

# Merchant Networks and EMV Migration

## Opportunities and Issues

You are a Canadian merchant, and that means you are in the beginning of a new chip card acquiring era. Your card acquiring equipment and the way you accept debit and credit cards will change.

If you own dozens of stores with multiple cash registers, and your sales staff work shifts round the clock, this White Paper is for you and about you. Read it but remember: whatever is said here is to trigger your own thoughts. **This paper will not save you money and time, or prevent stress, but your actions can.**

### 1. How Chip Migration Impacts You

- **POS investments.** You will have to pay, one way or another, sooner or later, for your point of sale (till) hardware and software migration. Below we will discuss how to spend this money in the best way at the proper time.
- **Fraud.** You are told you will reduce your fraud-related losses. Yes, you will if you migrate to chip technology in the proper way in the proper time. We will talk about this too.
- **Staff training.** You will have to pay for your staff training. Again, there are good and bad ways to spend this money. We will talk about that.
- **New Technology.** You will have more business opportunities with new card technology. We will talk about how this technology can change your business.

### 2. Is Liability Shift Scary?

Visa liability shift (Oct 1 2010) is not yet the Apocalypse. Let us see how Liability Shift works. Before you read the following, please note that entire legal aspects of fraud liability are very complex. They are depicted in Visa® and MasterCard® dispute resolution rules, and the rules change two times per year. Thus, you will find below the description of the simplified and most typical situations. Please do not refer to this example for the legal purposes.

#### ***2.1. Liability Shift from the Card Issuer to You***

Let us consider the following example:

- Today is Oct 2 2010.
- A bad guy with a counterfeit Visa® card comes to your store and buys something. He skimmed the magnetic stripe from the real, genuine card. (Chips cannot be skimmed, which is why we are moving to them).
- Your POS (till) is still not chip-enabled so the card is read via magnetic stripe and the fraud is not detected.
- When the real cardholder claims that he/she did not make this transaction, you will pay.

If the bank has not yet provided the real cardholder with a chip card, liability will be determined based on the old magnetic stripe rules as it was before Oct 1, 2010. There is a very important part of the liability shift scheme; liability is shifted only for the chip cards.

The above is the illustration of the chip liability shift. There is also Chip + PIN liability shift. In that case the bad guy has stolen the original chip card but he does not know the PIN. If you accept this card (via the chip or not) because your POS does not capture the PIN, you will pay.

You can see now that an important question is how many old style Visa® magnetic stripe cards, will be replaced by chip cards by October 2010. The card issuers have their own business plans. The credit card lifecycle is 3-5 years. If the issuers start replacing them today, and if they do this systemically, they will replace almost all credit cards by 2012. Thus, the liability will not be completely shifted to you (if your devices are not ready) in one night. The fraud liability will develop the pressure on you gradually, worse in the later stages.

There are also the following important factors:

- What if you operate in Windsor, ON, and your main customers come from the US? Remember, that there is no liability shift for US card issuers, and in 2010, their cards will be as magnetic striped as they are today.
- Remember: only Visa® will have liability shift in Canada in Oct 2010. MasterCard® and Amex® have not published anything.
- Bear in mind that Interac® intends to ban magnetic stripe POS by 2015. Here we go. This is the promised Apocalypse date for the magnetic stripe: Happy New Year 2016!

## ***2.2. Liability Shift from You to the Card Issuer***

The liability shift also works in the opposite way. If you have your POS ready for accepting the chip cards and PIN, and the card issuer does not have chip cards yet, you will not pay in case of fraud. The liability is still with the issuer.

But wait a minute! Who pays for the fraud today, when everything is done via magnetic stripe? The issuers pay, you do not. You are liable only if your staff did something wrong. If you equip your POS with chip readers and PIN-pads and your client comes into your store with a magnetic stripe card, your staff is still obliged to do everything right with this magnetic stripe card even after the liability shift!

Both before and after liability shift, dealing with magnetic stripe cards, your staff must capture cardholder signatures and verify them, visually inspect the cards to determine whether they are genuine and take all the other normal steps to ensure that the card is authentic and the party presenting the card is the rightful owner.

The outcome from this observation is the following. If your acquiring system is chip-compatible, then the more chip cards are in your customers' wallets, the more you save on fraud prevention and simplified card acceptance procedures.

### **2.3. When the Time Comes**

Now you can see that the **liability shift date is not a reliable criterion for saving money on fraud. The criterion is the proportion of your clients with the chip cards in their wallets.**

Thus, the ideal world would behave in the following way. There are no chip cards in your clients' wallets before you become chip-enabled, and all your clients have chip cards the day after you become chip-enabled. Unfortunately the real life is far from that ideal.

Based on that understanding, you can time your strategy. Let us talk about your strategy now.

## **3. Your Migration Strategy**

### **3.1. Invest to Understanding**

First of all, invest money in research. Find the answers to the following questions:

- What should my card acceptance process look like? Will it change from the existing process?
- Since I have to modify my hardware and software anyway, what else can I improve in them for the same money?
- What additional opportunity can my business gain from the card technology, and how can this be accounted for in my new card acceptance strategy?
- What are my fraud liability-related risks, and when is the proper time to migrate to chip+PIN acquiring?
- When and how should I train my staff?

### **3.2. Invest in a Small Pilot**

Before you spend all your money and achieve 100% chip+PIN readiness, build a small pilot with your VAR, and see how it works. Re-factor your solution based on the gained experience.

Here is a funny question: where will you get this experience if there are almost no chip cards in your clients' wallets yet? You may need so called test processing environment and test cards. Ask your acquirer and VAR to provide this for you.

### **3.3. Accomplishing the Migration**

After you have done your pilot and you see that everything works smoothly, you are ready to spend the main part of your investment money. You have balanced your risk and time with your financial capabilities and you are well on your way. We wish you success!

## **4. All that Staff**

Let us talk about your sales staff and how you should spend money for their training.

### **4.1. When to Spend Training Money**

Training staff can cost a lot, and the question you must ask is "when is it best to train my staff?" Do not spend money on staff training unless your people can practice chip transactions at least once a day, otherwise, they forget everything you have taught them. This issue can be related to the problem of test cards and test environment mentioned above.

### **4.2. Staff Training and POS Software Quality**

If your staff training does not go smoothly, something may be wrong with the POS software. Discuss the problem with your VAR.

Find the proper balance between the money you spend on POS software and the money you spend on training. Good POS software will not only save you money on training but facilitate positive customer experiences as well.

That is why you need a pilot.

## **5. Opportunities**

Chip card technology impacts your business. You can make this impact positive if you understand the new capabilities and create the best way to use them.

### **5.1. Tips and Chips**

Most likely, you are not in a restaurant business, but let us consider a restaurant example, anyway. Even if you do not own a restaurant, you eat in them sometimes and are familiar with this business process. This example demonstrates that chip card acceptance may require some changes in the business process.

You know how the tip authorization works with magnetic stripe cards. Chip card acceptance may require a different approach. The client-cardholder does not give the card to the waiter to take to the point of sale. Instead, the waiter approaches the table with a portable POS, and the card is inserted into the chip reader. The restaurant business owner should find the answers to the following questions, and the answers will be different for different types of restaurants and different categories of customers:

- How and when are the tips to be specified by the client and captured by the POS?
- Is the procedure convenient for clients and waiters?
- When is the client supposed to make a decision about the tip amount: before the waiter brings the POS, at that very moment, or after?

- Should the process be the same for debit cards and credit cards?
- What are the psychological aspects of this process? Will you get more or less tips compared to the magnetic stripe technology?

The answers are not easy for the restaurants owners. What are the applicable questions for your business? Think and be aware of how much time you may need to plan your pilot.

To help you plan better, consider the following examples as well.

### **5.2. Offline Authorization**

You have a network of agents/salesmen that visit your customers at home or in their offices to sell your product.

- The agents can accept magnetic stripe cards but the procedure of manual imprint and signature capture is time consuming.
- It is possible to skim the card numbers and reuse them fraudulently.
- In many cases online authorization is required.

With chip cards the process could be easier. A palm-top POS will capture the transaction. In some cases, if the card is programmed for this by the card issuer, the transaction would be authorized offline. The card is always in the cardholders' hands. The agent does not need to see and record the card number.

The same scheme works with taxi drivers and restaurant waiters.

This example, again, demonstrates that the new technology can impact your business, and can give you new opportunities. Think of how you will be able to use them.

### **5.3. Contactless Cards**

New types of chip cards do not even require that the card be inserted into the POS. Tap and go technology has proved to be efficient in fast food restaurants. It also works well with any business where payment must be done at the entry to or exit from the service zone (e.g. theaters, transit fares). The service time can be reduced significantly. This technology works for small payments where the PIN is not used and the risk is small.

### **5.4. Loyalty Programs**

Your loyalty program can be an application that can reside in the same chip card your customers use. A stand-alone loyalty card may not be needed. Of course, in this situation you would need to collaborate with a chip card issuer, creating your own brand name card.

The chip card is more intelligent than the magnetic stripe one. You can create a loyalty application and place it into the payment chip card. The application stores some data related to your clients shopping activity. Your POS will then be able to calculate the loyalty policies based on the data stored on the card.

For example, the fast-food restaurant can give a cardholder the fifth free hamburger if the previous four were purchased within the last month period excluding Sundays. Another example is a transit service: the cardholder is eligible for a day pass for the rest of the day if three rides have been already purchased today.

These examples demonstrate that there are capabilities you could hardly have with the magnetic stripe cards unless you use a stand-alone loyalty card authorized online.

What is remarkable here, is that storing encrypted personal information on the card, as opposed to storing it in your database (as you do now with your regular loyalty program), eases privacy protection concerns. The amount of data you have to protect in your database becomes smaller. It is still reasonable to store some critical data in your centralized database system. This will help to restore the data on the replacement card in case the client loses the card.

## 6. Questions?

We are sure that you still have more questions. Do not hesitate to send them to us:  
[e.lishak@lifecycleintegrity.com](mailto:e.lishak@lifecycleintegrity.com)

=====

(c) Eugene Lishak, Lifecycle Integrity inc. 20 May 2008. Canada.