WHITE PAPER

atm marketplace

Navigating the ATM Transition to EMV for Regional Financial Institutions

A trusted partner can ensure that an ATM fleet is prepared to meet the looming deadlines and provide enhanced security for consumers.

By Gary Wollenhaupt
Contributing writer,
ATMmarketplace.com

Sponsored by:
RED HAWK
Fire & Security

Despite years of war against it, card skimming is the largest source of fraud in the ATM industry. Security experts estimate that the average skimming results in a loss of $30,000. To combat that loss, the industry has introduced EMV, or the chip-and-PIN card, named for the card associations that launched the security standard (Europay, MasterCard and Visa).

These smart cards carry a computer chip that houses the card data and that must be presented to a properly equipped ATM or point-of-sale terminal to complete a transaction. Since 1998, when the transition to EMV began, about 99 percent of all European ATMs have become EMV compliant. However, many cards around the world still use a magnetic stripe that provides an opportunity for skimming.

Because fraud almost always migrates to the weakest, most unprotected areas, delays in introduction of EMV to the United States have left the market vulnerable, with criminal activity rushing into the region as neighboring Canada and Mexico made the switch. Criminals in countries that have implemented EMV obtain card data there and then use it in the U.S. to make fraudulent transactions. Because many cards still have magnetic stripes, criminals can skim data from the card but are blocked from using the data in countries that require EMV cards because they can't clone or copy the cards embedded with EMV chips. The criminals must move to countries that don't use EMV to create fraudulent cards to use for withdrawals.

Conservative estimates put card-skimming losses worldwide at around $1 billion per year. Visa and MasterCard are introducing a liability shift for EMV compliance in the U.S., which means any party in the payments system that is not EMV compliant will bear the cost of fraud losses. Implementation of EMV in the U.S. is designed to curtail that global criminal activity.

This paper, sponsored by Red Hawk Fire & Security, outlines the complexities of the

EMV transition facing financial institutions and the value of using a trusted partner to manage the process.

Transitioning to EMV in the U.S.

After successful implementation in Europe, Canada, Mexico and much of Asia, EMV is finally making its way to the U.S.

MasterCard began the process with a requirement that all ATMs that accept its Maestro international card be made compatible with EMV cards by 2013.

The challenge became tougher with an additional deadline for ATMs that accept any MasterCards to be compliant by 2016. FIs that do not meet the guidelines face greater liability for fraud.

Initially, MasterCard applied the liability shift only to those fraud cases where an international-issued chip card was used at the ATM in question. Now, if a U.S. ATM used by a fraudster is not EMV compliant, the ATM owner (i.e., the FI) is liable for the losses. In this instance the fraud shift applies only in the case that the compromised card was issued by a foreign bank. Domestic liability shifts for MasterCard are scheduled for October 2016.

Visa has announced its timetable for EMV migration for the ATM channel.

- Effective April 1, 2015, U.S. third-party ATM acquirer processors and subprocessors must be able to support EMV chip data.
- Effective Oct. 1, 2015, liability will shift in Asia Pacific, excluding China, India, Japan and Thailand.

Objectives of EMV migration:

- Define international specifications for both issuing and accepting smart cards
- Reinforce the security of the payment system by limiting counterfeit cards and defining a greater security role for the issuer at the point of sale
- Provide a framework for offline transactions
- Define a structure for multi-application use

- Effective Oct. 1, 2017, liability will shift in China (excluding domestic transactions), India, Japan, Thailand and the U.S.

Additionally, Visa said that as of April 1, 2013, a liability shift now applies to all qualifying transactions taking place in Australia and New Zealand. Liability shifts are also already in effect for Europe, Canada, Latin America and the Caribbean, Central and Eastern Europe and the Middle East and Africa.

Fortunately, the major ATM manufacturers and outsourcing vendors in the U.S. have successfully managed EMV migrations in the other markets around the globe. For instance, Diebold has manufactured EMV-compliant ATMs since the launch of its Opteva ATMs in 2002. Diebold was the first ATM manufacturer to join the Visa EU Smart Partner Program in 2002 to encourage migration to EMV in Europe.

NCR Inc. has shipped EMV-compliant motorized card readers in SelfServ ATMs since 2010. Smart Dip Card readers have

been compliant since the introduction of SelfServ in 2008. Both companies offer upgrade kits for ATMs that meet software and hardware requirements.

Also, ATMGurus, the Long Beach, Miss., subsidiary of Triton Systems of Delaware LLC, offers upgrade kits for popular Triton ATM models that include an approved card reader, key pad and other hardware to allow an installed model to meet both EMV and PCI Security Standards Council regulations with one upgrade. Similar kits are available for units from Nautilus Hyosung, Diebold, NCR and other manufacturers.

Managing the transition to EMV

To fully implement EMV, the three main constituents of the payment system — the cards, the electronic funds transfer terminals and the systems — must be upgraded to permit EMV transactions. Also, national bodies, such as Interac in Canada, may promulgate specific requirements for each market.

ATM deployers are faced with two choices: They can either attempt to coordinate the transition to EMV on their own or hire a trusted partner to orchestrate the process. If they choose to outsource, that single point of contact streamlines all of the ATM services and simplifies portfolio management.

"Senior management at most FIs prefer their internal resources stay focused on business issues, as they recognize information technology processing can be entrusted to outsourcing companies with proven expertise," said Robert Hunt, senior research director at CEB TowerGroup, a Boston-based research firm. "Deploying innovative products managed by a dedicated, performance-oriented service partner can be an appealing option, in part because outsourced processing enables banks of all sizes to concentrate more fully on delivering popular services and an outstanding customer experience."

Research firm Aite Group estimated that it costs about $2,000-$4,000 to upgrade an ATM to be EMV capable. While ATM owners in particular may be dismayed by the cost of upgrading a large fleet, the only alternative is accepting the fraud liability.

With deadlines looming, ATM deployers don't have much time to plan and implement necessary upgrades. By contrast, it took Europe five years to move from 52 percent EMV compliance to 97 percent, according to Lachlan Gunn, coordinator of the European ATM Security Team.

"The European experience indicates that those that do not succeed in meeting the deadline will be heavily penalized as fraud migrates to their machines (compliant ATMs will not dispense cash if counterfeit EMV cards are used), and demands start arriving from EMV card issuers for loss reimbursement," Gunn wrote in his blog on ATMmarketplace.com

Conclusion

The transition to EMV-based chip cards can be an important component of a comprehensive security program to combat fraud for regional FIs. Experts in the industry recommend planning an upgrade strategy as soon as possible. NCR, Triton and other manufacturers caution that waiting until the last minute before the deadline could lead to shortages of upgrade parts and technicians capable of installing them, as well as potential issues with processing networks.

To implement such massive changes as deadlines loom, regional FIs could benefit from working with experienced providers that have been through the process in other countries. Major manufacturers such as NCR and Diebold have already been through the experience with FIs in other countries that have already adopted EMV. For instance, NCR has implemented its EMV-compliant software on more the 250,000 ATMs worldwide.

About the sponsor: *Red Hawk Fire & Security is an industry leader with more than 1,400 employees and 50,000 clients across the country. Relentlessly dedicated to helping protect businesses from the risks they face every day, Red Hawk's comprehensive portfolio of life safety and security offerings employs cutting-edge technologies and advanced systems integration to create flexible solutions for companies of all sizes. The Red Hawk team of industry experts brings an unmatched breadth of expertise and years of hands-on experience to every solution. The company serves clients in banking and financial services, retail, education, health care and manufacturing and is headquartered in Boca Raton, Fla.*