CLUBSolutions

EMV Credit Cards and how it affects your club

September 2015

These days everybody is talking about fraud prevention and the new EMV credit card standard. With credit card fraud on the rise, it seems there's a new story every day in the media about some large organization being "hacked" and customer credit card data being stolen. EMV (Europay, MasterCard, Visa) microchip credit cards have been active in Europe and Canada since 1999 and implements an enhanced security feature, which combats "card present" fraud. So, why has it taken so long to activate this technology in the United States? The simple reason is the enormous amount of effort required by banks, merchants and processors to implement the technology. Processors (organizations that manage authorizing credit card transactions between banks and merchants) will need to rework their systems to process EMV transactions; merchants (gym owners) will need to purchase new hardware; and banks will need to issue EMV enabled credit cards to all of their customers. As Europe has completed its migration to EMV, the region has seen an 80 percent reduction in "card present" credit card fraud while the U.S has seen a 47 percent increase in "card present" fraud.

So, what exactly is EMV; how does it work, and why do we need it?

Our current credit cards use a magnetic stripe laid across the back of the card to store information. This information does not change and is called "static." EMV credit cards have a microchip embedded, which interacts with the point of sale (POS) to create a dynamic authentication code for each transaction. This microchip enables the payment processor to have a high certainty that the card is authentic and the transaction is not a fraudulent transaction. Had EMV credit cards been in place prior to the hacks in major US retailers recently, the affect would have been minimalized and it is unlikely the hackers would have been able to re-use the data. One important thing to note is that with EMV credit cards, they combat "card present" or, "in person" transactions only. Online or telephone based transactions are still susceptible to data compromise.

Why should you use EMV?

While there is no hard deadline for EMV implementation, there is a "Liability Shift" date of October 1st, 2015 wherein the responsibility of paying for fraudulent transactions will trickle down. Today when a consumer finds a fraudulent transaction on their account, they call and notify their bank of the transaction and the bank researches the fraud. In most cases the bank refunds the money to the consumer's account and the credit card company (Visa, M/C, Discover, etc.) absorb the costs. After October 1, the responsibility for absorbing the costs will cycle down to the organization that does not support EMV. Think of the credit card companies at the top, then the payment processors, followed by the merchants (gyms). If the payment processors offer EMV transaction processing but the merchants choose not to deploy it, the gym owners will be responsible for absorbing the costs of the fraudulent transaction. One item to note with the EMV liability shift in the health club industry is that the rate of fraud within this market is (very) small.

What's involved in setting up EMV and do clubs need it?

Health clubs will need to work with their payment processors to purchase EMV-POS hardware to support EMV transactions. At this time, credit card processing companies are ramping up their support organizations and pushing out EMV enabled hardware to integrators. Health club management software companies are working to integrate the EMV technology into their platforms. Request information from your payment processors on when they will have this technology available and what the deployment steps will be.

What's the Club Cost?

The hardware cost for clubs transitioning to an EMV-POS system (basic system upgrade) is around $300-$800. For wireless terminals and/or NFC (Near Field Communication) capable terminals, which allow mobile access will cost more. If you have a POS system in place, you will only need the new reader hardware that can process chip-enabled EMV credit cards. Club owners can also expect to see higher processing fees dictated by the banks and credit card companies for EMV transactions due to the additional overhead required.

Summary – weighing the risks and costs

Credit card fraud within the U.S. has been growing in the past few years. Criminals who are hacking into major retailers are looking for credit card data. The use of EMV credit cards will make the capture of this data unusable to attackers. While there is no set deadline for all U.S. transactions to be processed by EMV hardware, there is a strong belief that this is coming. Recent hacks of major retailers have made consumers very aware of security, as it relates to credit cards. When an organization suffers a breach, they lose customers and they feel the company is not protecting their data. It's looking quite a bit like insurance. You don't drive a car, or own a house knowing the negative consequences of not having insurance. Retail businesses will most likely feel the same regarding the investment in an EMV-POS system. At this time, the risk of not going to EMV enabled hardware is the risk of gym owners having to pay for the fraud committed at their locations and the possible loss of consumer confidence.

Jose Calvillo
Chief Information Security Officer
ASF Payment Solutions
Jose.calvillo@asfpaymentsolutions.com