consulting | technology | outsourcing

Accenture Payment Services

Payments Transformation – EMV comes to the US

High performance. Delivered.

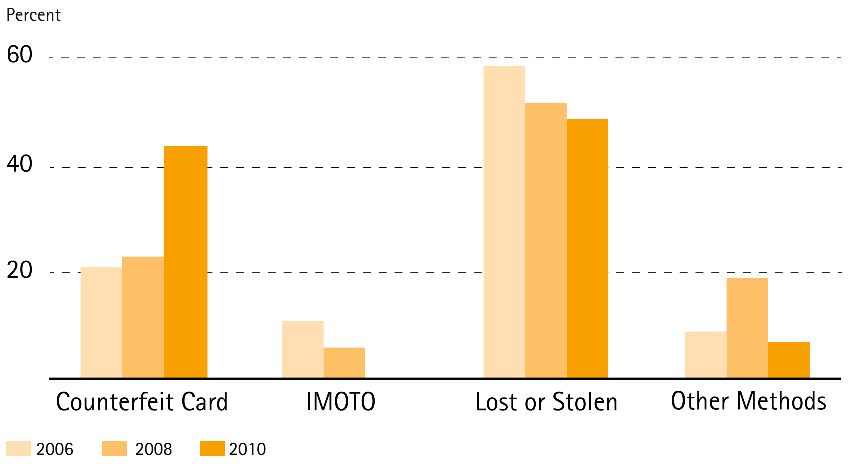
In 1993 Visa, MasterCard and Europay (EMV) came together and formed EMVCo[1] to tackle the global challenge of combatting fraudulent transactions due to the increase in fraudster's abilities to copy the data from the magnetic stripe card. The mandate of this organization was to develop a set of specifications for both terminals and cards to address security and interoperability of cards with devices, which are today referred to as the EMV specifications. In 2012, EMVCo reported that 1.62 billion payment cards had been issued that comply with EMV specifications representing 44.9 percent of all cards issued globally and that 23.8 million POS terminals were EMV enabled which is 75.7 percent of all POS devices deployed in countries that have started migration; these figures exclude the United States.

The strong resistance to EMV in the US has primarily been a result of not being able to justify the increased costs of issuing chip cards over magnetic strip only cards, which is one of the pre-requisite for complying with EMV standards. Merchants have also not been motivated to adopt EMV primarily due to the increased costs required to upgrade their technology infrastructure to support EMV. Together these economic forces have undermined the business case for US investment in EMV.

Today the US is rethinking EMV, particularly as the domestic fraud continues to climb with the growth of skimming, and fraud migrating from neighboring countries where EMV has already been implemented and has been limiting the ability for skimming cards from these countries. (Skimming refers to the methods for electronically capturing the card data and sometimes the PIN without the cardholder's knowledge.) This can occur while a cardholder is performing a genuine transaction at a terminal such as an ATM.

[1] Jointly owned and operated by American Express, JCB, MasterCard and Visa

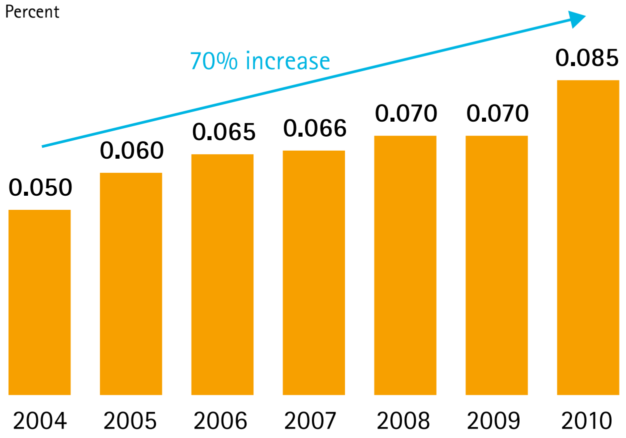
Figure 1. PIN (ATM and debit) transactions



Source: American Bankers Association 2007, 2009, 2011.

Note: The survey question asked respondents to report the method by which fraudsters committed card payment fraud. The survey included 176 commercial bank participants for 2006 and 170 for 2008. For 2010, the survey included 117 full participants and 68 participants who completed an abridged version of the survey. IMOTO: Transaction by Internet, mail order, or telephone order. Other includes card not received for 2010.

Figure 2. US bank card fraud rates



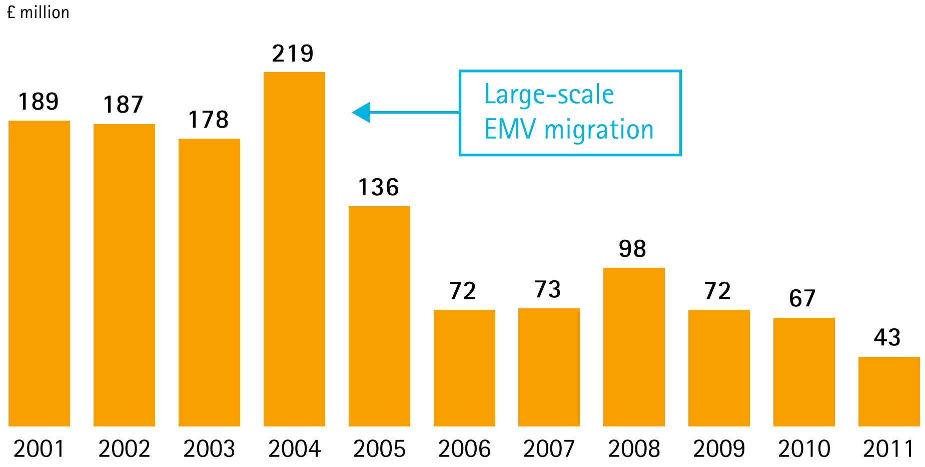
Since 2004, bank card fraud rates have increased by 70% in the United States.

Source: Retail Payments Risk Forum calculations, Payments, Bankcard Profitability Annual Report

Note: Fraud rate calculations are based on MasterCard andVisa consumer andcommercial credit dollar volumes and fraud losses.

Figure 3. Card fraud losses at UK retailers (face-to-face transactions)

UK bank card fraud rates



Source: Fraud The Facts 2012 by Financial Fraud Action UK

Fraudsters capture the magnetic stripe data along with the PIN and then used this data to conduct fraudulent transactions (See Figure 1).

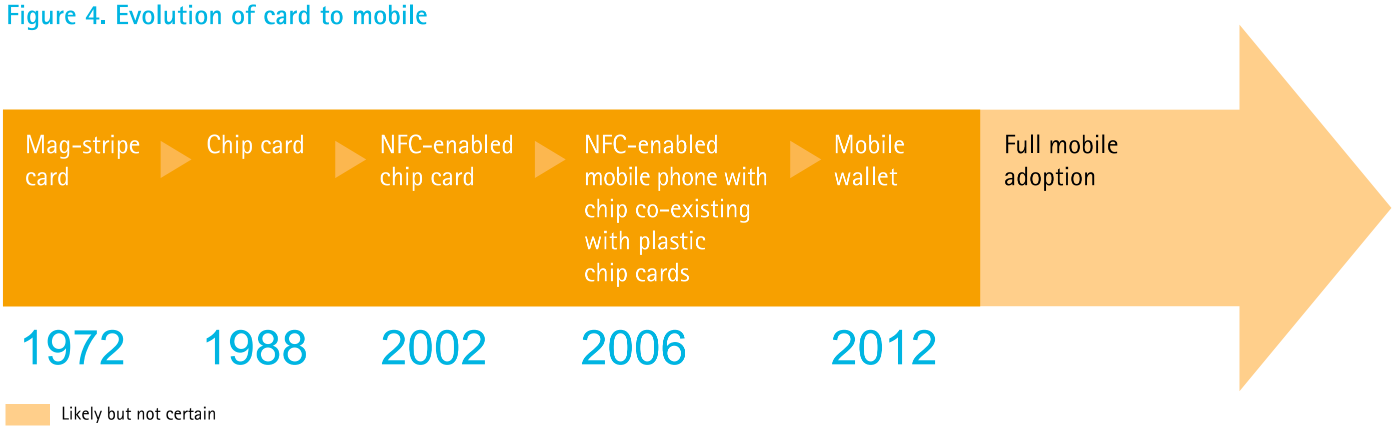
The business case for the US adoption of EMV has been difficult to justify in terms of the payback period and overall manageable rate of fraud so the rationale to move has been slow. However, as more countries migrate to EMV the fraudsters will migrate to the easiest targets. Given most of the countries around the world have started their migration to EMV or are well on the way to completing their implementations of EMV, the US can expect to see the rates of fraudulent transactions continue to climb as the US becomes the easiest target. A leading indicator of this inevitability is that despite the increasing sophistication of the US Issuers' fraud management systems, US card fraud has risen 70 percent since 2004 (See Figure 2).

In contrast, the UK has demonstrated positive results from their migration to EMV. They saw fraud decline by approximately 80 percent, after reaching a peak in 2004 (See Figure 3).

The business case for EMV now goes beyond physical card fraud reduction and considers contactless and mobile payments as well by combining NFC (Near Field Communication) with EMV for use on chip cards and in mobile phones. Although contactless and mobile payments have not yet reached maturity, many predict it is just a matter of time, as Figure 4 shows, given:

- The Payment Networks are advising Merchants to implement NFC in combination with enabling of EMV on POS devices
- Issuers recognizing consumer adoption of contactless card and mobile payments is going to continue to grow, chip costs are decreasing and chip cards can now offer increased functionality. (i.e., dual interface chips—support both contact and contactless)
- Merchants, Financial Institutions, and key technology companies are recognizing the capabilities of smart phones as a means to enrich the consumer's experience

Figure 4. Evolution of card to mobile



To advance the adoption of EMV, the major card brands—Visa, MasterCard, American Express and Discover have mandated that Acquirers support EMV in 2013. They also announced that a "liability shift" will go into effect in October 2015. The impact of the liability shift means that when a chip card interacts with a magnetic stripe-only terminal, the Merchant will be liable for counterfeit and fraudulent transaction losses. By contrast, outside the US the liability is placed on the cardholder if a correct PIN is used, although at times, Issuer customer service may step in to reverse payments made in error.

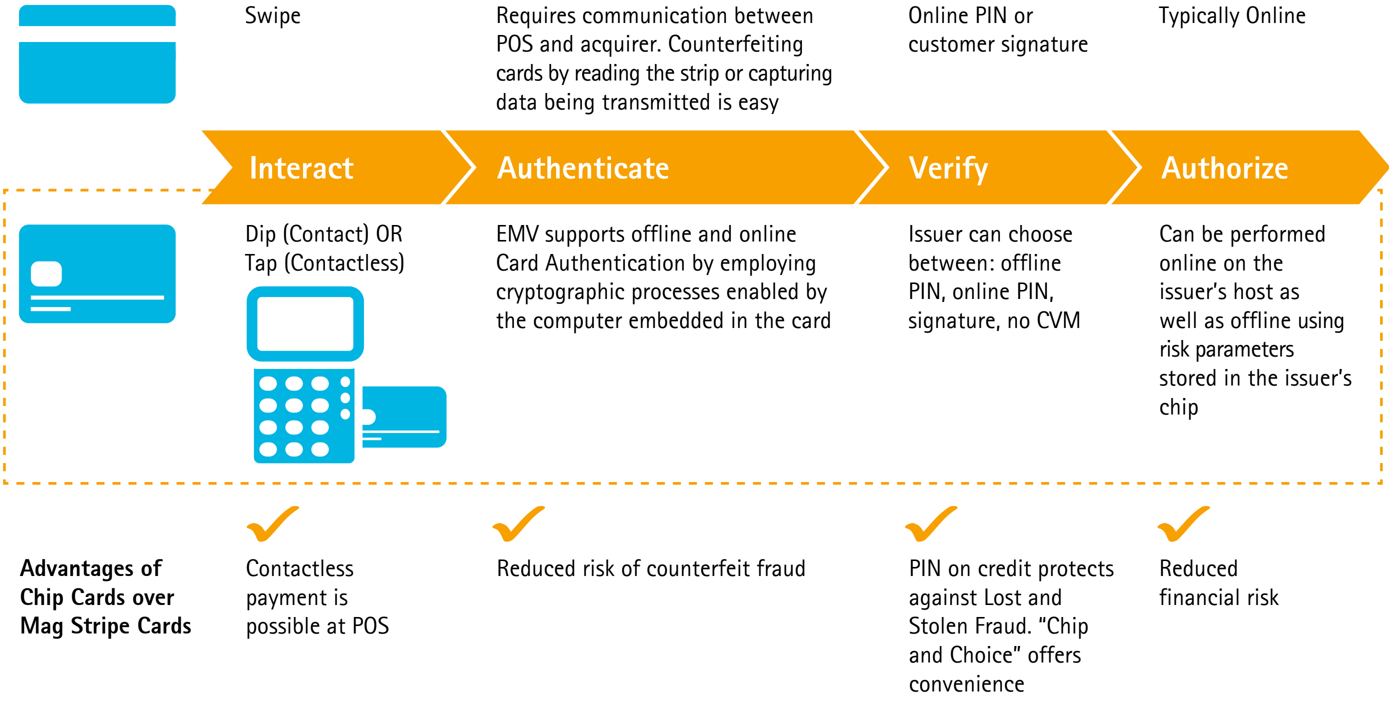
In 2009, EMVCo expanded the EMV specifications to include "contactless" payments. This enables Issuers to move forward with dual interface cards and NFC enabled mobile phones and wallets that are globally interoperable and protected by the security of EMV.

The US's migration to EMV will require significant investment to meet the necessary requirements throughout the value chain of Issuers, Acquirers, Consumers, and Merchants. A few of the specific changes that will drive increased costs are:

- Issuance of chip enabled cards
- Deployment of EMV certified devices with Payment Card Industry (PCI) certified PIN pads
- A more complex card payment lifecycle and management systems are needed to support: public key cryptography, script processing, and card risk management parameters
- Merchant and consumer education required to address behavioral changes
- Authentication and Verification methods that are to be used at ATMs where institutions offer ATM services

Figure 5 highlights some of the differences and benefits between the traditional magnetic stripe card and EMV-enabled cards.

Figure 5. Chip Cards are different from Swipe Cards in many ways and offer several benefits over the latter



	Interact	Authenticate	Verify	Authorize
	Swipe	Requires communication between POS and acquirer. Counterfeiting cards by reading the strip or capturing data being transmitted is easy	Online PIN or customer signature	Typically Online
	Dip (Contact) OR Tap (Contactless)	EMV supports offline and online Card Authentication by employing cryptographic processes enabled by the computer embedded in the card	Issuer can choose between: offline PIN, online PIN, signature, no CVM	Can be performed online on the issuer's host as well as offline using risk parameters stored in the issuer's chip
Advantages of Chip Cards over Mag Stripe Cards	✓ Contactless payment is possible at POS	✓ Reduced risk of counterfeit fraud	✓ PIN on credit protects against Lost and Stolen Fraud. "Chip and Choice" offers convenience	✓ Reduced financial risk

Four Key Decisions

In approaching the migration to EMV, participants within the payments ecosystem need to focus on four key decisions which have impact the business case and the consumer interaction at the POS. These decisions are:

1. **Card/Data Authentication:** Offline or Online

2. **Cardholder Verification:** "Chip & PIN", "Chip & Signature" or "Chip and No Customer Verification"

3. **Method of Verification:** Offline or Online PIN verification

4. **Support for Durbin:** The ability to route domestic debit transactions over the merchant preferred network.

1. Offline or Online Authentication?

The first decision identifies how the authenticity of the card will be assured. Card authentication is the process whereby an EMV card is identified as authentic before a payment can occur, and provides safeguards against counterfeit card creation. Card authentication is done using one of the two authentication methods and is either offline or online.

For offline authentication, the card is authenticated by the POS terminal using cryptographic certificates created or embedded within the chip card or mobile phone. In order to facilitate offline authentication, the Issuer must embed their secrets and certificates onto the chip and distribution of public keys associated with each payment brand accepted must be managed in the terminals.

For online authentication, the card is authenticated, by the Issuer using cryptographic certificates created by the card or mobile phone. The Issuer may choose to do this authentication process online every time, thus removing the need to embed the secrets and certificates in the card.

Or, the Issuer can acknowledge that not all terminals (i.e. transit, vending, etc.) support online capabilities and that some lower value transactions can be authorized by cardholder specific Issuer controlled parameters in the Chip, therefore allowing offline authentication at these devices.

If the Issuer elects to only support online authentication, then the POS terminals used for payments on these cards must be connected to a participating Payment Network and the network must be available for the transaction to be authenticated and approved. Merchants expect that EMV cards will also support offline authentication removing the need for their devices to require online capabilities and providing significant economic advantages especially for low value transaction and fall back in the event of network failures.

2. "Chip & PIN", "Chip & Signature" or "Chip and No Customer Verification"

Once the card has been authenticated, the next step is to verify the cardholder. The EMV specifications identify three different ways the cardholder can provide verification. These are referred to as the Cardholder Verification Methods (CVM) and include: PIN, Signature, or No CVM under specific situations. In Canada, Europe and many other parts of the world Issuers have opted for Chip & PIN, given their concerns over the use of signatures for customer verification.

A solid understanding of cardholder behavior is essential in defining an Issuer's CVM strategy. It is critical for the Issuer to understand and balance the level of fraud reduction they want to try to attained when they define the Cardholder Verification Methods they prefer. In addition they need to consider the attitude of cardholders regarding use of PINs. For example, "Chip & Signature" may facilitate smoother consumer adoption rates due to the process being similar to the way authentication is handled today. However, "Chip & PIN" increases the sense of security a consumer feels and provides additional saving associated with lost and stolen fraud (See Figure 6).

Adopting the use of "No-CVM" requires adherence to Payment Brand and Network rules which define how the Merchant and POS devices support this feature. It is best suited for low value transactions at unattended terminals such as mass transit.

The decisions on how to configure Cardholder Verification is dependent on Issuer preference, payment brand and network regulations, and consumer attitudes.

3. Offline or Online PIN Verification

The third decision, depends on the prior decisions made and if PINs are to be used will they be verified offline or online? Offline cardholder verification verifies the PIN inside the chip. In contrast, online PIN verification requires the PIN be encrypted and forwarded through the Acquirer's and payment brand networks for verification by the Issuer's host. This process also requires the Merchant terminals to be online and have a PCI compliant PIN Pad. The capabilities of the Acquirer and Payment Networks to allow the Issuer's host to receive and verify the PIN entered at the POS is required. When the POS is not online, this is not possible.

While most POS terminals and transactions in the US are online, many terminals and most credit card networks do not support online PIN. Therefore the adoption of online PIN for credit cards will require Merchants, Acquirers, Payment Networks and Issuers to upgrade to their systems, POS terminals, and networks to support online PIN verification.

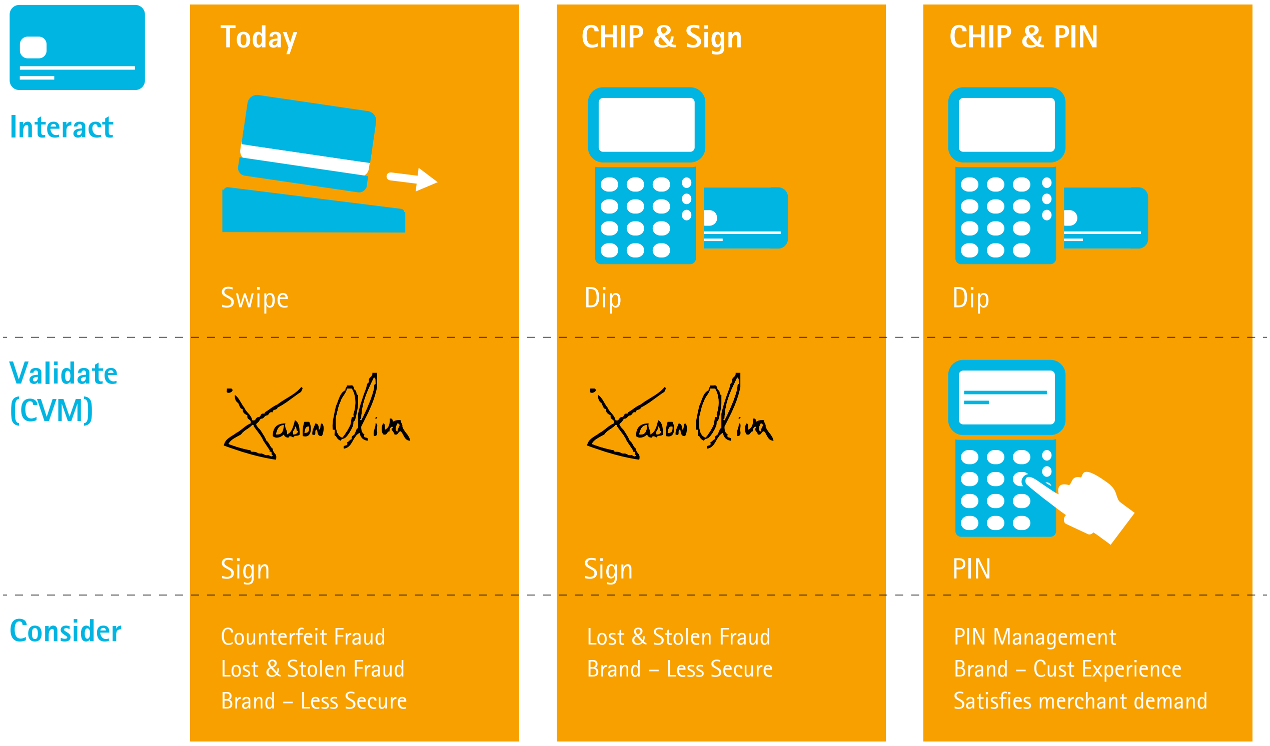
Another key challenge Issuers must address is how they will support PIN management and consumer choice, given that PIN integrity in the card and on the Issuer's host must be synchronization whenever it is changed. To develop this capability Issuers need to consider pre-issuance mailers, Interactive Voice Response (IVR), Bank Website, ATM and/or Branch mechanisms to allow the consumer to easily select and change their PIN.

4. Support for Durbin

One of the complications associated with implementing EMV is the original design objective of assuring Issuer control and consumer choice and the regulations defined by the Durbin amendment. Durbin amendment requires Issuers to identify two or more unaffiliated debit networks for routing domestic debit transactions which has created an interesting conflict.

The industry at large recognizes that the solution must be one that all stakeholders agree on. Industry wide discussions are taking place within one of the working groups of the EMV Migration Forum and until a common approach is agreed to moving forward with upgrading debit cards to EMV may be delayed.

Figure 6. Organizations can implement CHIP & Signature, if synchronizing the PIN in the card and on the issuer host is a challenge



	Today	CHIP & Sign	CHIP & PIN
Interact	Swipe	Dip	Dip
Validate (CVM)	Sign	Sign	PIN
Consider	Counterfeit Fraud Lost & Stolen Fraud Brand – Less Secure	Lost & Stolen Fraud Brand – Less Secure	PIN Management Brand – Cust Experience Satisfies merchant demand

Accenture's approach

Accenture believes that NFC and EMV offer the security and convenience necessary to address the increasing growth in card fraud and the industry's drive to replace the physical cards in ones wallet with the power of the mobile phone. Further, Accenture recognizes that there is room and need for other technologies such as QR codes and cloud enabled payments to co-exist within the evolving mobile payments ecosystem.

Recognizing the opportunities and challenges associated with the migration to EMV; Accenture has brought its global reach and experience built through our work with players across the entire payments value chain together, to help our clients navigate their way through the questions and decisions that must be made in developing their organization's NFC and EMV strategy.

Accenture uses a three-phased approach to help organizations reach the right decisions relative to their investment in NFC and EMV deployment strategies. Some of the key questions for Issuers are shown in the accompanying information panel. Our approach to answering such questions is founded on our proven payments operations model; underpinned by our solid track record of delivery on many EMV migration projects worldwide. The three stages are:

1. Business Impact and Strategy Definition

In this first phase, Accenture would conduct a series of management workshops to gain insights into the client's strategic objectives, existing card products and services. We would simultaneously share our global EMV experiences in a series of educational workshops, designed to enhance the client's knowledge of the consumer, merchant, business, process, technical and industry implications of EMV. This process allows clients to leverage Accenture's experiences, analytic capabilities, and provides the foundation for establishing strategic direction. We would then work with the client team to assess the impact key business decisions will have on all stakeholders. Our goal is to produce with you a sound enterprise wide understanding of the implications and opportunities associated with the deployment of EMV.

2. Business Case Development

Using the insights gained from the first phase as the foundation, Accenture employs proven methodologies to develop the client's business case, allowing clients to reach informed, financially robust decisions necessary to assure a successful EMV deployment. This phase has the following objectives:

- Illustrate the benefits/impact of EMV on client performance
- Specify the necessary investments (IT, personnel and implementation related) required to realize the proposed benefits
- Estimate a project ROI and other KPIs to support the enterprise wide decision on the go forward approach.

3. Solution Roadmap and Implementation Plan

The final phase of the process builds upon the first two, by leveraging Accenture's deep global knowledge of EMV, experience in defining a market leading operating models and skills at developing implementation plans and migration roadmaps; we work with our clients to assure that all the elements necessary for an optimal EMV solution and successful transition are understood and addressed. Specific deliverables in this phase include:

Operating Model

- Define Target Operating Model & Blueprint
- Service Model
- Organization Foundation
- Process
- Technology Assessment
- Define the Payments Architectural Building Blocks
- Conduct a Gap Analysis

EMV Migration Roadmap

- Develop program roadmap, identify key milestones and dependencies for effective coordination and execution
- Identify scenarios, risks, potential issues, and mitigation plans for the migration to an EMV solution

Accenture's EMV capabilities are complemented by market leading assets in consulting, systems integration, and outsourcing. With our EMV experience, knowledge and leading practices, we help our clients implement EMV solutions that best fit their needs and role in the card payments value chain.

Some key questions for Issuers to ask

- Which market segments are we currently serving and which ones in the future would we like to serve?
- What training and communication will our clients' customers expect as the transition to EMV transition occurs?
- What payment products should we migrate first?
- Should we deploy dual interface cards and support contactless NFC transactions from day one?
- Should we support single or multi-application cards or both?
- What modes of verification (PIN or signature) and authentication (online, online preferred or offline preferred) should be supported?
- Should data preparation and card personalization be in-house or outsourced?
- How should we support modifications to card risk management parameters and activate additional features to cards already in customer's hands?
- How should we restructure our Risk, Fraud, Dispute and Customer Management capabilities if we deploy EMV?

For More Information

To find out more about how Accenture can help your bank transform its payments strategy, operations and capabilities, please contact:

Massimo Proverbio
Global Managing Director—
Accenture Payment Services
massimo.proverbio@accenture.com

Jim Bailey
Lead—Accenture Payment Services,
North America
james.e.bailey@accenture.com

Jeremy Light
Lead—Accenture Payment Services,
Europe, Africa and Latin America
jeremy.light@accenture.com

Matthew Friend
Lead—Accenture Payment Services,
North America
matthew.friend@accenture.com

Ian Hooper
Lead—Accenture Payment Services,
Asia-Pacific
ian.hooper@accenture.com

Or visit www.accenture.com/payments

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with 261,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$27.9 billion for the fiscal year ended Aug. 31, 2012. Its home page is www.accenture.com.

Accenture Payment Services

Accenture Payment Services helps banks, payment service providers and businesses improve business strategy, technology and operational efficiency in five key areas: core payments, card payments, digital payments, transaction banking, and compliance, risk, and operations. Accenture and its more than 1,500 professionals dedicated to payment engagements can help banks simplify and integrate their payments systems and operations to reduce costs and improve productivity, meet new regulatory requirements, enable new mobile and digital offerings, and maintain payments as a revenue generator. More than 100 clients worldwide have engaged Accenture Payment Services to help them turn their payment operations into high performing businesses.