Your Reference Guide to EMV Integration: Understanding the Liability Shift

CHASE Paymentech™

UNDERSTANDING EMV

EMVCo was formed in February 1999 by Europay®, MasterCard® and Visa® to establish and maintain global interoperability and acceptance of chip payment cards. EMV technology defines how the applications on the chip work, including debit, credit and additional programs such as gift and loyalty cards.

WHAT IS A CHIP CARD?

Chip and PIN payment cards are embedded with a microchip that can store and process data securely and assists in enhancing security, reducing fraud and chargeback levels. The data stored on the chip is virtually impossible to copy and helps to protect payment information and prevent certain types of payment card fraud. Chip technology is designed to evolve as future enhancements become available.

CHIP MIGRATION IN CANADA

Preventing the growth of fraudulent activity is one of the main driving factors behind chip implementation in Canada. Chip technology is Canada's response to payment card fraud, making it increasingly difficult for fraud organizations to target cardholders and businesses alike. As such, chip cards are increasingly being issued by Canadian financial institutions to support and migrate to this technology.

Working together to develop Canadian standards for chip, the "Payment Brands" (American Express®, Interac®, MasterCard, Visa) have established migration plans and programs to assist with circulating chip cards to the market. These plans are as follows:

- Visa and MasterCard have announced liability shifts that will take effect in October 2010. Merchants who have not upgraded to a Chip and PIN terminal by October 2010 will be exposed to additional chargeback categories to today's environment.
- Interac has stated that they plan to have 100 percent of their cards converted to chip cards by December 2012. As such, merchants will be required to upgrade to a Chip and PIN terminal to meet security requirements outlined by Interac.
- American Express has not currently announced any mandates, but will support issuer, acquirer and merchant migration plans.

In addition to the Payment Brands and the financial institutions, merchants play a key role in chip migration. The liability for any fraudulent transaction that would have been prevented by chip technology will fall on the merchant who has not yet migrated to chip. As such, it is important that merchants upgrade their terminals to accept Chip and PIN cards so that they help shield against the impact of this liability shift and also provide security enhancements to their payment platform.

CHIP TECHNOLOGY AND RESULTING LIABILITY CHANGES FOR CARD-PRESENT, DOMESTIC POS TRANSACTIONS ONLY[1]

Overview of the Possibility of Chargebacks for Fraud for Missing Signature and/or Imprint (electronic or manual)

POS Terminal type	Card type	Expected Verification Method	Does the Issuer have the possibility to chargeback for a fraudulent transaction involving missing signature and/or imprint?	
			Pre-01 October 2010	Effective 01 October 2010 Liability Shift Date
Magnetic-Stripe	Magnetic-Stripe	Signature	Yes	Yes
Magnetic-Stripe	Chip & Signature[1]	Signature	Yes	Yes
Magnetic-Stripe	Chip & PIN[1]	Signature	Yes	Yes
Chip[2]	Magnetic-Stripe	Signature	Yes	No[4]
Chip[2]	Chip & Signature[1]	Signature	Yes	No[4]
Chip[2]	Chip & PIN[1]	PIN	No[3]	No[4]

[1] A Chip card (both Chip & PIN and Chip & Signature cards) will have a magnetic-stripe for operability at magnetic-stripe terminals. A Chip & Signature card uses signature rather than PIN as the verification method.

[2] A Chip POS terminal has the ability to read both Chip and magnetic-stripe cards and has a functioning PIN pad.

[3] **Pre-01 October 2010**, where a Chip POS terminal is used **and** the verification method is PIN, Issuers are not permitted to chargeback a fraudulent transaction for missing signature and/or imprint (electronic).

[4] **Effective 01 October 2010**, where a Chip POS terminal is used, then **regardless** of the verification method used, Issuers will no longer be permitted to chargeback a fraudulent transaction for missing signature and / or imprint (electronic).

Understanding the Liability Shift

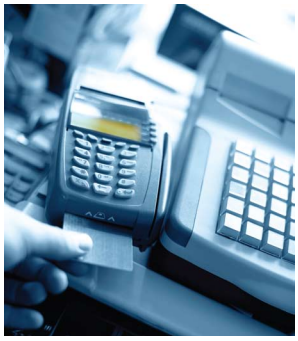
CHASE Paymentech

Drivers and Benefits for Chip Technology

Although there are a number of factors driving EMV migration in Canada, mitigating fraud is the leading reason merchants are striving to upgrade their point-of-sale (POS) in advance of the liability shift. This new technology not only provides interoperability but also helps increase security against fraud.

Chip and PIN technology provides the opportunity for merchants to help decrease the occurrence of fraudulent activity and as a result, may have a positive impact on their bottom line. There are additional benefits from this technology, as it also helps provide the following for Canadian merchants:[2]

- A uniform payment experience for both credit and debit transactions;
- A stronger method of authentication over signature-based transactions;
- Validation by the issuer for credit transactions is done after the consumer uses their PIN, not by the signature comparison done by the merchant;
- Potential improvement to checkout speed;
- Potential reduction in credit card disputes, chargeback and other associated costs; and,
- Potential reduction in paper supplies.



First Steps Towards EMV Migration

As a merchant, you play a critical role in initiating, planning and facilitating the migration process. The migration to chip will require most POS systems to be upgraded or replaced, testing the new systems and staff training. As such, multiple lines of business within your organization will need to participate in varying roles to execute an EMV roll-out.

Here are some considerations for merchants prior to project initiation:[3]

- ***BUSINESS CASE DRIVERS:*** Financial and non-financial.
- ***PROJECT COMPLEXITY:*** Hardware, software, network, operational procedures, financial procedures and security must all be taken into consideration prior to project initiation.
- ***RESOURCE REQUIREMENTS:*** In addition to IT staff, involvement from Finance, Store Operations, Loss Prevention and Help Desk areas may be required.
- ***PROJECT SCOPE:*** Proper definition of project scope and consistent communication to the project team are critical.
- ***PROJECT TIMELINE:*** Carefully estimate and allocate time required for key activities.
- ***CERTIFICATION TIMELINES:*** Acquirers will require each integrated merchant solution to be certified with their acquirer host. Certain Payment Brands may also have additional certification requirements. Each Payment Brand has proprietary testing processes.
- ***TRAINING:*** Important for the trial and rollout of the solution. Training will likely also be required for staff in areas such as Finance, Operations and Loss Prevention.

Before undertaking an EMV migration project, merchants first need to decide which internal and external resources are needed to help reach migration goals. As a merchant, if you decide to initiate a migration project with your POS software vendor, then you will need to reach out to that vendor to understand what considerations need to be made to help meet deadlines.

If you decide that working with Chase Paymentech on your migration project is your preferred option, then speak with your Relationship Manager. Together with Chase Paymentech's Merchant Implementation Team (MIT) and Retail Sales Consulting, they will help to support you with the outline for your migration requirements (hardware/software), integration options, timelines and other considerations. Your Relationship Manager may also serve as a project team member for the duration of the project.

Your Reference Guide to EMV Integration: Implementation Best Practices

CHASE Paymentech™

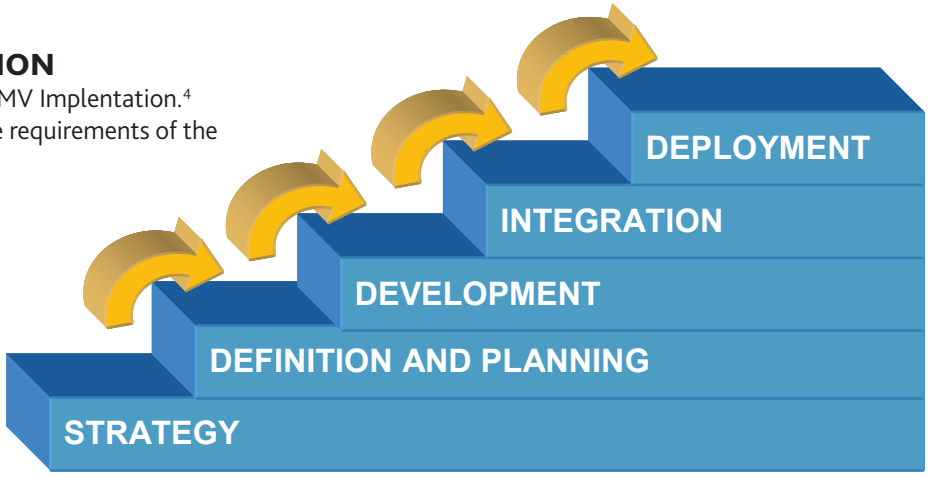
This section of the EMV Integration Guide summarizes the phases typical of an EMV implementation. Moreover, it helps to provide a framework for the various tasks that merchants may need to account for when initiating their project plan. Every merchant has their own implementation requirements based on their existing hardware and software payment configuration and may require internal resources and external partners to execute these. As a result, no two implementation projects are the same; however, all merchants share the same goal: a successful migration to EMV.

Because it is the merchants' responsibility to ensure that their POS system meets EMV standards and is compliant, understanding what may be required during an implementation is important. Generally, attributes of a successful EMV migration program include:

- Multiple stages of planning.
- Established goals, objectives and strategy that are communicated and has stakeholder approval.
- A strong business case.
- A Project Management team that includes subject matter experts, technical resources, and partner resources (acquirer, VAR, etc).
- Scheduled ongoing audits and reviews.
- Ongoing project management meetings that provide updates and identify any risks.
- Testing throughout the project.
- A small pilot to identify any adjustments needed prior to a full scale roll out.

PHASES OF AN EMV IMPLEMENTATION

Summarized below are five phases of a typical EMV Implentation.[4] Again, these phases may differ depending on the requirements of the individual merchant.



Key considerations for each phase are outlined below to provide a guideline as to the types of resources, tasks and deliverables that may be required to develop and execute an EMV Migration project. As each implementation will differ from merchant to merchant, the deliverables within each phase and the phases themselves will reflect this. In addition, the distribution of tasks and deliverables for each merchant will vary depending on the role internal resources and external partners play in the project.

PHASE 1: STRATEGY

- Understand EMV and its impact on your company.
  - Initial implementation.
  - Future requirements.
- Define the value proposition for your company.
- Outline your project objectives.
  - What are the critical success factors for your organization?
- Clarify your scheme requirements/input.
- Review any central co-ordination requirements and input.
- Initial assessment of impact on your various lines of business and review any outsourcing options, if needed.
- Develop a budget estimate.
- Develop a presentation for the various internal stakeholders.
- Present to management and obtain approval to move to Phase 2.

PHASE 2: DEFINITION AND PLANNING[4]

- Define your business requirements.
  - Include all lines of business that will be affected.
  - Define the priorities (example: corporate vs. franchise locations).
  - New services/applications/products to be offered to your customers.
- Develop your technical and functional requirements based on your business needs.
- Planning.
  - Pre-migration planning.
  - Organizational planning.
  - Project roadmap.
- Define the budgetary implications to various lines of business.
- Payment scheme input/requirements.
- Define any consultancy needs.
- Establish the deliverables, if any, for your vendors (Chase Paymentech, VARs, others?).
- For any outsourced project aspects, define:
  - Timeframes.
  - Costs.
  - Mandated deliverables.
  - Measurements for success/failure.
- Agreements.
- Central project requirements and representation from lines of business, stakeholders, vendors, etc.
- Project Management.
  - Milestones.
  - Deliverables.
  - Regular status updates.
- Assign your project team.

PHASE 3: DEVELOPMENT[4]

- Coding requirements.
- Unit testing.
- Documentation and support materials.
  - User manuals, quick start guide, troubleshooting, call centre scripts, FAQs, etc.
- EMV certification.

PHASE 4: INTEGRATION[4]

- Merchant Implementation Team (MIT) Planning.
- Integration tests, including regression testing.
- Internal support team education and training.
- Internal staff training.
- Pilot implementation.
- Review issue resolution and escalation processes.

PHASE 5: DEPLOYMENT[4]

- Software and hardware roll-out.
- Maintain your subject matter experts for subsequent phases – multi-application, contactless, two factor authentication, etc.
- Review any lessons learned.

Your Reference Guide to EMV Integration: The Certification Process

CHASE Paymentech™

BACKGROUND

The migration to EMV / Chip and PIN technology impacts both acquirers, such as Chase Paymentech, and its merchants. Some of the implications for both parties include:

	CHASE PAYMENTECH	MERCHANTS
HARDWARE AND SOFTWARE UPGRADES	All new hardware must be EMV certified, signed and tested by Chase Paymentech.	Existing POS terminal hardware and software will need to be upgraded or replaced with chip-enabled equipment.
HOST SYSTEM UPGRADES	EMV introduced more data into the authorization and clearing messages than with the current mag-stripe technology. All processing systems will need to be modified to handle this additional data.	Any integrated systems must be re-certified with the addition of EMV certification requirements by the Payment Brands.
TERMINAL MANAGEMENT	New applications and hardware need to be managed separately.	The replacement or upgrade of the terminal has to be carefully managed as it creates opportunity for fraudsters to obtain devices.
CHECKOUT PROCEDURAL CHANGES	N/A	All front-line staff need to be trained as the transaction process is different at the checkout.

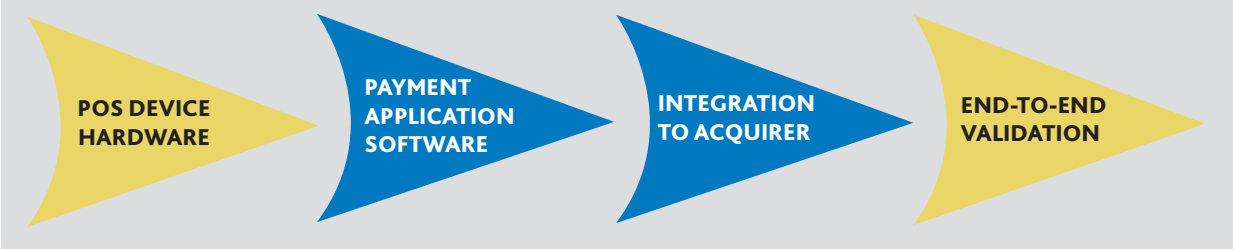
In summary, the migration to chip is not a one-sided process, but involves merchants, acquirers, issuers and even cardholders. To ensure a smooth transition, an understanding of the migration and certification process is required. From there, each merchant can decide which option best suits their requirements.

THE ROAD TO EMV

Moving to EMV has many benefits for merchants. It provides an opportunity to help reduce costs and streamline store processes to realize efficiencies. The EMV compliance process consists of several stages:[5]

- **Stage 1:** The equipment itself must be 'Type Approved' to satisfy EMV requirements.
- **Stage 2**: The payment application software must be validated. Each Payment Brand has its own terminal application software requirements that need to be met.
- **Stage 3:** After hardware and software validation, the connection between the POS terminal and the acquirer must be validated.
- **Stage 4:** The entire chain for transactions must be established and validated. Integrated merchants will need to participate in testing application software and the merchant-acquirer connection validation phases.

STAGES OF THE EMV COMPLIANCE PROCESS



The Certification Process

STAGE 1: POS DEVICE HARDWARE[5]

Chase Paymentech will be able to supply to its merchants who rent POS terminals, hardware that meets outlined EMV Level I and II requirements. If a merchant opts to purchase rather than rent their terminal device; as a best practice, the merchant should:

- Request a copy of the Type Approval certificate. The certificate should include the configuration of the device and the software/firmware version numbers that were used to Type Approve the device.
- Validate that the device they are purchasing is identical, in all regards, to the device that was Type Approved.
- Ensure that the POS device is approved for use by the relevant Payment Brands. (American Express, Interac, MasterCard and Visa).
- Validate that the device complies with the rules and operating procedures of the relevant Payment Brands and the acquirer.

As POS technical specifications vary by Payment Brand, a brief overview of the requirements for each are outlined in the table below. These requirements are applicable to all acquirers:

REQUIREMENTS BY PAYMENT BRAND[5]

Payment Brand	American Express	Interac	MasterCard	Visa
POS Device Hardware Technical Specifications	PCI PED testing requirements specifications.	Device must be certified using the Interac-Chip PIN Entry Device (PED) Technical Specifications and Testing Requirements (TSTR)	Device must be EMV L1 and L2 Type Approved and must meet PCI PED specification. Please ask your acquirer for details.	Device must be EMV L1 and L2 Type Approved and must meet PCI PED specification. Please ask your acquirer for details.

STAGE 2: PAYMENT APPLICATION SOFTWARE[5]

Payment Application Software is the payment brand-specific software application that must be loaded onto the POS device to support the individual Payment Brand EMV chip transactions. The payment application software must also be validated.

Merchants who have purchased their own payment application software are responsible to ensure that the solution deployed complies with all the Payment Brand specifications. It is important to ensure that the payment applications are functioning as expected and do not result in any interoperability issues.

A brief overview of the requirements for each Payment Brand's payment application software are outlined in the table below:

PAYMENT APPLICATION SOFTWARE CERTIFICATION REQUIREMENTS BY PAYMENT BRAND

Payment Brand	American Express	Interac	MasterCard	Visa
Payment Application Software Certification Requirement	American Express ICC Payment Specification (AEIPS) Chip and PIN Test Plan.	Self-Certification by application owner using an Interac-approved test tool vendor. The Association reviews the test result to ensure compliance.	Terminal Integration Process (TIP).	Acquirer Device Validation Toolkit (ADVT).

STAGE 3: MERCHANT CONNECTION TO THE ACQUIRER NETWORK[5]

This stage in the EMV compliance process is to ensure that the POS set up transmits the appropriate data to the acquirer host. Acquirers (and VARs if applicable) must ensure that this connection has been validated and certified as part of the certification process. Merchants who provide their own solution are responsible to work with their acquirers to certify the connection between the merchant system and the acquirer network. Merchants with a proprietary switch will need to ensure that their network can support EMV chip transactions.

The Chase Paymentech certification queue is open to both merchant and vendors. There is no cost from Chase Paymentech to validate and certify the connection between the merchant system and the acquirer network; however, MasterCard may charge for their brand certification and additional EMV development and testing tools may be required. Your Relationship Manager can help you get started.

STAGE 4: END TO END VALIDATION[5]

This is the last stage in the EMV compliance process and is managed by the acquirer. End to end validation occurs between the acquirer and the appropriate partners. Merchants who rent or lease their terminals from an acquirer or VAR should confirm the extent of their participation in the end to end validation with their acquirer/VAR. Integrated merchants who purchase their own POS solutions will be advised by their acquirer/VAR if merchant involvement is required in this stage of compliance process.

MIGRATION IMPACTS

Given the elements and various stages of an EMV compliance project, it is also important to understand the impact that the migration process will have on your POS hardware and software infrastructure. For EMV migration, a new software application will be required and must be certified by the Payment Brands as outlined in the phases above. Below is a high-level overview of the requirements for hardware and software:

HARDWARE:
- EMV Certification (Level 1 and Level 2)
- PCI DSS

SOFTWARE:
- Visa (ADVT)
- MasterCard (TIP)
- Interac (Self-Certification, PCI PED)
- American Express (AEIPS)

Given the migration requirements above, the table below briefly summarizes the various factors that may influence which certification option a merchant selects. It is important to also factor in any restrictions based on the current POS hardware and software a merchant is using, as this may limit a merchant's certification options.

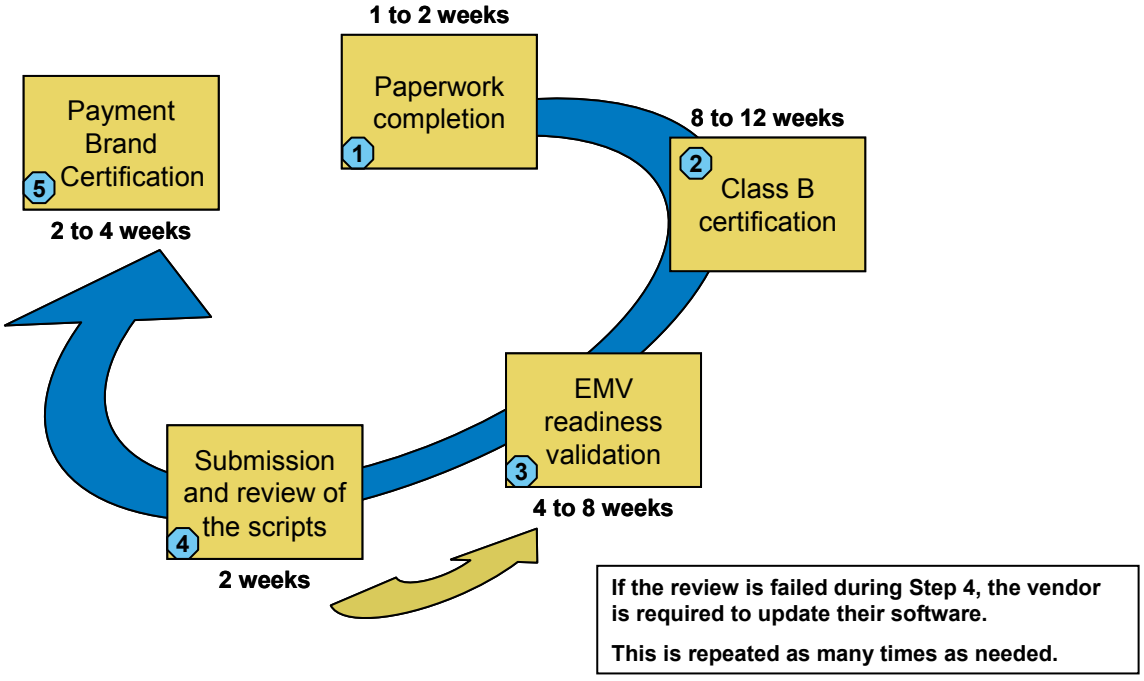
OPTION	COST	ESTIMATED DURATION	CUSTOMIZATION	COMPLEXITY
Direct Certification	High	6-12 months	High	Requires full EMV knowledge
Interoperability	Medium	3-6 months	Use existing certification	Requires EMV knowledge
ECRi	Low	2 weeks	None Send transaction to stand alone POS	No EMV knowledge required

EMV MIGRATION OPTIONS AVAILABLE WITH CHASE PAYMENTECH:

OPTION 1: DIRECT CERTIFICATION

Complete customization of the POS application and payment application. This may be the logical choice for larger merchants and those with proprietary systems. The direct certification option is similar to the one you may have completed for magnetic stripe. In addition, for Class B you will need to complete the EMV certification for the brands you want to support. This kind of certification is customer specific.

Benefits: This is a choice for larger merchants with a proprietary system. Direct Certification provides a complete customization of your POS and payment applications.



OPTION 2: INTEROPERABILITY

This option leverages an existing EMV certification which may shorten the testing process. In this option, you leverage the test cases and application of the original certification and confirm that the results are identical. Usually, this option is selected by merchants that already work with a middleware vendor.

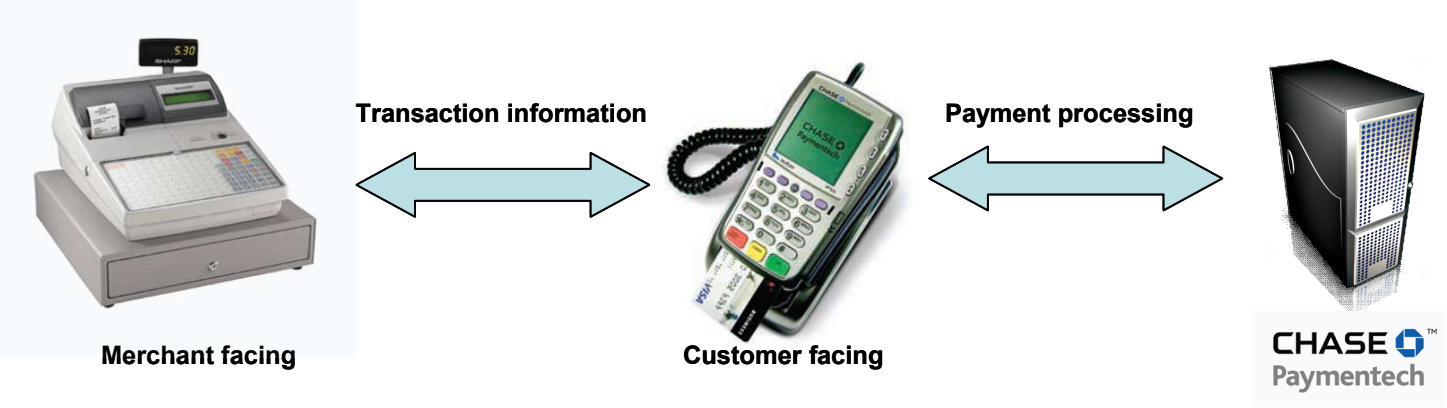
Benefits: Compared to a full certification, interoperability may be faster and more cost effective because you can leverage an already existing EMV certification. Assuming that changes to the systems are minor, testing can be done using the same environment that was used for the original certification. Some merchants already work with a middleware vendor which may have an existing EMV certification.

The Certification Process

OPTION 3: ECRi

A semi-integrated solution, with no direct certification required. An interface application connects your cash register directly to a standalone POS device that is EMV certified. The terminal manages all of the payment data.

Benefits: Compared to other certification options available, ECRi provides a straightforward implementation with simple coding and no certification required. As all the payment data is contained within a PCI-certified payment device (not the merchant system), ECRi provides a viable EMV migration option. Chase Paymentech will update the payment application as part of the regular upgrade programs, relieving the merchant from some of the maintenance requirements.



FINAL CONSIDERATIONS

In preparation for migration from mag-stripe to EMV, Chase Paymentech has outlined a number of EMV certification options to assist merchants in their migration projects and provide good alternatives to reach certification that is in line with their business and technology needs. That being said, there is no "one size fits all" approach to EMV migration. This is especially the case for integrated merchants. As such, it is recommended that merchants outline and discuss all their requirements for EMV migration with their Relationship Manager so that they can collectively determine the best course of action.

Sources:
1. Visa Canada. "Visa Canada Guide: Chip Chargeback Matrix for Liability Shift and No Fallback Transactions." October 2007.
2. EMV Canada, "Canada's Migration to Chip." www.emvcanada.ca. Accessed 17 February 2010.
3. EMV Canada. "EMV Chip Implementation Milestone Guidelines." (September 2007). www.emvcanada.ca. Accessed 17 February 2010.
4. ACI Worldwide. "EMV Implementation." March 2007.
5. EMV Canada. "EMV Certification Overview for Merchants." (September 2007). www.emvcanada.ca. Accessed 17 February 2010.