NOW is the time to Take the Lead on EMV™
at the POS and the ATM – and Here is HOW to do it

Elan™
Our People. Your Success.

The liability shift for EMV implementation is rapidly approaching. Now is the time to plan how EVM will impact your operations and customer service. EMV will impact every stakeholder – from issuers and acquirers to merchants and consumers. Let us help you plan a strategy for successful and cost-efficient deployments.

Start by understanding the proposed EMV timelines

It is critical to understand the details of the proposed timelines because they can have far-reaching consequences for your institution and your cardholders.

The network EMV liability shift time line is important for the issuer to understand and take into consideration when formulating its EMV strategy. The networks have not established a mandate for when issuers must begin issuing EMV cards, however, liability shift dates for merchants and ATM acquirers may have an impact on when issuers decide to begin their rollout. The liability shift date for merchants is October 1, 2015. Liability shift dates for ATM acquirers are scheduled for October 1, 2016 for MasterCard® and October 1, 2017 for Visa®.

It is important to note that when compared to today's environment, the liability shift does not increase an issuer's liability. Issuers are currently liable for fraudulent transactions at the point of sale. What the October 2015 liability shift may do is give the issuer the opportunity to shift liability, for fraudulent transactions, to the merchant if its cardholder uses a chip card and the merchant's point of sale device is not enabled to support EMV technology. If both parties are equally EMV compliant, the issuer continues to bear the liability for the fraudulent transaction.

It is expected, given the media attention surrounding the recent data breaches at merchant locations, big box stores will be ready to accept EMV transactions by the October 2015 liability shift date and merchant acquirers will be able to support EMV transactions on behalf of the small to mid-size merchants. Therefore, the opportunity for issuers to pass on liability for fraudulent transactions may be smaller than originally thought.

Understanding how the Durbin Amendment (Regulation II) impacts EMV

The Durbin Amendment requires that any debit card presented to a merchant be processed on at least two independent debit networks – one for signature debit and one for PIN.

This issue came to the forefront in 2013 when a Federal District Court decision was announced. In the decision, Judge Richard Leon found that the Board of Governors of the Federal Reserve System did not follow congressional intent when it determined the amount of interchange a financial institution, with assets over $10 billion, could receive was $0.21, plus 5 basis points, plus an additional $0.01 if the issuer qualified for the fraud adjustment. Judge Leon also found that the Board erred when it interpreted the requirement to have two unaffiliated networks available to a merchant should be based on the card, and not based on the transaction.

Judge Leon's ruling further complicated the issue as the industry grappled with how to allow for the choice of additional signature networks on the same transaction at the point of sale. In March 2014, the U.S. Court of Appeals overturned Judge Leon's ruling finding that the Board acted reasonably in how it interpreted the language of the Durbin Amendment, including the

unaffiliated network requirement. While the ruling created more certainty for the industry from a regulatory standpoint, complications with EMV due to the Durbin Amendment still remained.

As pointed out, EMV technology was not designed with the Durbin Amendment in mind. The unaffiliated network requirement introduced a wrinkle for the U.S. EMV migration, in that debit card acceptance had to be solved before the industry could move forward. In order to comply with this requirement, the industry had to choose whether to support numerous payment

applications and application identifiers (AIDs) on the same card or create a common AID solution in which all payment networks could participate. In the end, the use of a common AID was introduced by Visa, MasterCard and the Secure Remote Payments Council that allowed networks to share use of a single AID, making it easier for the industry to comply with the Durbin Amendment. The common AID solution supports a quick-to-market EMV approach for regional PIN networks – and multiple routing options for merchants. Additional payment network partnerships are expected to be announced in 2014, providing card issuers a scalable solution to migrate their debit portfolios to Durbin-compliant chip cards.

Creating a Bullet-Proof Business Case for EMV

What is the cost to move to EMV?

What are the associated risks, if clients choose not to move in 2015?

As a first step, card issuers and ATM acquirers must create an EMV Business Case to evaluate risk and cost of the program. Some institutions will immediately move their cards to EMV – to change the calculus and mitigate counterfeit fraud exposure. Others will choose to hold off on their investment, until U.S. merchants and ATM acquirers have fully migrated to EMV – which ensures interoperability across all terminals and improves cardholder experience at the point of sale and ATM.

Step 1: *Calculate Risk Exposure*

To take a proactive approach, you should start your EMV project planning this year. Complete risk and cost benefit analyses are required. Financial institutions and ATM acquirers should conduct their own internal due diligence, by answering the following questions:

- What are the institution's PIN and Signature Debit counterfeit fraud losses today?
- Is there appetite to incur additional fraud, and if so, how much incremental fraud risk is the card issuer willing to take – before migrating cards and terminals to EMV?
- What is the card portfolio size - including inactive and active cards? (Inactive or non-activated bank cards have potential for fraud.)
- How many cards are replaced year-over-year, due to card expiration or lost/stolen?
- Border regions typically report higher counterfeit fraud activity. Are branch and ATM terminal locations within close proximity to a cross border country? (e.g., Canada or Mexico)
- Does the client use fraud detection or anti-skimming service products today?
- If the institution owns ATM terminals, determine the fleet size. Using a segmentation analysis, determine which terminals require complete, or chip card reader (only), replacement.

- Are ATM manufacturers providing competitive incentives, if EMV is bundled with Windows 7, or other PCI upgrades? This may result in a cost savings to the client.

The response to the above questions will gauge the client's risk factor and lay the foundation for EMV costs.

Step 2: *Develop a Budget Plan*

Based on responses to questions above, a formula can be derived, using industry estimates relative to past EMV migrations:

- **Cards** – The reported all-in chip card cost is estimated at $2.00 to $5.00 per card. Pricing differs, if issuers request additional functionality be added to the chip (e.g., multiple payment applications, support of a contact and contactless interface, or support of offline components). Added program set up and certification fees may also apply, on top of card production costs. It's best that clients work through their designated vendor to estimate payment network, card bureau and processor program costs. Make sure you look for an in-house data preparation solution will support use of the issuer's existing magnetic stripe BIN in a gradual portfolio migration environment; or new BIN, if considering a mass reissue. Gradual card migrations may take over a year – however, it's also the preferred approach that allows institutions to budget their EMV migration year-over-year. Make sure your plan supports the complete card lifecycle – as magnetic stripe cards expire; new plastics are replaced with micro-chips.

- **ATM** – Reported ATM terminal upgrade costs are approximately $2,000 per terminal. All terminals have various levels of upgrades needed, from complete hardware replacement, to upgraded EMV chip card readers. ATM owners are encouraged to call their ATM manufacturer provider to assist in deriving a cost replacement estimate – and to determine any incentives for bundling software upgrades.

- **EMV Certification** – Industry pricing indicates payment networks can charge incremental fees for Card Personalization Validation and Issuer End-to-End Testing Demonstration, in some cases. As with standard card program certifications. Ask your vendor to assign a Project Manager to guide you through an approximate four month implementation process.

Step 3: *Choose an EMV Card Profile*

When considering their first chip card program, card issuers should select the simplest profile with the fewest acceptance implications. The U.S. primarily operates in an online payment environment, whereby the transaction is authorized online – at the point of sale and ATM. International regions operate in both an online and offline payment environment, therefore, cardholders may still experience minimal acceptance gaps, without the support of an offline PIN personalized to the chip. Examples of offline terminals include unattended kiosks, Toll and Transit merchants (typically, small ticket transactions).

Another key decision by the card issuer is whether to choose a chip-and-PIN profile (synonymous with debit, using a PIN) or chip-and-signature profile (credit, using signature as the preferred cardholder verification, and not PIN). Chip -and-signature transactions are not as secure as chip-and-PIN, but due to its dynamic encryption ability – is more secure than a magnetic stripe credit card transaction.

Chip-and-signature credit cards are generally accepted everywhere chip-and-PIN cards are, with the exception of certain unattended kiosk terminals equipped to request a PIN to complete the chip card transaction.

A recent survey by The Members Group (TMG) found the majority of both Visa and MasterCard issuing clients plan to issue contact-only, signature-based EMV cards that authorize only in an online environment. Issuers should be aware of the added counterfeit fraud protection that comes with using a PIN, as it authenticates the card to the cardholder.

Analysts predict that the United States will evolve to a hybrid combination of both profile options to best support the type of business, transaction type, and compatibility. Take the simplest approach when considering your first migration to EMV like the one below:

- Select the simplest card profile, such as Online PIN authorization and authentication.
- Include a PIN, for secure cardholder authentication.
- Do not add higher functionality levels at first card issue, such as support of offline authentication or contactless. Consider these options as merchants support them.
- Add (only) one global network application to your chip (examples: Visa VSDC, MasterCard M/Chip or Discover DPAS). Adding multiple payment applications requires added space on the chip's operating platform, therefore, larger chip size equals a higher cost to personalize and certify.
- Include at least one common U.S. Debit AID to the chip so that merchants have multiple, unaffiliated PIN network brands as routing options. Visa, MasterCard and Debit Network Alliance have announced U.S. Debit AID solutions – offering portability in changing PIN network relationships without card reissue.
- Consider one International AID for acceptance, typically provided by Visa or MasterCard, if the institution has a business need.

Card issuers should get assistance with prioritization of preferred Cardholder Verification Method (CVM) settings to guarantee multiple acceptance options at point of sale and ATM:

- Online PIN
- Offline Enciphered PIN
- Signature
- No CVM

Step 4: *The importance of Communications and Cardholder Education*

In 2014, card issuers should consider developing their Marketing and Communication Plan to educate cardholders on the differences between chip cards and magnetic stripe cards.

Chip cards will be inserted into POS and ATM chip terminals, and left in the terminal until the transaction is completed. Consumers will enter their PIN when prompted. In some instances, institutions have announced their intent to offer Credit Rewards cards with PIN entry, to replace signature as the method of cardholder identification, as PIN is a more secure authentication method.

To ensure cardholder convenience, debit and credit cards will continue to carry a magnetic stripe for use at non-chip enabled terminals. The cards will be swiped and a signature will continue to be required for credit card transactions and a PIN for debit transactions.

EMV does not protect against Card Not Present (CNP) fraud. The EMV Migration Forum is working with merchants, acquirers and issuers to enhance the use of multiple identification factors for e-Commerce transactions, to include a PIN and One Time Password (OTP). Some payment networks are actively piloting display cards, adding the OTP feature directly to the payment card. The card will produce a unique encrypted code for each online purchase.

Another fraud mitigation tactic allows a randomized PIN, whereby a PIN pad is displayed on the website's checkout page with the digits on the pad depicted randomly. As the cardholder enters their PIN, only the encrypted XY coordinates of the digit clicked are transmitted for authorization.

Institutions should consider the following topics to educate cardholders:

- Tell consumers chip cards are coming, and when they've arrived
- Why their card has a new look (silver or gold chip on the front plastic)
- Why they're getting a new card
- How to use the new card at POS terminals and ATMs
- Assure cardholders that it's okay to use the card at non-EMV compliant terminals
- How to make an Internet purchase

In summary

Every financial institution has different fraud characteristics, clients and products that need to be considered in the EMV planning process. Starting to plan now is "smart business" and will help ensure a successful transition.

Elan™
Our People. Your Success.

ATM and Debit Processing Solutions
ATM Managed Services
MoneyPass ® ATM Network