MVP

INFORMATION FOR A SAFER FINANCIAL EQUIPMENT INDUSTRY

Why Upgrade to EMV at the ATM?

A Brief History

Since the inception of the credit card concept established by Diner's Club, Inc. in 1950, criminals have been working hard to find new and inventive ways to commit card fraud. This long-term research and development has effectively rendered the security measures on magnetic stripe cards obsolete.

It is due to this long-term focus on perfecting their craft that card fraud has hit an all-time high globally. Counterfeiting of cards, especially, has been gaining an even greater percentage of fraud compared to standard lost or stolen cards. It is this advancement in fraud that pushed the card networks to smart chip technology. Since its introduction in the United Kingdom in 2005, EMV has been gradually implemented throughout Europe, Africa and the Middle East, Asia Pacific, Latin America, Mexico and Canada.

The Risks for Banks & Credit Unions

Many Americans have little knowledge of the complete payment cycle or the encryption communication process involved when it comes to EMV (Europay-MasterCard-Visa) technology.

However, since the implementation of the EMV liability shift at point-of-sale (POS) terminals in 2015, U.S. consumers have steadily become more aware of the benefits of chip card technology. The integration of EMV at major retailers with prior security breach concerns such as Target and Home Depot have reinforced a basic understanding of the added protections chips provide for in person transactions. Yet many merchants, ATM operators and even financial institutions are slow to move toward complete EMV integration – putting themselves at ever increasing risk.

Liability Risks

While many would argue that the main problems with EMV implementation in the United States revolve around the complicated structure of the U.S. financial system. The plethora of processors, banks, credit unions and equipment providers makes the landscape far more difficult to navigate – especially when attempting to implement something as in-depth as encrypted card processing. However, a good portion of the blame can be attributed to the actual EMV Liability Shift.

"Liability Shift" refers to the announced dates at which the card networks have determined their fraud coverage policies will change. Traditionally, the financial liability for fraud was held by the card issuer – typically banks and credit unions. After the liability shift, the financial burden falls on the party in the payment chain that failed to be EMV compliant. If all parties are EMV compliant, the card issuer retains liability.

For financial institutions, this liability shift means a temporary reprieve from financial liability for fraud as, once a bank or credit union transfers their issued cards to EMV, any instance of fraud occurring at a non-EMV terminal is now the merchant or ATM operator's responsibility. In addition, traditional card-present fraud with smart-chip enabled cards is much more difficult – effectively reducing the number of fraudulent transaction claims across the board.

MVP

Why Implement EMV at the ATM?

As the experience of Citibank Latin America portrays, the changeover to smart chip technology, is pushing criminals to the path of least resistance – non-EMV compliant POS terminals and ATMs. As fraudulent activity migrates away from chip enabled machines, any non-compliant ATMs are at a significantly greater risk.

Banks and credit unions that have EMV enabled machines reduce their exposure to fraud by making their machines less of a target. By implementing smart chip technology at their ATMs, financial institutions can protect their bottom line by taking full advantage of the added fraud protection offered by the changeover to EMV.

But most financial institutions do not simply issue cards – they also operate ATMs. At these in-house ATMs the institution is not only the card issuer, they are the ATM operator as well. Just as under the prior liability model, being the issuer and operator ensures the financial responsibility remains the responsibility of the bank or credit union.

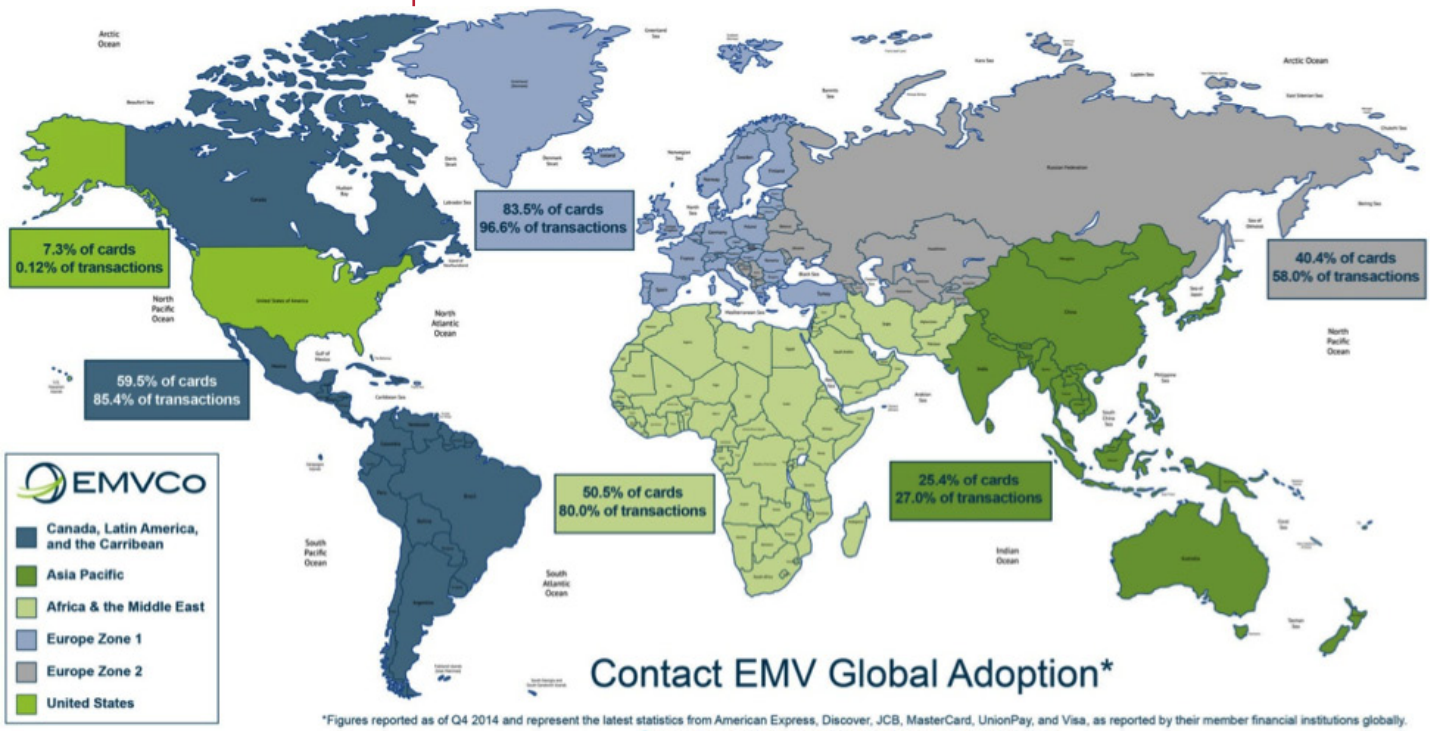
There are many reasons banks and credit unions may not have selected to upgrade their ATMs, yet. Banks and credit unions, especially those with a large card base, may have decided to concentrate on upgrading their cards before tackling their ATMs. Chip cards are more expensive than mag stripe cards and the financial burden of upgrading their cards may have forced some banks and credit unions to put off upgrading their ATMs due to budgetary restraints. Or it may be because upgraded ATMs do not directly affect the liability model at institution machines that a bank or credit unions are selecting not to upgrade. No matter the reason, these institutions may be inadvertently creating risk far greater than they expect.

Increased Risk Through Fraud Migration

In all instances of EMV integration, countries and regions have experienced a temporary increase in counterfeit fraud as criminals extended extra effort to take advantage of the closing window of opportunity. Once the window closes, fraudulent use of card information typically occurs outside of EMV compliant markets. Once EMV was integrated in the UK market, card networks and issuers adjusted their acceptance requirements for foreign transactions – creating a significant drop in fraud. In 2015 counterfeit fraud in the UK was reported to remain around £43.4 million, according to a Payments Card & Mobile report.

While ports, large cities and vacation spots have typically been at higher risk for fraudulent activity, EMV implementation changes the game for criminals. Due to the closing window of opportunity, areas with low population, including rural settings are in equal or greater danger.

Just after the Latin America transition to EMV, Citibank Latin America addressed EMV implementation concerns at the 2014 ATM & Mobile Innovation Summit. Alvero Cordoba, ATM & channels head for Citibank Latin America spoke of an instance where rampant card fraud forced the bank to reduce their ATMs in a specific country from thousands to a mere 300. Yet, despite the significant decrease in ATM availability, fraud had increased the next month.



*Figures reported as of Q4 2014 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures are reported by region and do not imply country-by-country statistics.