e-commerce transactions are not included.

Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions

Published in January 2018 by the U.S. Payments Forum, this document provides information about and guidance for stakeholders regarding the rapidly changing mobile and digital wallet landscape. The white paper describes five wallet models (device-centric mobile proximity, device-centric mobile in-app, card-not-present card-on-file, QR code, and digital checkout), and typical wallet specifications, including interaction methods, credential storage, and tokenization.

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. Since 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.

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 to understanding those requirements:

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 type 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 U.S. Payments Forum guide outlines potential causes of fallback transactions and actions that can be taken to address the problem.

NEW U.S. Automated Fuel Dispenser Chip Fallback Transaction Process Best Practices

This June 2020 white paper by the U.S. Payments Forum provides essential guidance on options for supporting fallback transactions in the petroleum environment. The white paper defines fallback and covers processing magnetic stripe transactions for card programs that are not supported on the contact EMV interface of automatic fuel dispenser terminals.

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 information:

- 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 U.S. Payments 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: (1) EMV offline authorization; (2) deferred authorization of an EMV card transaction; and (3) 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 requirements. EMV does not encrypt cardholder data. Existing security measures, including encryption and tokenization, may be used with 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 information may be 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 applicable, 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:

__UPDATE__ Options for Reducing Level 3 EMV Certification Time for Retailer Systems Using Electronic Payment Servers

Published by the U.S. Payments Forum in May 2020, this white paper discusses solutions to help reduce the implementation time and effort required for the automatic fuel dispenser (AFD) community to meet the April 2021 fraud liability shift deadline. The white paper documents the "Redundancy Reduction Approach (RRA)" – an approach that may reduce the number of formal Level 3 (L3) certifications required, reduce time lags when a solution is being certified, and reduce wait time between submission, review, and response.

EMV Level 3 Contactless Certification Recommended Solutions to Reduce Deployment Time

Published in July 2019, this document identifies possible testing and certification challenges to implementation and deployment of Level 3 (L3) certified contactless implementations for merchants.

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

This 2017 white paper published by the U.S. Payments 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 provides 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. Use cases are included for:

- ATMs;
- Terminals, including semi-integrated and standalone;
- Acquirer processor platforms;
- Value-added resellers (VARs);
- Gateways; and
- Unattended and automated fuel dispensers.

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 integration testing may be handled by a solution provider. Note that this workshop 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.

Chargebacks 101: The Basics

This Conexxus webinar, from December 2018, focuses on a high-level overview of the chargeback process. It touches on why chargebacks occur, including the most common reasons for chargebacks, as well as fraudulent chargebacks. Further, the discussion goes into how to respond to chargebacks and how to prevail in your representments. It also takes a broad look at the changes to the chargeback environment and the recent rule change on signatures.

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 are not 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.

6.3 Fraud Considerations

Understanding Fraud Liability for EMV Contact and Contactless Transactions in the U.S.

Published in February 2019 by the U.S. Payments Forum, this document provides information collected from certain payment networks to help payment industry participants better understand the corresponding network's policies. This document includes details for each of the participating networks regarding their respective liability shifts for counterfeit and lost-or-stolen fraud, for POS devices, ATMs, and AFDs. The liability policies documented in the white paper were developed by the payment networks independently and provided to the Forum to summarize the policies for industry stakeholders. The white paper also includes information on technical fallback and manual key-entered transactions, cross-border transactions, mobile transactions, and contactless transactions.

True Costs of Fraud

Published in November 2018, by the U.S. Payments Forum, this document highlights many of the forms fraud takes and the effects it has on the various stakeholders, providing insights from different perspectives. The white paper presents three example case studies from different stakeholder perspectives to illustrate the cost of fraud. The consumer, the card issuer, and the merchant were selected to highlight as stakeholders because they experience the most pain points in mitigating fraud risk and the most measurable losses when calculating the cost of fraud.

6.4 Security Improvements

NEW EMV 3-D Secure

EMV 3-D Secure provides a risk-based model for customer authentication with a significantly improved customer experience compared to previous 3DS versions. It also extends capabilities to mobile transactions in addition to web-based (e-commerce) transactions. The white paper will give merchants and issuers a better understanding of what EMV 3DS is and how it can help reduce fraud in the payments ecosystem.

Published in March 2020, this white paper published by the U.S. Payments Forum provides:

- A timeline on the development of the 3DS protocol and differentiates between previous and current versions of the protocol;
- Explains the benefits of EMV 3DS;
- Defines terminology commonly associated with EMV 3DS;
- Discusses the latest improvements and attributes of the 3DS protocol, including enhancing the customer experience, providing universal device support, allowing greater data sharing, and supporting added elements to meet regulations for strong customer authentication (currently rolling out in the EU, but similar requirements are likely to be imposed in the future in the U.S.); and
- Outlines the transaction flow with EMV 3DS.

EMV 3-D Secure Data Elements Webinar

Published in February 2019, this webinar provides an overview of EMV 3DS and presented detail about the new EMV 3DS data elements to provide an educational overview for merchants, issuers, and other payments industry stakeholders.

6.5 Tokenization

EMV Payment Tokenization Primer and Lessons Learned

Published in June 2019, this white paper focuses on the current state of EMV payment tokenization, providing the reader with an understanding of payment tokenization, the payment scenarios in which tokenization can be used, and the services that are commonly used in payment tokenization.

7 Other Considerations

7.1 ATMs

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

Implementing EMV at the ATM Webinar

This webinar covers the following topics to assist the ATM community as they make the transition to chip.

EMV Troubleshooting Guide for ATM Owners and Operators

This white paper, published in 2017 by the U.S. Payments Forum, provides recommendations to help ATM owners/operators prevent some common transaction problems, and offers suggestions for troubleshooting problems when they do occur.

Implementing EMV at the ATM
This 2015 U.S. Payments 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 U.S. Payments 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. Use the search function to location relevant documents.

7.2 Unattended Payment Terminals (Non-AFD)

If your site includes unattended payment terminals (i.e., not coin-operated) 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 U.S. Payments 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. Use the search function to locate information on EMV.

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 these types of CNP transactions, the following resources provide information and potential ways to mitigate CNP fraud:

CNP Fraud around the World

Published in March 2017, this white paper reviews the experiences and lessons learned from other countries that have a similar landscape to the U.S. in order to provide a foundation for the U.S. payments industry to build out layered, effective, and systematic mitigation strategies to assist in the reduction of CNP fraud.

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud
This 2016 U.S. Payments 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 Risks of Not Upgrading

Beginning in April 2021, fraud liability will shift to merchants when it occurs at gas pumps that are not EMV or chip card enabled. If you are still figuring out how to make the change, you are not alone. If you do not upgrade to EMV, though, you risk losing money through increased chargebacks. Even worse, failure to upgrade could cause serious harm to your business or even put you out of business. The following resources detail some of the risks to not being EMV compliant by April 2021:

__NEW__ #213 EMV: Ready or Not

This podcast episode of Convenience Matters, hosted by representatives from NACS and Conexxus in February 2020, details why ignoring the October 2020 deadline to accept chip cards at the gas pump could be a costly mistake. The same issues apply now that the deadline has been moved to April 2021.

EMV: Can You Afford NOT to Upgrade

This recorded session from the 2019 NACS Show, is intended to arm merchants with vital information on EMV, including industry preparedness, to assess what the costs and risks will be if the EMV deadline is ignored. In addition, it provides a case study of how a

35-store multi-branded retailer successfully implemented outdoor EMV with the help of multiple vendors in order to limit liability and manpower concerns as the deadline approaches.

Are You Ready for Oct 1, 2020? Part 1: EMV Fundamentals and the Risk of Not Upgrading

This webinar is Part 1 of a series hosted by Conexxus in late 2019. Part 1 explores the basics of contact and contactless EMV for the c-store industry, explains common terminology and discusses work underway to streamline certification. In addition, it discusses the current state of the industry on EMV deployment, industry fraud, and trends, as well as fraud prevention techniques. It also provides tips for getting your own fraud numbers. Again, most of this information applies to the new April 2021 deadline.

Are You Ready for Oct 1, 2020? Part 2: Practical Considerations for Implementing Outdoor EMV

This webinar is Part 2 of a series hosted by Conexxus in late 2019. It covers practical considerations on EMV implementation at the dispenser, including replacements vs retrofit kit decisions, scheduling and installation, and technical requirements. As with Part 1, the information applies equally to the new April 2021 deadline.

9 Additional Resources

Resources available from the following organizations 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.

__NEW__ NACS: Convenience Matters Podcast Episodes

- #230 EMV Upgrades Made Easier
- #242 Protect Card Payments at the Gas Pump

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.

Canadian Card Technical Acceptance

This resource provides guidance and clarification for merchants, acquirers, point-of-sale (POS) terminal vendors, and POS solution integrators on application selection logic used by U.S. POS terminals to avoid certain interoperability issues when processing Canadian cards. It also proposes optional use of "Preferred AID Logic" for debit co-badged cards on U.S. POS terminals, where guidance for a preferred AID has been provided by all applicable payment networks. The solution outlined in this document is payment network agnostic and includes possible adjustments to the Preferred AID selection intended to accommodate the possibility of changes in issuer business arrangements.

Dover Fueling Solutions Resources for EMV Implementation

Dover Fueling Solutions published three white papers related to enabling EMV preparing for a site assessment, and how the 2020 liability shift has exposed certain vulnerabilities.

Gilbarco Veeder-Root EMV Migration Guide

Gilbarco Veeder-Root published a webpage that provides an EMV FAQ. It also links to the Gilbarco Veeder-Root EMV Migration Guide.

Invenco Open Guide to EMV

This guide has been developed to help everyone understand the October 2020 shift to outdoor EMV. It is written in easy to understand language on the following topics:

- How to cost-effectively transition to an EMV Outdoor Payment Terminal (OPT) while saving on installation time and reducing risk factors;
- What you should look for in an EMV OPT; and
- How to future-proof your EMV investment.

NCR Resources for EMV Implementation

NCR's website provides several resources to prepare merchants for their EMV implementations. The site contains videos regarding what to consider while planning your EMV project and tips for getting your customers ready for EMV. There is also an e-book available titled "Assessing Your October 2020 EMV Risk."

Verifone Resources for EMV Implementation

Verifone published a webpage that gives a brief overview of what EMV is. It also links to the Verifone EMV Handbook.