FAQ EMV™

EMV Overview

What are the benefits of EMV cards?
A: Several factors are driving the U.S. card market to migrate to chip-based cards using the EMV specifications. EMV offers advantages for consumers, financial institutions and merchants and has captured the attention of the U.S. card market. Advantages include:

- **Improved security over cards that solely use a magnetic stripe.** Whereas a magnetic stripe card delivers the same static cardholder data to the terminal for every transaction, an EMV chip card and an EMV-capable terminal exchange unique data for each transaction using sophisticated cryptographic authentication technology. As a result, any transaction data that is stolen cannot be used to produce counterfeit card(s). Also, every EMV transaction authorization request includes additional data that allows the issuer to verify that the card used is genuine and that the transaction data has not been modified.

- **Worldwide interoperability, delivering an improved experience for international travelers and military personnel stationed abroad.** With most countries already migrated to EMV, consumers may increasingly find limited acceptance of magnetic stripe cards outside the United States., resulting in inconveniences at ATMs and POS devices.

- **Longer term, the adoption of EMV in the United States paves the way for financial institutions to offer mobile payments and mobile applications (apps) that support NFC (near field communication) technology.** NFC enables communication between apps on mobile devices, tablets and other consumer electronics when in proximity to an NFC capable terminal.

How does an EMV transaction work?
A: There is a fundamental difference between a magnetic stripe and EMV chip transaction. With a magnetic stripe card, the stripe stores data that is read by a terminal. The terminal reads the magnetic stripe and initiates an online credit, debit, or prepaid transaction. Subsequently, the transaction is routed to/through branded payment networks and/or various payment processors for authorization. The physical card and stripe no longer play a role in the transaction once the initial data is read.

An EMV chip and an EMV-capable terminal interact dynamically in real time using more sophisticated cryptographic authentication technology. During an EMV transaction, the chip is capable of processing information and actually determines some of the rules for the payment. The terminal helps enforce the rules set by the issuer. These rules can include defining the cardholder verification method, including PIN or signature, requiring online authorization or even authorizing a low-dollar transaction offline. It’s up to the issuing bank, in collaboration with their payment processor, to define which of these services is required for the current transaction via the rules placed on the chip.

Why are EMV credit and debit cards and EMV payment transactions more secure?
A: EMV secures the payment transaction with enhanced functionality in three areas:

- **Card authentication — protecting against counterfeit cards.** The card is authenticated during the payment transaction, protecting against counterfeit cards. Transactions require an authentic card validated either online by the issuer using a dynamic cryptogram or offline with the terminal using offline data authentication (usually referred to as SDA, DDA, or CDA). EMV transactions also create unique transaction data, so that any captured data cannot be used to execute new transactions.
• **Cardholder verification** – authenticating the cardholder and protecting against lost and stolen cards. Cardholder verification ensures that the person attempting to make the transaction is the person to whom the card belongs. EMV supports four cardholder verification methods (CVM): offline PIN, online PIN, signature, or no CVM. The issuer prioritizes CVMs based on the associated risk of the transaction (for example, no CVM is used for unattended devices where transaction amounts are typically quite low).

• **Transaction authorization** – using issuer-defined rules to authorize transactions. The transaction is authorized either online and offline. For an online authorization, transactions proceed as they do today in the United States with magnetic stripe cards. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction. In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized, without sending the transaction information to the issuer. Offline transactions are used when terminals do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications costs are high.

**How do EMV chip and PCI DSS work together?**

**A:** EMV chip has strong security features that have been proven to reduce counterfeit card fraud at card-present retail environments. The PCI Data Security Standard (PCI DSS) provides other complementary levels of security necessary when the cardholder information reaches the merchant’s system. The PCI DSS contains 12 key technical and operational requirements. Rather than focusing on a specific category of fraud, the PCI DSS seeks to protect cardholder and sensitive authentication data anywhere this data is present within the payment eco-system, thus limiting the availability of this data to fraudsters. When used together, EMV chip and PCI DSS can reduce fraud and enhance the security of the payments ecosystem.

**How does EMV address payments fraud?**

**A:** First, the EMV card includes a secure microprocessor chip that can store information securely and perform cryptographic processing during a payment transaction. EMV cards carry security credentials that are encoded by the card issuer at personalization. These credentials, or keys, are stored securely in the EMV card’s chip and are impervious to access by unauthorized parties. These credentials, therefore, help prevent card skimming and card cloning, two of the common ways magnetic stripe cards are compromised and used for fraudulent activity.

Second, when performing an EMV transaction, the card is authenticated as being genuine, the cardholder is verified, and the transaction includes dynamic data that is authorized online or offline, according to issuer-determined risk parameters. As described above, each of these transaction security features helps to prevent fraudulent transactions. Third, even if fraudsters are able to steal account data from chip transactions, this data cannot be used to create a fraudulent transaction in an EMV or magnetic stripe environment, since every EMV transaction carries dynamic data.

And lastly, EMV may also help to address card-not-present fraud with cardholders using their EMV cards and individual readers to authenticate Internet transactions.

**How does EMV work with online purchases?**

**A:** It’s important to acknowledge that the current EMV adoption plans will only reduce the potential for fraud during card present transactions and will not impact card-not-present fraud, which is of concern due to the growing use of e-commerce.
For card-not-present transactions, security enhancements continue to evolve and will likely include the use of tokens (pseudo card numbers that represent the card during a transaction) as an additional measure to further improve online payment security. The use of additional equipment/readers would provide a single, one-time password to validate the card-not-present purchase. These devices are currently in use in other countries.

Through the use of MasterCard’s Chip Authentication Program (CAP) and Visa’s Dynamic Passcode Authentication (DPA), the EMV smart card is used to authenticate the user and verify the cardholder’s PIN while offline. The cardholder inserts the card into a small handheld device that generates the one-time password and is displayed directly on the device. During the online transaction, the cardholder transmits this one-time password to the issuing bank, where it is verified using the EMV back-end authentication system. The card may also have an integrated ‘keyboard’ that creates the one-time password and displays it on a mini display embedded in the card. Both of these methods constitute two-factor authentication which includes something the user knows (e.g. PIN) and something the user has (e.g. smart card). It’s noted that handheld readers have been distributed to tens of millions of cardholders in Europe and Asia, but consumers have complained that it’s inconvenient to have a card reader in hand to do online transactions. Other forms of two-factor authentication are surfacing, such as mobile phone-based two-factor authentication and we’ll likely see other methods developed as technology advances.

These methods should be employed within the context of a broad, comprehensive risk management initiative that employs best practices, such as real-time transaction scoring, blocking of suspected fraudulent transactions, real-time case management and monitoring, and tracking and monitoring of fraud alerts on compromised cards.

**What are some of the roadblocks to EMV migration in the United States?**

**A:** The migration to EMV in the United States has been hindered in part by the difficulty of identifying a compelling business case. There’s significant investment associated with the move to EMV. While a traditional return on investment may be difficult to calculate, given the challenge of forecasting the resulting reduction in fraud, the industry now views these expenses as the cost of doing business in the payment card space.

Market readiness has also slowed EMV adoption. Given the size of the U.S. card market, a mass migration to EMV will require implementation processes that are scalable, defined and repeatable with reasonable deployment timelines and costs.

Developing a debit solution that is viable and supports the requirements of the Durbin Amendment (Regulation II) has also hindered EMV migration. Recently, the industry’s debit networks have begun to reach business agreements to license the technology Visa and MasterCard have offered to move the market forward. These developments facilitate the move to EMV for debit by providing a viable and critical enabling technology: the Universal Application Identifier, or UAID.

Merchants or merchant acquirers will likely upgrade their POS systems to be EMV compatible consistent with in-place terminal replacement cycles. Many of the country’s largest merchants have already completed the re-terminalization process.

Absent national law or regulatory changes, issuers are not required to migrate their card bases to be EMV compatible. Nonetheless, over the next three to four years we expect 60 percent to 70 percent of United States’ card bases to complete EMV migrations.
Liability Shift and Migration

Do I need to switch from magnetic stripe cards to EMV chip cards? What is the liability/penalty if I choose not to issue EMV by a card association’s deadline?
A: No, issuers are not mandated to migrate from magnetic stripe to chip cards. However, effective October 2015, both Visa and MasterCard will shift the POS transaction liability for certain types of card fraud, including fraud resulting from counterfeit, lost, or stolen cards, away from the party that has the most secure form of EMV technology, creating a sense of urgency for issuers and merchants. If neither or both parties are EMV-compliant, the fraud liability remains the same as it is today.

If we reissue all of our cards by October 2015, will all merchants be able to accept chip cards?
A: According to research from Javelin Strategy & Research, “EMV IN USA: Assessment of Merchant and Card Issuer Readiness,” April 2014, more than half of U.S. retail locations are projected to be EMV-capable by the end of 2015. With POS vendors embedding de facto EMV capabilities in devices and with the added incentive of not being “the next Target,” the largest national retail chains will be at the vanguard of the EMV transition with the majority of merchant locations expected to be ready for EMV card acceptance by the end of 2015. Retail establishments with fewer than 20 employees are not expected to exceed 25 percent readiness for EMV by the 2015 milestone.

Instant Issuance of EMV Cards

Can EMV cards be instantly issued in-branch?
A: Yes. Using instant issue hardware and software, EMV-compliant cards can be issued in-branch.

Can we offer temporary debit EMV chip cards?
A: The card associations have only approved magnetic stripe debit cards to be used as in-branch non-personalized temporary cards. Therefore, issuing non-personalized EMV temporary debit cards in-branch is not an option.

Will Fiserv support an instantly issued magnetic stripe temporary secure debit card that will be replaced with a permanent EMV chip card, delivered through the mail?
A: Yes, however, a separate EMV-enabled BIN is required. The BIN for the temporary card can be deactivated/turned off once the permanent card is received, as it is not tied to a cardholder name.

Do we need to be certified to produce EMV chip cards in-branch?
A: An issuer needs to certify for a new card type, such as an EMV card program. As long as you have already been approved by Visa or MasterCard to produce magnetic stripe cards in-branch, there are no additional audits required to begin issuing EMV chip cards in-branch.

What type of plastic does Fiserv offer to support instant issuance of chip cards?
A: Fiserv has several plastic options available for issuers:
- Issuers can order custom white chip plastic with their own KMCs and use their own card design. White EMV plastic can be used with a retransfer printer. Card designs may need to be adjusted to accommodate chip placement. Fiserv will not offer generic white chip plastic as an off-the-shelf option; clients must purchase their own custom inventory.
- Issuers can order custom white plastic with their own KMC and use one of The Card Collection designs. Fiserv has revised The Card Collection designs for placement of the chip. Because The Card Collection designs are proprietary, Fiserv can procure plastic on your behalf and ship it to your branch.
How does key management work for instant card issuance?
A: There are new keys required for EMV (e.g. issuer master key or iCVV). During the installation of in-branch equipment, keys will be loaded into the instant issue software to support personalization of EMV cards in your branch.

Types of EMV Programs

Should we issue our credit, debit, prepaid and HSA cards as EMV cards?
A: The decision to migrate any card portfolio to EMV should include an assessment of the risk and cost of fraudulent transactions, the additional costs of EMV migration, and the perception and expectation of cardholders. For example, the cost of fraudulent transactions for a non-reloadable prepaid card may not be sufficient to justify the time and expense of issuing EMV cards.

Time Required for Implementation

How long will it take to implement an EMV program?
A: The end-to-end process is estimated to take up to six months, depending on the readiness of each vendor in the supply chain. This includes project planning, defining the issuer requirements (e.g. card design, cardholder verification methods, etc.), generating EMV keys, communication (internal and cardholder), and testing and certification. Once certification is achieved on your initial EMV program, subsequent EMV chip issuance will take less time.

Should I be contacting my processor now to begin the migration?
A: Given the long implementation time and the potential that many issuers will want to implement EMV at the same time, it’s important to contact your processor far in advance of a desired launch date. Within Fiserv, a process exists to support clients that want to get into the queue to implement EMV (issuing cards and/or upgrading ATMs). Please contact your Fiserv Account Executive for additional information.

Costs

What is the additional cost to implement an EMV program?
A: EMV migration expenses come in the form of one-time fees and ongoing fees. Some of these costs include higher costs to produce the chip plastic and personalize the cards, upgrade expenses for ATM hardware and software, card processing software upgrade fees, expenses to upgrade instant card issuance equipment, and the potential cost for a new BIN. Card issuers will incur additional marketing expenses to improve consumer understanding of EMV, how it works and its benefits.

Card production costs include plastic (with chip), development and testing, and issuance. The cost of these components will depend on quantity and complexity of the program. EMV chip cards typically cost more than magnetic stripe cards, but many issuers find that this cost is offset by a decrease in card present fraud. Since the widespread implementation of chip and PIN technology in the United Kingdom, domestic fraud losses on U.K-issued cards has been reduced by 34 percent and fraud losses from counterfeit cards are down 63 percent. It’s important to note that because issuers don’t reissue all cards at the same time, a gap can occur between when costs are incurred and when fraud reductions are realized. Issuers may sustain upfront software implementation costs as well as ongoing outlays for card reissuance. Based on the experience of several European countries, fraud reduction won’t be significant until an issuer’s entire portfolio has been reissued. Fraud scenarios are subject to the networks’ liability shift, which doesn’t begin until 2015.
Pricing for plastic and personalization is available from the Fiserv Sales and Account Executive team.

**Program Details and Specifications**

**Plastic and Chip Cards**

**Will the EMV chip replace the magnetic stripe on the card?**
**A:** The magnetic stripe will continue to be the required baseline card-reading format and must be supported on both contact-only and dual-interface cards. Javelin states that more than half of U.S. retail locations are projected to be EMV-capable by the end of 2015 thus leaving a significant portion of retail locations not able to accept a chip card.

**Are there advantages to supporting dual-interface cards?**
**A:** Dual-interface cards support contact EMV transactions (insert the chip card into the terminal for the duration of the transaction) and contactless EMV transactions (tap the chip card on the terminal). Contactless EMV transactions are faster than contact EMV transactions and reduce the likelihood that a cardholder will leave their card behind.

**Should we add contactless functionality to the EMV card?**
**A:** Supporting dual-interface cards adds some complexity to the EMV implementation and increases the cost of each card. Most countries have waited until the “second generation” of EMV issuance to add contactless functionality. By this time, it usually becomes clear if merchants are able to support contactless transactions and if the need for faster transactions justifies the higher costs.

**How does contactless technology relate to EMV?**
**A:** Issuers are now issuing EMV cards that support contact and/or contactless EMV transactions. Contactless EMV transactions use the ISO/IEC 14443 protocol for communication with EMVCo defining the EMV Contactless Communication Protocol Specification that is common for all payment brands. EMV has also published specifications for contactless POS readers that work with the payment brands’ contactless applications.

The EMV specifications provide a basis for contactless EMV payments, but do not specify all payment application functionality. Payment brands can implement contactless payment for EMV transactions to function in both offline and online transaction environments and to leverage the EMV cryptogram security function to validate the authenticity of the card and the transaction.

**Are The Card Collection™ designs available as EMV chip cards?**
**A:** For Central Issuance: A subset of The Card Collection is available as EMV chip cards. The inventory is owned by Fiserv and is a pay-as-you-go program for our clients. Designs are available for credit and debit Visa and MasterCard programs.

For Instant Issuance: Issuers can order custom white plastic with their own KMC using one of The Card Collection designs. Fiserv has revised The Card Collection designs for placement of the chip. Because The Card Collection designs are proprietary, Fiserv can procure plastic on your behalf and ship it to your branch.
What are the options for chip memory and what chip size does Fiserv recommend?
A: Many different chip memory sizes are available and the amount of memory needed is determined by the functionality required on the card. A contact EMV card that only supports online transactions may only need 8K of memory. A dual-interface EMV card that supports offline transactions may require 16K or more. Other applications would require additional memory (e.g. loyalty or transportation). Contact your Fiserv Account Executive for additional information about the options available.

What are the applications that I may want on the chip?
A: Chip cards can contain multiple applications, such as rewards, loyalty, or healthcare, but today most applications are related to financial payments. The issuer will need to determine which applications it wants to support, what its processor can support for authentication, authorization and transactions and what applications its personalization bureau can personalize. Issuers may discover that mandates from a card association or regional switch network may largely determine the applications that must be present on chip cards.

How does the contact chip alter the design of my cards? Are there specific branding specifications that I need to follow regarding the placement of the contact chip?
A: Yes. The placement of the contact chip on the front of the card is consistent on all EMV and dual-interface plastic. The Fiserv procurement team will work with issuers to ensure product specifications are met.

Is the RFID label required on EMV cards?
A: The RFID label is not required on any contact EMV cards. Visa currently requires the RFID label on contactless and dual-interface cards but this requirement will be removed in 2015. MasterCard currently has no requirement for the label.

What is the difference between the Operating Systems options – Native, Java Card on GlobalPlatform™ and MULTOS? Which of these will Fiserv support?
A: The three main operating systems are native or proprietary, Java Card on GlobalPlatform and MULTOS. There are a few other options, but they are used in specific regions (e.g. Advantis in South America).
- **Native** operating systems are unique to each card manufacturer. Chip cards based on native operating systems tend to be low cost, but they tie the issuer to a single supplier and may have proprietary personalization requirements.
- **Java** is the leading operating system based on number of units shipped. Developers tend to prefer Java, since they are familiar with the technology. Java comprises the broadest number of suppliers and products available. However, each different product will require some customization of personalization scripting.
- **MULTOS** has fewer products/vendors available. However, it’s easiest to switch between products, because the same scripts are used to personalize multiple MULTOS products.

It’s important to remember that the cardholder experience and EMV transaction will be the same no matter what operating system is used on the chip card. Fiserv will support all three operating systems.

What is a typical EMV card reissue cycle and how durable is an EMV card?
A: An EMV chip can last longer than a magnetic stripe, because a chip embedded in layers of PVC is more durable than a mag stripe placed on the exterior of the card. However, because the cards will continue to leverage the magnetic stripe for the next several years, most issuers will continue to reissue
cards on a three-year cycle, eventually extending it to four or five years when the majority of transactions take place using the chip.

**Transaction Processing**

**Do I need to have my current processor involved in the EMV Migration?**  
**A:** In order to launch an EMV card program, your processor, card manufacturer and personalization bureau must be involved in the project. EMV will impact card manufacturing and issuance, transaction processing, authorization decision (risk management), disputes and operations.

**What is a Universal Application Identifier (UAID)?**  
**A:** Within an EMV transaction, different technology standards are distinguished from each other using an Application Identifier (AID). An EMV card is personalized with one or more AIDs and the POS or ATM terminal contains a prioritized list of supported AIDs. An EMV transaction takes place using the highest priority matching AID between the card and terminal. In some cases, the cardholder might be presented with a choice if there are multiple matches.

Many debit networks have reached business agreements to license EMV technology from Visa and MasterCard for debit transactions. Visa and MasterCard have established common or universal AIDs (UAIDs) to distinguish between a U.S. debit transaction (that can be routed to different debit networks in compliance with U.S. regulations) and “standard” EMV debit transactions (for cards issued in other countries and when U.S. debit cards are used abroad). Fiserv does not recommend issuing EMV debit cards without including the UAID.

**Do I need to implement a Chip and PIN approach to EMV?**  
**A:** The card brands support a range of cardholder verification methods (CVMs). In the United States, CVMs include signature, online PIN, offline PIN and no CVM (usually restricted to low-value transactions). CVM decisions must reflect card brand rules, merchant and processor capabilities, and risk management strategy. For example, brand rules dictate that all ATM transactions must use online PINs, but many merchant POS terminals do not have the capability to support online PINs. Also, although PINs are generally acknowledged to be a better verification of a cardholder’s identity than signatures, most U.S. credit cardholders do not have or know their PINs. Some issuers will choose to continue supporting signature transactions given their robust fraud detection systems and online transaction processing. Fortunately, EMV cards can support multiple CVM rules that reflect different scenarios (e.g. always require online PINs at ATMs, allow signatures at POS terminals, etc.). There are a small number of unattended terminals in Europe that only support offline PIN.

**What is the minimal functionality I need in EMV processing that will still provide the advantages of increased security for my cardholders?**  
**A:** Because there are varying functionalities available for smart card processing, your processor is in the best position to answer this question. Security within an EMV transaction primarily is driven by validating a cryptogram that is generated by the chip card and passed to the issuer within the authorization request message. This cryptogram is called an Application Request Cryptogram (ARQC). By validating the ARQC, the issuer can determine if the card is genuine and if any crucial data from the transaction has been tampered with or modified (e.g. the transaction amount). The issuer should also be able to generate and Application Response Cryptogram (ARPC). This allows the issuer to reset certain parameters in the card and for the card to confirm that the issuer response message is genuine and has not been modified.
Can my network or association handle the EMV data and verification for our programs?
A: Many processors offer a service to validate the ARQC and generate the ARPC. This is often referred to as On behalf of services. Your processor can assist in this area.

Is online or offline better?
A: It’s important to understand that there are two different types of online/offline decisions. A cardholder PIN can be validated online (by the issuer) or offline (by the chip card). Also, a transaction may be authorized online (by the issuer) or offline (by the chip card, based on rules preset by the issuer). Debit cards should be configured to support only online transactions. Allowing offline debit card transactions will result in overdrafts.

Do we need a new BIN for EMV cards?
A: No. Issuers may use the same BIN for both magnetic stripe and EMV chip cards. BINs are assigned by the network or processor and issuers should refer to them for additional direction. All options are available to issuers, including new BINs or extended BIN(s) if preferred.

Key Management

How involved am I in the key management process?
A: As your card provider, Fiserv will work with issuer key custodians and initiate a key ceremony. There are new keys required for EMV (e.g. issuer master key or iCVV). Additional keys will be needed if offline data authentication will be supported.

Risk Management

Do I still need my other risk management tools if I move to EMV?
A: EMV is an enhancement to risk management, not a replacement for risk management. Magnetic stripe transactions will continue for several years. Also, it’s important to acknowledge that EMV adoption will only reduce the potential for fraud during card present transactions and will not impact card not present fraud, which is of concern due to the growing use of e-commerce.

For card not present transactions, security enhancements continue to evolve and will likely include the use of tokens (e.g. pseudo card numbers that represent the card during a transaction) as an additional measure to further improve payment security. The use of additional equipment or readers would provide a single, one-time password to validate the card not present purchase. These devices are currently in use in other countries.

EMV should be used within the context of a broad, comprehensive risk management initiative that employs best practices such as real-time transaction scoring, blocking of suspected fraudulent transactions, real-time case management and monitoring, and tracking and monitoring of fraud alerts on compromised cards. Before making any changes to a current risk management strategy, Fiserv advises that issuers consult with their partners.
Getting Started

What should I do to prepare an EMV strategy?
A: Given the October 2015 liability shifts by Visa and MasterCard, the potential for fraud reduction and the need to support card use internationally, the migration to EMV in the United States is inevitable. However, these factors should not force financial institutions to rush into an EMV migration prematurely or without careful consideration.

Planning for an EMV implementation requires choices in four key areas:

1. Card interface
2. Card authentication method
3. Transaction authorization
4. Cardholder verification method

Issuers may also need to address four additional areas: key management, PIN management, script processing and fraud risk management parameters.
## Issuer Considerations

<table>
<thead>
<tr>
<th>Roadmap Option</th>
<th>Consideration</th>
</tr>
</thead>
</table>
| 1. Card Interface  | **a) Contact**  
|                    | • Contact cards and readers are widely deployed in markets outside of the U.S.                                                             |
|                    | **b) Contactless**  
|                    | • Contactless cards and readers are a growing trend in global deployment.                                                                    |
|                    | • Issuers will need to recognize the difference between contactless MSD and contactless EMV and choose which to support. At this time, some early contactless MSD cards may not be accepted outside of the U.S. |
|                    | **c) Dual interface**  
|                    | • Supporting both interfaces incurs additional costs.                                                                                     |
| 2. Card Authentication | **a) Online**  
|                    | • Issuers must choose whether to validate card data on their own or allow card brands to validate on their behalf. Issuers must choose whether to receive full chip data or early chip data. |
|                    | **b) Offline**  
|                    | • Issuers must choose whether to support offline card authentication and if they will employ SDA, DDA and/or CDA.                              |
|                    | • Issuers must support a public key infrastructure for offline card authentication.                                                            |
| 3. Transaction Authorization | **a) Online**  
|                    | • Issuers must choose whether to receive full chip data or early chip data for card authentication.                                           |
|                    | **b) Offline**  
|                    | • Issuers can apply various risk parameters to allow the EMV chip to authorize transactions offline on their behalf. Risk parameters may include checking transaction amount limits and the number of consecutive offline transactions before requiring an online authorization to be performed. |
|                    | • Offline authorization has impact on the clearing data and process.                                                                        |
|                    | • Issuers will need to modify their clearing and settlement systems to receive additional chip data (generally in the same format as Field 55 in the authorization request). Clearing and settlement systems should ensure that offline transactions can be identified. |
| 4. Cardholder Verification | **a) Signature**  
|                    | • Signature is included in the CVM list on the chip unless otherwise specified by the payment brands.                                         |
|                    | **b) Online PIN**  
|                    | • Issuers can include online PIN in the CVM list. The online PIN infrastructure will need to be supported by issuer. ATMs only support online PIN. |
|                    | **c) Offline PIN**  
|                    | • Issuers can include offline PIN in the CVM list. The offline PIN infrastructure will need to be supported by the issuer for PIN management.    |
## Roadmap Options

<table>
<thead>
<tr>
<th>Roadmap Option</th>
<th>Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Offline PIN and online PIN should be synchronized to prevent cardholder confusion.</td>
</tr>
<tr>
<td></td>
<td>Issuers will need to support Field 65 through full chip data processing in order to perform issuer scripting (for example, for unlocking and changing offline PIN).</td>
</tr>
<tr>
<td>d) No CVM</td>
<td>No CVM is included in the CVM list unless otherwise specified by the payment brands.</td>
</tr>
</tbody>
</table>

Smart Card Alliance

Financial institutions need to budget, develop a workable migration plan and educate:

- Engage in discussions with all partners involved in the delivery of an issuer’s debit, credit and/or prepaid programs, including the card producer/personalization bureau, card processor, ATM manufacturer, instant issue provider, network provider and card association. Look to these partners for insights and guidance.
- Gain an understanding of the expenses associated with this undertaking and prepare for the investment.
- With the landscape still evolving, consider a transitional approach for introducing chip cards, adding card features and enhancements, and migrating the existing card base to the new EMV chip cards.
- Begin planning early to accommodate reissue cycles and avoid a mass reissue, which could increase fraud. In the short term, issuers may want to consider adjusting expiration dates on newly issued cards to coincide with the liability shift dates of Visa and MasterCard to minimize card reissue costs.
- Consider that EMV chips extend the life of the card, potentially extending reissue cycles to five years once magnetic stripe is retired.
- Develop a plan for new card issuance, card reissue and card replacement.
- Develop a communication plan to educate and increase awareness for staff and cardholders. Emphasize that the experience at the point of sale is different with an EMV card. The card must be in constant contact with the terminal throughout the transaction process due to the dynamic nature of data exchanged between the chip on the card and the terminal during the transaction.
- Address assignment of PAN numbers. EMV requires each cardholder to utilize a unique PAN for application transaction counter (ATC) increment authentication. If the issuer decides to issue a single PAN to joint cardholders, they should proactively work on a strategy to move to a unique PAN for each card issued.
- Review card designs. Placement of the EMV chip within a card product must conform to specific Visa and MasterCard specifications. Ensure that the current card design is compliant or it may require a design and approval process to support EMV capabilities.
- Analyze your portfolio. Identify international travelers that may want or need to be early adopters to ensure their card product is optimal for transacting in EMV markets. Start by issuing a basic EMV-compliant card product, such as credit with basic features and then leverage chip technology to add new functionality in line with market demand.
Should we do a mass issue, especially if we have multiple card programs?
A: Due to the complexity of an EMV migration project, we don’t recommend beginning with a mass reissuance of cards. It’s better to begin with a smaller pilot program and/or natural reissuance cycle. Depending on fraud rates and a desire to meet the liability shift deadline, a mass reissuance of remaining cards can be considered at a later date.

Industry Rollout

How do I find out which merchants in my institution’s footprint support EMV?
A: You should contact your card association to see if a list of EMV-ready merchants is available. Today, some merchants, like McDonalds, CVS and Taco Bell, have contactless-enabled terminals; however, a contact terminal is required for an EMV transaction. Retail giants Wal-Mart, Best Buy and Home Depot have installed EMV-capable terminals at their stores located on the U.S. borders of Canada and Mexico and are extending their EMV programs across the United States.

According to research from Javelin Strategy & Research, “EMV IN USA: Assessment of Merchant and Card Issuer Readiness,” April 2014, more than half of U.S. retail locations are projected to be EMV-capable by the end of 2015. With POS vendors embedding de-facto EMV capabilities in devices and with the added incentive of not being “the next Target,” the largest national retail chains will be at the vanguard of the EMV transition, with the majority of merchant locations expected to be ready for EMV card acceptance by the end of 2015. Retail establishments with fewer than 20 employees are not expected to reach 25 percent readiness for EMV by the 2015 milestone.

The Fiserv Solution

What is the EMV solution from Fiserv?
A: Fiserv delivers a cost-effective, comprehensive and integrated EMV solution through a single point of contact who understands the issuer’s business. We’ll lead issuers through every step of the migration process, starting with an in-depth discovery session, including investments required and potential business case for EMV, followed by decisions regarding the chip card, the processes to obtain EMV certification from associations, and how to educate staff and customers. Our solution includes:

- Strategic guidance and portfolio optimization
- Plastic procurement and card personalization
- Transaction processing
- Risk management
- Consumer and financial institution education

Once issuers are ready to begin, we provide the project management support needed to ensure a seamless and efficient migration from magnetic stripe to chip cards.

Is Fiserv ready to personalize EMV cards today?
A: Yes. Today, Fiserv is positioned to assist our clients with the procurement and personalization of EMV compliant cards. We continue partnership with the leading card brands, the Smart Card Alliance, EMV Migration Forum, EMVCo and the MULTOS Consortium to support and continue development of a worldwide interoperable smart card infrastructure. We strive to be a valued source of information to our clients as they analyze and set their strategies for EMV.
Will Fiserv support EMV for all my card programs including debit, credit, prepaid and HSA?
A: Fiserv can support EMV for all card programs. However, the decision to migrate any card portfolio to EMV should include an assessment of the risk and cost of fraudulent transactions, the additional costs of EMV migration, and the perception and expectation of cardholders. For example, the cost of fraudulent transactions for a non-reloadable prepaid card might not be sufficient to justify the time and expense of issuing EMV cards.

What is the significance of the Accel™ announcements with Visa and MasterCard regarding a Universal AID?
A: The Accel announcements are important, because they offer the issuer and merchant communities an EMV debit solution in the U.S. market. Satisfying debit regulatory requirements by ensuring merchant routing control and issuer participation in a minimum of two unaffiliated networks in a chip environment has presented barriers to EMV entry in the U.S. market for years. Movement of Accel into the EMV environment by supporting the front-of-card brands enables its issuers to transition to EMV in a compliant, streamlined and cost-effective manner, as well as enabling its merchant participants to preserve their network of choice rights. This direction supports the message Accel has communicated over the last 18 months: to support the issuer’s front-of-card choice.