Petroleum Industry: EMV Frequently Asked Questions

Version 1.0

September 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: transaction-speed@uspaymentsforum.org.

Table of Contents

1. Introduction

Like most brick and mortar retailers, the petroleum industry has been busy preparing for the acceptance of EMV payment cards. Developing, testing, and deploying software for petroleum-specific point-of-sale (POS) systems is complex and a long process. The introduction of EMV cards impact several components related to retail petroleum payment processing, including POS, payment servers, indoor payment terminals, forecourt controllers, fuel dispensers, and the special purpose acquirer systems that handle petroleum-specific payment types. The nature of these payment components creates inherently more complex development, testing, and certification efforts for petroleum retailers. Because of this complexity, it was necessary for the petroleum industry to await the completed credit and debit specifications before finalizing their development and programming.

The purpose of this document is to provide a common, consistent understanding of EMV issues in the U.S. retail petroleum industry. The target audience includes retailers, technology vendors, payment networks, acquirers, and other stakeholders involved in the processing of payments from retail petroleum sites.

2. Frequently Asked Questions

The FAQs in this section were developed with input from various contributors within the petroleum industry such as merchants, POS vendors, fuel dispenser manufacturers, acquirers, processors, payment networks, and other industry stakeholders.

1. **What are the characteristics of the petroleum industry that complicate EMV implementation?**

There are several characteristics of retail petroleum payment processing that complicate EMV implementation. Some are listed below.

- *Outdoor payment. The majority of payment card fuel purchases in the U.S. occurs at the dispenser. This requires special purpose site systems that can communicate with outdoor payment terminals, card processors, dispenser hydraulics, and a variety of other industry-specific site devices, some of which (e.g., tank monitors) are required for legal and regulatory compliance.*
- *Pre-authorization. The outdoor and indoor pre-authorization messages must be processed before the sale amount is known. The amount in these pre-authorization request messages can be a specific fixed dollar amount (e.g., $50), an amount specified by the payment network (e.g., $1), or a preconfigured limit that can vary by site and card type.*
- *Partial authorization. Fuel retailers may get authorization responses that indicate the full requested amount is not available, and the transaction has been approved for a lesser amount. Certain payment networks require the site systems to allow the consumer to dispense up to the approved dollar amount.*
- *Fleet cards. These are special purpose payment cards for vehicle fleet operators that collect additional information with each purchase through both the pre-authorization and settlement transactions. Collecting this additional information and transmitting it to the fleet card issuer require processing hosts that can handle the special requirements of fleet issuers and route the information to the correct fleet issuer. To complicate this further, each fleet card issuer has different specifications.*
- *Availability of certified technicians. Service activities on dispenser electronic components, including installing EMV-capable dispenser card terminals and upgrading electrical or data wiring above the dispenser junction box, may require technicians that have been certified by the automated fuel dispenser (AFD) manufacturers and/or POS vendors. The recommendation is to check the requirement with the respective merchants' POS and AFD providers.*
- *Full service locations. At sites in New Jersey and Oregon, fuel can only be dispensed by an attendant. For outdoor transactions, the consumer hands the card to the attendant and the attendant performs all terminal interactions. This will present a challenge for any PIN-preferring cards, as the PIN pad is located at the dispenser.*
- *Single POS/payment server for indoor and outdoor payment terminals. Most retail petroleum sites have a single payment server or POS system that handles both indoor and outdoor purchases. These single payment servers also have to integrate with indoor and outdoor terminals that may be from different terminal suppliers.*

- *Complex channels of trade. Very few retail petroleum sites are owned and operated by the oil company that supplies the fuel. The result is that payment components at sites may be owned by the oil brand, specified by the oil brand but owned by the site operator, or selected by the site. This creates complex, multivendor environments at many locations.*

2. What changes will petroleum retailers need to make for EMV?

The components at a retail petroleum site that will need to be replaced or upgraded to support EMV transactions include:

- *Site payment application and processor connection. This is on the critical path for all petroleum retailers: their site payment application must be updated to one that can handle EMV payment cards, standard magnetic stripe cards, fleet cards and all of the associated message specifications.*
- *EMV compliant indoor terminals/PIN pads.*
- *EMV compliant outdoor terminals. These may be from a different supplier than the indoor terminals/PIN pads.*
- *Communications between the forecourt devices and the payment server inside the store. Existing magnetic stripe outdoor terminals communicate with in-store components using very old low-speed communication protocols. The longer EMV messages, legacy protocol, optional functionality (e.g., multimedia) and more frequent terminal-payment application interactions most likely will require upgrading the communication speed between the dispenser island and the store.*
- *Terminal management systems. EMV terminals contain more logic than magnetic stripe reading PIN pads. It is highly recommended that more sophisticated support and remote management systems be used for keeping this logic current.*

3. How will debit card processing be supported when implementing EMV?

The U.S. Payments Forum has developed a standard approach to debit processing in the U.S. Terminal manufacturers, payment application developers, and acquirers have participated in the definition process and have implemented solutions that process debit cards in accordance with EMVCo specifications and debit network requirements while supporting the U.S. Durbin Amendment mandates. Contact the acquirers or the oil brand for the specific debit processing options they support in their EMV solution.

For additional details, please refer to the U.S. Payments Forum "U.S. Debit EMV Technical Proposal" white paper at http://www.emv-connection.com/u-s-debit-emv-technical-proposal/.

4. What is PIN bypass, and what are the issues with PIN bypass on the forecourt?

PIN Entry Bypass, commonly referred to as PIN bypass, is a terminal function in an EMV environment. PIN bypass may be optional or required based on specific payment network or merchant requirements and may be invoked when all of the following occur:

- *The CVM list of the selected AID has PIN as the preferred cardholder verification method (CVM) and the terminal supports PIN, and*
- *The terminal prompts the cardholder for a PIN, and*

- *The **cardholder** desires to select an option on the terminal that skips PIN entry*

PIN bypass can be configured in any terminal, inside or outside (if supported by the terminal manufacturer); however, the merchant may assume additional risk for certain transactions and incur higher processing costs.

For additional information please review the U.S. Payments Forum "PIN Bypass in the U.S. Market" white paper at http://www.emv-connection.com/pin-bypass-in-the-u-s-market/.

Refer to individual payment network guidelines for the U.S. regarding terminal requirements.

5. **Is the prompt for debit/credit required?**

Ultimately, this is a merchant decision. Some merchants have asked their POS vendors to keep functionality and implementation for EMV the same as magnetic stripe, but the terminal may have to support use of the "Credit"/"Debit" prompt instead of the application label or application preferred name displayed in standard EMV processing. The merchant may support an implementation with the same debit/credit choice as today (as long as provided by their supplier), including the option to avoid entering a PIN.

The payment networks indicate that there is no need to support the credit and debit button as the U.S. common debit AID solution will allow merchants to determine routing on debit cards through other means, specific to each network. Contact your acquiring processor/oil brand to confirm your selected approach is compliant as payment networks may have different approaches.

Issuers will determine if they want to support multi-account chip cards (credit and debit on the same card) in the future. For multi-account cards, the standard EMV application selection process will determine the display at the POS and the choice must be presented to the customer.

The application identifier (AID) selection process may be used to choose the application for use in a transaction from a card product. The CVM list associated with the selected AID, in comparison to the CVMs supported on the terminal, will determine if the consumer is prompted for PIN.

> *See guidance from the payment networks on integrating the debit/credit choice with the debit processing as outlined in the U.S. Payments Forum debit white paper, http://www.emv-connection.com/u-s-debit-emv-technical-proposal/.*

Refer to the video presentation on "Implementing EMV in the U.S.: How the U.S. Common Debit AIDs Facilitate Debit Transaction Routing and Ensure Durbin Compliance," http://www.emv-connection.com/implementing-emv-in-the-u-s-how-the-u-s-common-debit-aids-facilitate-debit-transaction-routing-and-ensure-durbin-compliance/, for additional information.

6. How will EMV transactions be handled at a full-service station – especially with pay-at-the-pump transactions?

There is no difference in EMV processing requirements between full service and self-service. With support of online PIN, the PIN processing requirements are the same with magnetic stripe and EMV. However, the merchant/acquirer has to certify the EMV compliant PIN pad that will be used to support PIN entry. EMV should not impact PIN usage at EMV compliant self-service fuel pumps. Refer to each payment network's CVM requirements. The chargeback liability follows what is described in the U.S. Payments Forum "EMV Chargeback Best Practices" white paper at *http://www.emv-connection.com/emv-chargeback-best-practices. Any clarification should be provided directly by the payment networks as there are some differences among them.*

Note: Full service states of New Jersey and Oregon have laws that require fuel attendants to dispense fuel. Oregon has a few exceptions; however, most transactions in those states will still be handled by an attendant. In these states, the site-level operational processes may have to be modified to support the scenario where a PIN-preferring card is presented and the outdoor payment terminals are configured to support PIN entry.

7. **Will zip code verification be maintained?**

Payment networks will continue to support the address verification service (AVS) and acquirers and merchants should support AVS the same as today for existing fraud mitigation. With EMV cards, AVS will help reduce lost/stolen fraud for outdoor transactions.

8. **How will gift card activation occur?**

There is currently no indication that the payment networks' gift cards will migrate to EMV chip technology. Therefore, activation transactions will continue to be processed as they are in today's environment.

9. **Will offline PIN be incorporated into U.S. EMV chip migration?**

Offline PIN is a feature supported by the EMV standard and issuers have the option of including this CVM on the cards they issue.

Each merchant makes the decision which CVMs will be supported in their terminals and what the CVM priorities are. (Note: The issuer defines the priority of the CVMs on each particular card.) If offline PIN is a valid CVM on the card, and if the terminal is configured to allow offline PIN, the terminal must process these transactions in compliance with the EMV specifications and payment network rules. Merchants can choose to support PIN. Requirements for online PIN and offline PIN may vary by network. Statements from U.S. card issuers indicate that most are preferring online PIN over offline PIN.

For additional information please see the U.S. Payments Forum resource "Minimum EMV Chip Card and Terminal Requirements – U.S." at http://www.emv-connection.com/minimum-emv-chip-card-and-terminal-requirements-u-s/. This document focuses on the minimum card and terminal EMV requirements for the U.S. payment networks. Some issuers and merchants, as they evaluate their business needs, may consider added functionalities that are beyond each network's minimum requirements, such as offline PIN support and offline data authentication.

> *The U.S. Payments Forum U.S. debit white paper at http://www.emv-connection.com/u-s-debit-emv-technical-proposal/ includes information on the debit transaction flow with different CVMs.*

Your acquirer or oil brand will be able to confirm if a minimum configuration is suitable for your business.

Refer to each payment network's requirements for their U.S. minimum terminal configurations.

In addition, merchants should evaluate these functionalities against the expected volume of issuers that may support them, and issuers should evaluate these functionalities against the expected volume of merchants that may support them.

10. **There appears to be a conflict between the current Mastercard contactless specifications and fleet specifications; e.g., contactless EMV specifications do not support required fleet tags that are currently in contactless magnetic stripe transactions.**

    Mastercard recommends that fleet card issuers move to EMV fleet as the contactless data (Application Transaction Counter and Unpredictable Number) positions within the Issuer Discretionary Data will also utilize the same positions as the fleet prompts.

11. **Can or should petroleum merchants support stand-in processing of EMV transactions?**

    Stand-in processing of EMV transactions refers to transactions that are processed when the card terminal cannot communicate with the acquiring host.

    Authorizing transactions while the terminal is offline creates risk for the merchant. This risk needs to be weighed against the potential benefit.

    Merchants should be aware that payment network documentation that refers to "offline" processing is generally referring to chip-based offline processing, and not to general outage situations.

    During a communications outage, merchants have three choices on proceeding with transactions:

    1. *Enabling store and forward. It is highly recommended that merchants performing store and forward authorizations should settle within 24 hours of the transaction. Refer to each payment network's guidelines on processing authorizations as deferred or delayed authorizations during outages or downtime for Automated Fuel Dispensers (AFDs). Also refer to the U.S. Payments Forum white paper, "Merchant Processing during Communications Disruptions," at http://www.emv-connection.com/merchant-processing-during-communications-disruption/. Merchants receive authorization protection on any transaction that subsequently receives an online approval. Merchants will also receive liability shift protection on any authorization request that includes chip data.*
    2. *Evoking chip-based offline approval processing. Some chip cards are able to support "offline approvals" without online access. Chip-based offline approvals can offer authorization and liability protection. However, offline approvals are not supported by most U.S.-issued cards which may accept the transaction but with no chargeback protection. Additional functionality is required to support offline approvals. This functionality can be implemented at the same time online support is implemented or can be implemented separately. Offline processing in some cases may require support for offline PIN which is described on question 9 above. This approach is not supported by magnetic-stripe-only cards.*
    3. *Enabling Forced Authorization. This approach involves "approving" transactions based solely on merchant parameters. While this is a relatively simple approach, the merchant is exposed to "No Authorization" chargebacks on all transactions cleared without authorization from the issuer.*

12. **How are fallback transactions supported?**

    A fallback transaction normally occurs when a chip card, presented at a chip terminal, cannot be read due to a technical issue with the chip or terminal reader which results in the technology "falling back" to process the transaction as a magnetic stripe transaction. This situation is not expected to occur frequently since the chips on the cards rarely fail. Due to being outside in the elements, AFD card readers may be more susceptible to problems which can lead to elevated fallback transactions.

In some situations, a fraudster may create a counterfeit card with an intentionally damaged chip in order to invoke this scenario; issuers and payment networks can detect high levels of fallback and may increase the cost to the merchant if excessive fallback transactions are presented.

For this reason, fallback transactions are deemed risky by the payments industry. Since the issuer holds liability on fallback transactions, they may choose to decline them when they are sent for authorization.

Refer to the U.S. Payments Forum "EMV Implementation Guidance: Fallback Transactions" at http://www.uspaymentsforum.org/emv-implementation-guidance-fallback-transactions/, for additional information.

13. How will the final value of the transaction be processed when there is a change in value (above or below) after the transaction was pre-authorized? Examples are:

- ✓ **More fuel purchased than was pre-authorized**
- ✓ **Card-based discounts – when an EMV payment card triggers a discount**
- ✓ **Dual-application cards – loyalty and payment in the same card may reduce the value of the transaction**

The value in Tag 9F02 (cryptogram amount) is used for cryptogram validation and should be transmitted to the issuer unaltered. The cryptogram amount may not match the transaction (authorized) amount in field 4 and the merchant should not compare two values or change the cryptogram amount to match the field 4 amount.

The same rules for changes between the authorized (field 4) and final transaction value apply in both the EMV contact, EMV contactless, and magnetic stripe scenarios.

14. How will "No Cardholder Verification Method" (No CVM) transactions be handled?

a) *In-Store and AFD*

Transactions can be processed as No CVM transactions if No CVM is the highest CVM supported by both the terminal and card.

Some merchants supporting No CVM transactions typically support multiple kernel configurations. In order to invoke No CVM processing, merchants change the terminal capabilities to match a kernel configuration that supports No CVM as the only available CVM option.

- ✓ *The use of multiple kernel configurations creates an environment that requires two or more EMV certifications – one for each kernel configuration. However, requiring a minimum of two kernel configurations and associated certifications increases merchant implementation timelines due to the additional certification requirements.*

b) AFD

AFDs typically do not support signature as a CVM; hence, presenting a card that supports only signature and No CVM to an AFD may result in No CVM being the selected CVM for use in that transaction.

c) *In-Store*

Merchants supporting multiple kernel configurations typically use the amount of the transaction to determine which kernel configuration to use for a transaction. They use a configuration supporting all CVMs for all transactions above the set limit and present the No CVM only *configuration for transactions below the limit; this is referred to generally as "small ticket programs." Merchants and payment networks have devised transaction processing methods that use No CVM to eliminate cardholder verification in the small ticket programs. The goal of these small ticket programs is to provide faster checkout in highly time sensitive consumer purchase scenarios including retail petroleum.*

Alternatively, if the transaction is less than the configured No CVM amount, and if the returned CVM result will only be signature or No CVM, the POS could simply not print receipts or collect signatures while indicating the POS collected a signature in the host response. In order to accomplish this, the terminal must be configured to not support PIN entry. This implementation would streamline the certification process and would be largely identical to what the merchant does for magnetic stripe/signature today. This alternate approach does require more care in making sure that indicators are suppressed as needed.

This approach could have lost/stolen fraud liability shift implications. CVM requirements, and associated liability exposures, vary by payment network and should be verified with supported payment networks.

For additional information, see the U.S. Payments Forum "Minimum EMV Chip Card and Terminal Requirements – U.S." resource at http://www.emv-connection.com/minimum-emv-chip-card-and-terminal-requirements-u-s/.

15. **How does point-to-point encryption (P2PE) and end-to-end encryption (E2EE) fit in the EMV landscape? The major acquirers now have solutions aimed at petroleum merchants.**

The decision to implement P2PE and/or E2EE is separate from the migration to EMV. There are multiple encryption approaches emerging for petroleum merchants, and the new EMV-capable payment components have added more encryption capabilities.

Encryption approaches can impact the payment application's ability to process the discretionary data required for fleet card transactions. This needs to be discussed with the individual P2PE and/or E2EE solution providers.

The requirements for E2EE options that stop at the processor level are determined by the processor. Contact your terminal provider and acquiring processor/oil brand for more details on these.

However, P2PE may impact both EMV and magnetic stripe implementations if prompt information is carried only in the magnetic stripe or chip-based magnetic stripe equivalent, and this data is included in the encryption process. P2PE providers may be able to extract the prompt information before encryption. Merchants should check with their acquiring processor/oil brand and/or P2PE provider.

Note: the Conexxus fleet tag proposal will include a tag where the prompt information and a tag where purchase restriction information can be placed, without being encrypted. (See www.conexxus.org.)

The PCI Security Standards Council has also clarified the impact of encryption on PCI certification requirements. For additional information, see PCI Point-to-Point Encryption (P2PE) Solutions, PCI Security Standards Council, https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

16. **Do the payment networks have recommendations regarding how encryption is implemented?**

    Encryption can impact some payment networks, for example, by blocking access to product code restrictions and prompt information in a fleet issuer discretionary data. This needs to be discussed with the individual payment solution provider or the oil brand.

17. **What are future EMV enhancements that will need to be supported by the petroleum industry?**

    Future EMV enhancements will be applicable to all retail verticals. Payment networks and debit networks issue additional information from time to time via releases and bulletins. Payment networks will share any new requirements via their standard communication processes with the acquirers, oil brands and vendors. Refer to each payment network for more details.

18. **Do fleet cards plan to support EMV at some point?**

    Fleet card issuers are not required to migrate to EMV; however, some have announced plans to do so. Any EMV fleet card must comply with relevant EMVCo standards and payment network specifications.

    Fleet issuers have multiple options. They can continue to issue magnetic stripe cards; they can issue EMV cards that support fleet requirements using magnetic stripe equivalent data; or they can add EMV data tags and enhanced functionality to EMV cards.

    Refer to each fleet card payment network for more details on their plans and requirements.

    Conexxus is drafting a standard for fleet card tags. Conexxus is allowing non-members to participate in these discussions, and will share the white paper once it is released.

    Fleet card implementation is an area where changes are likely to occur, and retailers and technology vendors should stay aware of these efforts.

3. Retail Petroleum Payment Glossary

Term	Definition
AVS	Address Verification Service. A fraud prevention technique that requires consumers to enter their billing zip code when making a purchase.
Channels of Trade (COT)	Operating models for the retail sites: • COCO - Company Owned Company Operated • CODO - Company Owned Dealer Operated • COFO - Company Owned Franchisee Operated • DODO - Dealer Owner Dealer Operated • DOFO - Dealer Owned Franchisee Operated
Chargeback	If a credit card sale is rejected before or after settlement, and it is subsequently determined that the merchant is liable due to improper authorization, the sale is *charged back* to the merchant.
Conexxus	U.S.-based technology standards organization for the petroleum and convenience industries.
Consumer	Commonly used to refer to the actual motorists that purchase the fuel and/or merchandise.
Customer	Has multiple meanings in the industry, but at most major oil companies the customers are their channel of trade partners – the independent retailers who purchase fuel at wholesale and operate retail sites.
Dispenser	The hardware that allows fuel to be passed from the underground tank to the consumer. May also contain an Outdoor Payment Terminal (OPT).
EPS	Electronic Payment Server. Device/application at the retail site that handles payment processing logic. This may be external or internal to the POS or forecourt controller.
Fallback	A fallback transaction normally occurs when a chip card, presented at a chip terminal, cannot be read due to a technical issue with the chip which results in the technology “falling back” to a magnetic stripe transaction.
FCC	Forecourt Controller. The computer system that handles communications between the dispensers, the dispenser card terminals, and the POS and EPS.
FEP	Front-End (payment) Processor.
Fleet Card	A payment card issued to an operator of a fleet of vehicles. The fleet issuer provides a number of value-added services including tracking mileage and fuel consumption by vehicle.

Force Authorization Force Approval	A force authorization is one that is not carried out via electronic communication (e.g., no authorization is received). Rather, the merchant either contacts the call center by voice to obtain approval or authorizes the transaction without going online and accepts the risk. Then, the force authorization is added to the batch, along with the approval code provided by the call center, so that it can be settled along with electronic authorizations. Force authorizations may be used when an electronic authorization results in a referral message or when the electronic network is experiencing an interruption in service. Force authorizations with a call center approval ("voice authorization") are protected from "No Authorization" chargeback, but are not protected against "Liability Shift" chargebacks. Force authorizations without an approval code ("force settlement") are not protected against "No Authorization" chargebacks. As used in this document, force approval is when no authorization is obtained and the clearing is simply submitted without an authorization. The merchant "approves" the transaction with certain risk parameters, meaning the fuel gets dispensed.
Forecourt Controller	A hardware device or software module that integrates the overall fuel components including fuel dispensers, tank gauges, OPTs, to the indoor POS. The forecourt controller may be a separate piece of hardware or integrated with the POS.
Forecourt	The area where the fuel pumps are present. It is the area outside the sales room or the convenience store of a gas station where customers park their automobiles for filling fuel. It can either be manned or unmanned. Also referred to as the "fuel island."
Oil Brand	Major oil brand. Sells fuel to a customer or retailer with whom the major oil brand name is on the canopy of the forecourt. Most major oil brands are the Merchant of Record with the acquirer. In most cases, they require their customers/retailers to process payment cards through the acquirer contracted by the major oil brand. Therefore, the customer/retailer's payment card processing contractual relationship is not with the acquirer, but with the major oil brand.
OPT	Outdoor Payment Terminal. Card terminal that is built into the fuel dispenser. The terminal typically includes a card reader, PIN pad, printer, and display screen.
POS	Point of Sale system. This is the "cash register" that store personnel use to process a transaction. It will typically have a cashier display, a customer display, a keyboard or touch screen, a cash drawer, and connections to the card processing system and the forecourt controller.
Pre-authorization or Pre-auth	A payment card transaction in which sale approval is requested without knowing the amount of the sale. This is commonly used for payment transactions at the pump. A pre-auth must be completed with a completion transaction that has the actual sale details.
Referral	A denial of immediate authorization with additional action required. Some examples:

	• The result code for a card transaction started outside may instruct the consumer to “see cashier.” • Card transaction inside or outside may result in a “call for auth” message, and the cashier refers the sale by telephone to the card issuer's voice authorization system for possible approval.
Settlement	Reconciliation and payment of balances due. Two categories are: • Merchant settlement: The merchant or oil brand settles with the site operators each day for the card sales that the site has conducted. • The merchant also settles with the payment networks that will be receiving the payment from the consumers.
Stand-in Processing	A backup system that provides authorization services on behalf of an issuer when the issuer or its authorizing processor is unavailable.
Store and Forward	The ability of a site payment application to process cards offline when it is not able to communicate with the card authorization host. Store and forward processing is risky for the merchant due to the potential for fraud. It can also increase card processing costs for the merchant.
Zip Code Prompting	See AVS.

4. Conclusions

The petroleum industry transition to EMV acceptance is lengthy and complex. Further, the POS terminals will need to be upgraded, both for EMV acceptance inside the store, and for EMV acceptance at the fuel dispensers. EMV dispenser upgrades require either a retrofit kit or complete replacement depending on the age of the existing fuel dispensers.

Petroleum merchants should also refer to the U.S. Payments Forum "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," at http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community, for clarification and details on testing requirements specific to petroleum merchants. A few clarifications include:

- No need to retest the same previously **successfully** tested solution when implemented with a new merchant on the same processing platform if there have been no changes impacting chip processing
- More flexibility in testing and retesting terminals from the same terminal family
- No requirement for testing and retesting for most changes in payment products that do not affect the EMV payment transaction process
- No need to retest indoor implementations when testing outdoors, if indoor was previously successfully tested and there are no changes to the in-store payment application or the kernel, since it is typically a separate process flow.

5. References

EMV - U.S.

- ✓ *Payment Processing for Retail Petroleum Convenience:* https://www.conexxus.org/content/payment-processing-retail-petroleumconvenience
- ✓ *U.S. Debit Technical Proposal white paper:* http://www.emv-connection.com/u-s-debit-emv-technical-proposal/.
- ✓ *Minimum EMV Chip Card and Terminal Requirements white paper:* http://www.emv-connection.com/minimum-emv-chip-card-and-terminal-requirements-u-s/
- ✓ *PIN Bypass in the U.S. Market white paper:* http://www.emv-connection.com/pin-bypass-in-the-u-s-market/
- ✓ *Implementing EMV in the U.S.: How the U.S. Common Debit AIDs Facilitate Debit Transaction Routing and Ensure Durbin Compliance:* http://www.emv-connection.com/implementing-emv-in-the-u-s-how-the-u-s-common-debit-aids-facilitate-debit-transaction-routing-and-ensure-durbin-compliance/
- ✓ *EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community" white paper:* http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.
- ✓ *EMV Chargeback Best Practices white paper:* http://www.emv-connection.com/emv-chargeback-best-practices

American Express

- ✓ American Express technical specification web site, www.americanexpress.com/merchantspecs

Conexxus

- ✓ Conexxus web site: www.conexxus.org

Discover

- ✓ https://www.discovernetwork.com/en-us/business-resources/chip-cards-emv/ or, contact your assigned Discover representative.

U.S. Payments Forum

- ✓ U.S. Payments Forum web site, http://www.uspaymentsforum.org/
- ✓ EMV Connection web site, http://www.emv-connection.com
- ✓ Chip Education for VARs, ISVs and Merchants, http://www.emv-connection.com/chip-education-for-vars-isvs-and-merchants/

EMVCo

- ✓ EMVCo web site, http://www.emvco.com
- ✓ EMVCo Approvals and Certifications, http://www.emvco.com/approvals.aspx

Mastercard

✓ Mastercard Connect web site, https://www.mastercardconnect.com/

PCI Security Standards Council

✓ U.S. EMV VAR Qualification Program, https://www.pcisecuritystandards.org/approved_companies_providers/var_qualifications_program.php

Visa

✓ Visa Online web site for Visa clients, https://www.visaonline.com
✓ Visa Chip US, www.Visachip.com
✓ Visa Technology Partner web site for vendors, https://technologypartner.visa.com/
✓ Visa clients: Contact your Visa representative.

6. Publication Acknowledgements

This white paper was developed by the members of the U.S. Payments Forum Petroleum Working Committee to provide an educational resource for petroleum merchants and others with an interest in the petroleum industry.

Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The U.S. Payments Forum wishes to thank the Petroleum Working Committee members and the payment networks for their contributions to the white paper.

The following members participated in the development and review of the Petroleum FAQs:

- Alan Fong, American Express
- Ben Dominguez, Visa
- Bob Slimmer, BP Products NA
- Bradford Loewy, Dover Fueling Solutions
- Bruce Murray, B2 Payment Solutions
- Charl Botes, Mastercard
- Cindy Kohler, Visa
- Clint Cady, W. Capra Consulting Group
- Dennis Ahenkora, Gilbarco Veeder-Root
- Ed Collupy, W. Capra Consulting Group
- Eugene Wong, Chevron
- Jeanean Davis, First Data
- Jim DuBoyce, W. Capra Consulting Group
- Kara Gunderson, CITGO Petroleum Corp.
- Kara Kazazean, Walmart
- Kelly Andrus, Tesoro Refining and Marketing Company
- Kevin Emery, Discover Financial
- Khari Towns, Discover Financial
- Marc Cleven, Visa
- Mark Carl, EchoSat Communications Group
- Robert Slimmer, BP Products NA
- Sam Schieber, W. Capra Consulting Group
- Sharon Scace, Wex Inc.
- Simon Hurry, Visa
- Steven Bowles, Wayne Fueling Systems
- Steven Cole, Vantiv
- Terry Mahoney, W. Capra Consulting Group
- Thomas Rapkoch, Visa
- Tim Weston, Wayne Fueling Systems
- Todd Horinek, Phillips 66 Company
- Tomas Levi, Gilbarco Veeder-Root

7. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are expressly disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the specific approaches, payment networks and other factors as expressly described herein, and that applicable rules, requirements, configurations and transaction processes may impact or be impacted by the specific circumstances of a given implementation and related results and/or liabilities.

Additionally, note that specific payment networks and/or acquirers/processors determine their own respective rules, requirements, policies and procedures for transaction processing, liability and other matters, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with their respective payment networks, acquirers/processors, and appropriate professional and legal advisors regarding all aspects of implementation, including but not limited to applicable rules, requirements, policies and procedures.

Nothing in this document constitutes or should be construed to constitute an endorsement or recommendation of any particular approach, service or provider, and all implementation decisions and activities should be properly reviewed in light of applicable business needs, strategies, requirements, industry rules

All registered trademarks, trademarks, or service marks are the property of their respective owners.