PIN Bypass in the U.S. Market

Version 2.0

Date: June 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.

Table of Contents

1. Introduction

This document addresses the EMV function of PIN Entry Bypass, how it can be implemented in the U.S. market, other actions that may process transactions allowing selection of cardholder verification method (CVM), and how those actions differ from PIN Entry Bypass.

2. PIN Entry Bypass

PIN Entry Bypass is an optional function in a traditional EMV environment that may be invoked when the following occurs:

- The CVM list of the selected AID has PIN as the preferred CVM for the given transaction and the terminal has a Terminal Capability indicator supporting "PIN"
- The terminal prompts the cardholder for a PIN
- The cardholder does not enter the PIN and invokes this function

NOTE: PIN Entry Bypass only relates to contact chip transactions. It does not apply to contactless.

The document is intended for terminal vendors, POS system integrators, merchants, merchant acquirers and issuers to offer guidance and explanation.

This document discusses PIN Entry Bypass as defined by the global EMV specifications for both debit and credit. For specifics on application selection related to debit in the U.S. market, please refer to the U.S. Payments Forum (formerly the EMV Migration Forum) white paper, "U.S. Debit EMV Technical Proposal."[1]

2.1 PIN and PIN Entry Bypass in the United States

The United States is considered a "chip and choice" environment. This means that issuers are free to issue either PIN-preferring or signature-preferring cards implemented through the sequence of entries in the CVM List associated with the selected AID.

PIN Entry Bypass has historically been implemented in other markets on a temporary basis during a market-wide migration to PIN. Given the "chip and choice" philosophy in the U.S. market there is no general, mandated, or managed migration to the use of PIN and thus the availability of PIN Entry Bypass is not constrained to a specific timetable. Individual issuers may assess their own policies relating to the approval of transactions where a PIN Entry Bypass has been performed and indicated properly in the transaction. In addition, since the U.S. Common Debit AID is always PIN preferring, cardholders may choose to utilize PIN Entry Bypass to avoid PIN entry at a point-of-sale (POS). Issuers and merchants may wish to support PIN Entry Bypass indefinitely for all cardholders in order to accommodate this behavior,[2] while recognizing there are potential risk considerations which are addressed later in this paper.

Merchants are urged to discuss PIN Entry Bypass with their terminal vendors, acquirers, and acquirers with networks prior to implementation.

2.2 Card and POS Device Assumptions in the Document

For the purposes of a PIN Entry Bypass transaction as discussed in this document, the following are assumed:

[1] "U.S. Debit EMV Technical Proposal," http://www.emv-connection.com/u-s-debit-emv-technical-proposal/.

[2] See additional information in the U.S. Payments Forum white paper, "U.S. Debit EMV Technical Proposal."

1) The profile associated with the selected AID has a CVM List that is "PIN Preferring" (offline or online) for purchase at the POS.
2) The terminal supports an EMV/PCI qualified PIN Entry Device, capable of processing a PIN.
3) The cardholder is presented with a recognizable EMV PIN Entry Bypass function, where a cardholder presses a button on the terminal to trigger EMV kernel functionality to cancel all PIN CVMs, move to the next non-PIN CVM in the hierarchy, and indicate this event in the authorization request.
4) The terminal will implement Cardholder Verification as described in section 10.5 of Book 3 of the EMVCo specifications.
5) The issuer will have the ability to identify that PIN was bypassed by interrogating the bit settings in the Terminal Verification Results (Byte 3 Bit 4 in the TVR).

2.3 PIN Entry Bypass – EMVCo Definition

The following is the EMVCo defined process for PIN Entry Bypass in Book 4 section 6.3.4.3[3].

PIN Entry Bypass

If a PIN is required for entry as indicated in the card's CVM List, an attended terminal[4] with an operational PIN pad may have the capability to bypass PIN entry before or after several unsuccessful PIN tries.[5] If this occurs, the terminal:

- shall set the 'PIN entry required, PIN pad present, but PIN was not entered' bit (Byte 3 bit 4) in the TVR[6] to 1,
- shall not set the 'PIN Try Limit exceeded' bit in the TVR to 1,
- shall consider this CVM unsuccessful, and
- shall continue cardholder verification processing in accordance with the card's CVM List.

When PIN entry has been bypassed for one PIN-related CVM, it may be considered bypassed for any subsequent PIN-related CVM during the current transaction.

When any form of PIN is determined as the appropriate CVM for a given transaction, based on the capabilities of the terminal and the processing of the CVM List in the card, as well as the cardholder being prompted for PIN, PIN Entry Bypass may be offered.

How CVM processing completes depends on the content of the issuer-defined CVM List. CVM processing may terminate and be unsuccessful or an alternative CVM may be completed.

---

[3] EMV 4.3 Specifications, "Book 4 – Cardholder Attendant and Acquirer Interface Requirements," Section 6.3.4.3, http://www.emvco.com/specifications.aspx?id=223

[4] Note that the EMVCo specifications do not address PIN Entry Bypass at unattended terminals. Payment networks may have different requirements or may not allow PIN Entry Bypass on different types of unattended terminals. Merchants and acquirers are advised to contact the payment networks for further information.

[5] This prevents a genuine cardholder who does not remember the PIN from having to keep entering incorrect PINs until the PIN is blocked in order to continue with the transaction.

[6] Terminal Verification Results

At the Terminal Action Analysis stage of the transaction, the terminal will compare the results of tests performed during the transaction flow and as recorded in the TVR with the issuer IAC and acquirer TAC instructions encoded in the Issuer Action Codes (IACs) and Terminal Action Codes (TACs). Depending on the result of this analysis the transaction may be declined offline or may be passed online to the issuer.

If an online authorization is requested, the chip data (specifically, the TVR) will indicate that PIN Entry Bypass has been performed. This information, along with other chip-related data or other controls, can be used by the issuer to assess the risk of the transaction and make an appropriate authorization decision.

Figure 1 illustrates the basic EMV transaction process flow with PIN Entry Bypass after an AID is selected.

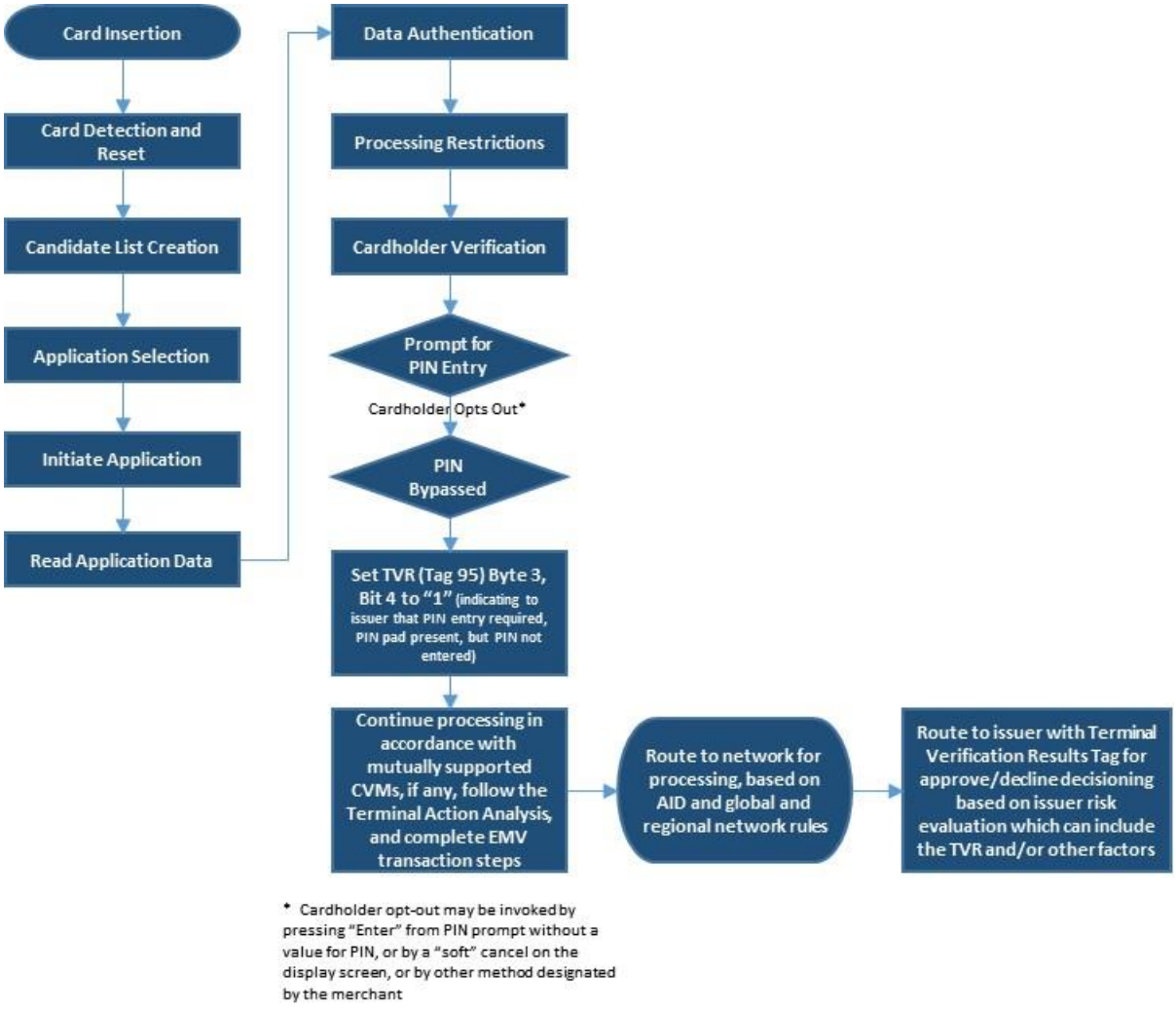

Figure 1. Generic PIN Entry Bypass for Credit and Debit Transactions

Although kernel support is required, functional control is from the POS application. Instead of managing PIN bypass availability dynamically, it can be set as a configuration, depending on how the POS application interfaces with the device and kernel. It can be configured to be turned on or off at an AID level if desired.

Note that selection of PIN Entry Bypass depends on the device and how the interaction between the POS application and the kernel is managed. It may be the manufacturer's interface application, or it may be a third party interface, or it may be the POS application that loads an EMV configuration file.

2.4 Impact to Stakeholders

2.4.1 Issuer Impact of PIN Entry Bypass

Historically, in cases where PIN Entry Bypass has been used, issuers have had time- or action-based parameters to facilitate the EMV PIN Entry Bypass process. In the U.S., individual issuers will likely choose their own approach according to their business requirements and view of the risk/customer service considerations. These approaches could include the following and are often paired with outreach to the cardholder:

- A grace period end date, at the cardholder level, after which the correct PIN has to be used or the transaction will be declined.
- Action-based parameters (other than an end date) which will result in a decline of the card's transaction if no PIN or an incorrect PIN is used. Those may include:
    - Once the correct PIN has been successfully used, PIN Entry Bypass is no longer permitted
    - Following some number of wrong attempts, PIN Entry Bypass is no longer permitted
- The adoption of a risk-scoring approach, similar to those used for other risk management activities, which takes into consideration items such as:
    - How long the account has been open
    - The dollar amount of the transaction
    - The geographic location of the transaction
    - The merchant category code (MCC) of the transaction
    - How consistently the PIN is bypassed
    - Criteria based upon the payment product type (e.g., consumer credit, commercial/corporate credit, traditional debit, reloadable prepaid, healthcare). *NOTE*: Issuers may want to consider impact of lost/stolen fraud migration to other cards or portfolios that are not PIN-preferring.

2.4.2 Merchant Impact of PIN Entry Bypass

PIN Entry Bypass is optional for merchants for credit and debit transactions.

NOTE: For debit transactions initiated through the U.S. Common Debit AID, the solutions for cardholder verification selection described in this document enable No CVM/signature transactions. Merchant implementation of PIN-only solutions would remove No CVM/signature as an option for the U.S. Common Debit AID. Merchants are advised to consult with their acquirers to understand network requirements.

The support of PIN Entry Bypass may enable transactions to be completed when otherwise a particular card transaction might be declined or alternative tender required (e.g., customer has forgotten their PIN). This may be particularly helpful during the migration and may be important for the merchant customer proposition, recognizing in the long-term, that issuers may include the fact that the PIN was bypassed in their authorization decisions.

2.4.3 Cardholder Impact of PIN Entry Bypass

POS devices will have various ways to bypass PIN. Merchants need to train their cashiers to assist cardholders with whatever method is implemented.

2.5 Implementation Consideration Note

If a debit transaction is processed without a PIN, then in order to help ensure a successful transaction:

I. The acquirer processor must select a network capable of supporting a No CVM/signature transaction; and
II. The network must route to the correct issuer/issuer processor platform.

3. Other Solutions for Selection of Cardholder Verification

As noted above, it is important to discuss alternative processes that may be deployed which also allow selection of cardholder verification methods.

In today's magnetic stripe card environment many U.S. POS systems either (a) do not prompt for PIN based on the value of the transaction, or (b) allow the cardholder to choose either signature or PIN verification methods on debit card transactions at the beginning of the transaction by selecting either "credit" (signature) or "debit" (PIN). If the cardholder selects "credit," they historically have not been prompted for a PIN.

The above scenarios "a" and "b" are discussed below in the context of an EMV-enabled environment.

3.1 Merchant Cardholder Verification Selection

There will continue to be scenarios where a PIN-preferring card, used at a PIN-enabled point-of-sale, will result in a transaction that proceeds without the cardholder being prompted for a PIN or any other form of CVM like signature, most often for low-value transactions.

The merchant selection use case enables the merchant to make the determination of whether or not to prompt the cardholder to enter a cardholder verification. Historically, the merchant will systemically make this decision based on the amount of the transaction, although amount does not necessarily need to be the deciding factor. In these situations, for transactions below the merchant's "No CVM Required" limit, the cardholder will not be prompted for a PIN or signature even if the card is PIN-preferring. This allows the merchant to reduce the cardholder's time in lane for low dollar transactions. For transactions above the limit, the cardholder will be prompted for PIN or signature and the transaction will proceed accordingly. Failure to capture a PIN over the network limit may result in a lost/stolen liability shift chargeback on PIN-preferring cards for networks that have a lost/stolen liability shift in place. Failure to capture a signature over the network limit may result in compliance action.

With merchant-selected no cardholder verification, the merchant may use a selectable kernel configuration to change the terminal configuration to influence the cardholder verification required, based on the attributes of the transaction at the time of the purchase. In this situation, some merchants may change the cardholder verification by suppressing support for PIN or signature, based on the transaction amount (for example, transactions under $50) or some other factor. This selectable kernel configuration approach allows terminals to dynamically invoke or initiate an approved EMV kernel configuration to support terminal capabilities on a per-transaction basis – for example, one in which the PIN pad is no longer enabled even if the PIN pad is physically present, thereby avoiding the prompting of a PIN for a given transaction.

The rules of a No CVM transaction may vary by network and, therefore, should be considered by the merchant as part of their overall EMV implementation strategy.

3.2 Issuer Preference for and Cardholder Selection of Cardholder Verification Method in the EMV Environment

This section reviews other scenarios for CVM selection in the U.S.

3.2.1 Debit/Credit Button for U.S.-Issued Debit Cards and CVM Choice

To maintain compatibility with magnetic stripe transactions, merchants may choose to continue the use of the debit/credit button on non-multifunded U.S.-issued debit cards. There are two options for how the debit/credit button may be implemented, once the list of AIDs on the card has been determined:

1. Selecting credit invokes the No CVM kernel configuration, and the U.S. Common AID is selected. This solution creates a situation under which the PIN pad is disabled and the transaction falls to the No CVM method. A signature may be captured if the transaction amount is over the No CVM limit. While this solution preserves merchant routing choice it has one drawback: this solution may result in lost/stolen liability on a PIN-preferring card, where the card network supports a lost/stolen liability shift. For networks that do not support a lost/stolen liability shift, failure to capture a signature over the network limit may result in compliance action.
2. Selecting credit invokes the global AID. Under this option, the global AID is presumed to be signature-preferring, and the issuer and cardholder are aware that the global AID is signature-preferring. As with the previous method there are drawbacks to this solution as well.
    - Selecting the global AID will limit routing choice to the global network on the card.
    - If the issuer and cardholder are not clear on the preferred CVM, the cardholder may not be provided with CVM choice. In other words, if the card is PIN-preferring on both AIDs, then clearly the cardholder will be prompted for PIN, and the transaction routing will still be limited to the global network on the card.

3.2.2 Scenario Requiring Cardholder Application Selection

There are specific cases where the cardholder may be required to select the application itself. In these and the other examples described below, CVM choice is driven by the issuer preference or by cardholder choice.

EMV is designed so that the issuer selects the CVM options for the card and the order of CVM preference during card personalization. Issuers may set CVMs independently by AID – either the same or different for each AID.

3.2.2.1 MULTI-ACCOUNT CARDS (U.S. OR INTERNATIONALLY ISSUED)

Regardless of whether the card is issued by a U.S. or international issuer, multi-funding account cards require cardholder application selection.

The EMVCo specification[7] recommends that if a card has multiple AIDs not linked to the same funding account, then the merchant terminal should display the AID labels on the screen for the cardholder to make the choice. The CVM in this case is largely driven by the CVM hierarchy as established by the issuer for the AID selected by the cardholder. Exceptions are low-value transactions as described in Section 3.1 above. Issuers need to educate cardholders on the CVM options for each AID. In the U.S., this method always applies in instances where the card contains multiple AIDs representing more than one funding account.

[7] EMV 4.3 Specifications, "Book 1 – Application Independent ICC to Terminal Interface Requirements," Section 12.4, step 4, http://www.emvco.com/specifications.aspx?id=223

Cards with multi-funding accounts: If any card has two or more AIDs that do not contain the same IIN and country code, the terminal should display the application labels or preferred application name set by the issuer for each unique AID on the card in order for the cardholder to select the payment method that they wish to enable (e.g., credit, debit, prepaid, small business).[8] Once the cardholder selects the AID, processing should proceed per standard EMV processing.

- If the card has a total of three AIDs, for example one for a credit account and two for a U.S.-issued debit account (global AID and U.S. Common AID), then the consumer may be prompted for the funding source; i.e., debit account or credit account. If the consumer chooses the debit account, then merchant preference of AID for routing will take place without further action by the consumer.
- Terminals (mainly unattended), that do not have a large enough screen and/or cardholder interface to display the multiple AIDs with different funding accounts, can select the AID with the highest priority established by the issuer.

3.3 Stakeholder Considerations

3.3.1 Issuer Considerations

Considerations for issuers are the initial set-up/hierarchy of cardholder verification methods, authorization decisions, and education. Unlike PIN Entry Bypass, where issuers receive notification that a PIN was prompted for but was bypassed by the cardholder, these other scenarios provide no distinct data to the issuer that is helpful in risk scoring. This is important because the issuers' approval decisions may impact the feasibility of one or more of the implementation options described.

Initial Set-up/Hierarchy of Cardholder Verification Methods and Liability Shift

When the merchant elects to process a transaction with no cardholder verification, the transaction is considered as one coming from a merchant terminal that has no PIN capability. Refer to the "Understanding the U.S. EMV Fraud Liability Shifts" white paper for information on potential impact on lost/stolen fraud liability.[9]

Education

Educating both cardholders and staff members (particularly those who interact directly with the cardholders) is one of the most important tasks when it comes to successfully implementing chip cards. Arguably, one of the most critical components of customer education is to ensure cardholders know to leave their card in the terminal (vs. swiping it) until the transaction is complete and, as importantly, understand that they need to take it out of the terminal at the end of the transaction. It will be important to recommend to all cardholders that they follow the screen prompts and that transaction flows will vary based on amount of transaction and merchant capability, as they do today.

[8] EMV 4.3 Specifications, "Book 1 – Application Independent ICC to Terminal Interface Requirements," Section 12.4, step 4, http://www.emvco.com/specifications.aspx?id=223

[9] "Understanding the U.S. EMV Fraud Liability Shifts," http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/

3.3.2 Merchant Considerations

Transaction Processing

Unlike PIN Entry Bypass, where merchants provide data to the issuers within the authorization request that a PIN was prompted for but was bypassed by the cardholder, these other scenarios do not provide this information to the issuer. This is important because the issuers' authorization decisions can be influenced by multiple factors, including but not limited to the presence of PIN Entry Bypass indicators as a result of cardholder choice.

If a debit transaction is processed without a PIN, then in order to ensure a successful transaction:

I. The acquirer processor must select a network capable of supporting a No CVM transaction.

II. The network must route to the correct issuer/issuer processor platform.

III. Debit with No CVM must be thoroughly tested and the acquirer must be capable of determining if the particular issuer is capable of handling No CVM.

Selectable Kernel Configurations

A terminal may use a selectable kernel configuration to enable merchant selection of no cardholder verification transactions, driven by amount (or other criteria) or alternatively enabling a debit/credit or similar function. In some cases, a transaction that was initiated as a No CVM transaction may be routed to a network that requires the capture of a signature if the transaction amount exceeds the chosen network's limits. In such cases, the terminal may prompt the cardholder for a signature at the conclusion of the transaction even though it originated as a No CVM transaction. For more information regarding U.S. debit AID selection, please refer to the U.S. Payments Forum white paper, "U.S. Debit EMV Technical Proposal."

4. Summary

The U.S. is a “chip and choice market,” with both signature-preferring and PIN-preferring cards and profiles. For PIN-preferring cards, some stakeholders may decide to process transactions without PIN entry, using PIN Entry Bypass or other options described in this white paper.

As described in this paper, PIN Entry Bypass is defined in Book 4 of the EMV specification and can be 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.

Given the chip and choice landscape of the U.S. market, issuers and others will need to factor support for the options described in this white paper into considerations regarding implementation, fraud management systems and fraud mitigation strategies.

Last, the method by which prompts are defined and presented to cardholders in an EMV-enabled environment may differ from those in a magnetic stripe environment.

In conclusion, all three methods of providing CVM choice have pros and cons:

1. EMV PIN Entry Bypass from the U.S. Common Debit AID supports merchant routing choice, but may result in issuer declines and lost sales.
2. Use of the selectable kernel configuration with selection of the U.S. Common Debit AID supports merchant routing choice, but may occassionally result in lost/stolen liability on PIN-preferring cards for networks supporting a lost/stolen liability shift.
3. Selection of the global AID will limit routing choice to the global network on the card, but eliminates the lost/stolen liability shift concern.

While considerations for all constituents have been outlined in this paper, it is highly recommended that issuers, acquirers and processors seek guidance from the payment networks with whom they connect, and that merchants speak to their merchant service provider before planning implementation.

5. Publication Acknowledgements

This white paper was developed by the U.S. Payments Forum to provide an educational resource on the EMV function of PIN Entry Bypass, how it can be implemented in the U.S. market, other actions that may process transactions allowing selection of cardholder verification method, and how those actions differ from PIN Entry Bypass.

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 thanks the project team members who led and contributed to the development of the white paper.

Trademark Notice

6. 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