

Best Practices for EMV Migration

Deadlines are looming for U.S. migration to the EMV (Europay, MasterCard and Visa) payment card security standard, and ATM deployers need to start their planning and implementation process now.

SPONSORED BY:



By Robin Arnfield
ATMmarketplace.com



“The sooner ATM operators start developing EMV migration plans with their vendors and suppliers, the more likely their EMV migration will be completed in a smooth and timely manner.”

— Jim Outland, president of Paragon Data Services

EMV is designed to combat card skimming and counterfeiting; EMV-compliant cards contain an embedded chip as well as a magnetic stripe. The chip contains data needed to use the card for payment transactions, but it is protected by several security technologies that prevent counterfeiting.

Deadlines

The U.S. is one of the last countries to migrate to EMV. Most European, Latin American and Asian countries have migrated already or are in the process of doing so.

As part of their EMV migration roadmaps, Visa and MasterCard have established deadlines for counterfeit card fraud liability shifts for U.S. ATM acquirers. In October 2016, MasterCard will shift counterfeit card fraud liability to ATM acquirers that don't accept MasterCard-branded EMV cards at U.S. ATMs. Visa will shift counterfeit card fraud liability to ATM acquirers in October 2017.

Once those deadlines have passed, if an EMV card is used fraudulently at an ATM that doesn't support EMV, the acquirer will be liable for the issuer's fraud losses. The acquirer will pass on the cost of this fraud to the owner of the noncompliant ATM.

“Recent data breaches at high-profile retailers mean the dates for EMV implementation and the liability shift to acquirers are ‘cast in stone,’” said Jim Outland, president of U.S. consultancy Paragon Data Services.

Migrating an ATM network to EMV involves three processes. First, ATMs must have EMV Level 1-compliant card readers and PCI-compliant encrypting PIN pads. As defined by EMV standardization body EMVCo, EMV Level 1 is the standard for the hardware interface enabling data transfer between EMV cards and terminals.

Second, an EMV Level 2-compliant software kernel must be added to the ATM's application software. EMV Level 2 is the standard for the application software resident in the terminal that processes EMV transactions.



Third, the acquirer’s ATM network must undergo end-to-end EMV hardware and software testing to receive EMV Level 3 certification from the card networks whose cards the acquirer wants to accept. EMV Level 3 is the standard for the entire EMV infrastructure, encompassing the terminal hardware, software and network.

Start planning now

“[EMV Migration Guide](#),” an ATM industry report published by ATM Marketplace, recommends that ATM operators start planning their migration to EMV now, because leaving it to the last minute could be a costly mistake.

ATM vendors likely will not have the resources to assist large numbers of clients trying to migrate to EMV very close to the deadline, the report says. For example, there might be shortages of EMV card readers and resources for EMV testing and certification as the deadline approaches.

According to Tom Driscoll, solutions manager at NCR, the process of migrating to EMV can take 12 to 16 months.

“Don’t put EMV migration on the backburner, as those who lag behind are the ones who will be hardest hit by potentially absorbing the enormous costs of fraud,” Driscoll wrote in an [NCR blog](#). “Waiting could also hinder your brand reputation if your customers are fraud victims simply because you haven’t migrated to EMV.”

Planning

“EMV requires ATM hardware, software and operational changes that must be planned, scheduled, implemented, tested and certified,” Outland said. “Also, not all a deployer’s ATMs may be capable of being upgraded to support EMV, and will have to be replaced.”

As part of their EMV preparations, ATM deployers need to educate themselves about EMV technology and implementation options, assess their current infrastructure and determine appropriate changes. They then need to develop a project plan.

“The first step is to ensure that the technology and business stakeholders in your company gain a deep understanding of EMV, so that the planners can anticipate and cater for all key areas of changes,” said Frederique Slevin, principal product manager of retail payments at ACI Worldwide. “A lot of training material and webinars have been produced by industry stakeholders about U.S. EMV migration that can be leveraged. ATM owners should work directly with their ATM hardware supplier or ATM driving/acquiring host

EMV deadlines

On April 19, 2013, counterfeit card fraud liability shifted to U.S. ATM acquirers that do not accept EMV chip cards for Maestro debit card interregional transactions.

As of April 2015, all U.S. ATM third-party acquirers/processors and subprocessors must be able to support EMV chip data.

As of October 2015, counterfeit card fraud liability for both MasterCard and Visa will shift to U.S. acquirers that do not accept EMV cards at U.S. POS terminals.

In October 2016, counterfeit card fraud liability will shift to ATM acquirers that do not accept MasterCard-branded EMV cards at U.S. ATMs.

As of October 2017, counterfeit card fraud liability will shift to ATM acquirers that do not accept Visa-branded EMV cards at U.S. ATMs.



vendors to gain specific information about each of these impacted areas. The EMV Migration Forum, a subchapter of the Smart Card Alliance which specifically addresses the topic of U.S. EMV migration, should be a key resource for your planning.”

Debit cards

As part of their EMV education, ATM deployers need to keep up to date with technical developments relating to the establishment of a common solution for routing U.S. EMV debit card transactions.

An EMV card’s chip contains an application identifier that tells the acquirer which network to use to route a transaction.

As it was developed originally in Europe, where countries typically have a single debit network, the EMV specification does not allow EMV cards to give merchants a choice of debit network. However, the Durbin Amendment requires U.S. debit issuers to link their cards to two unaffiliated debit networks, giving merchants the ability to choose where to route transactions.

Visa and MasterCard have been licensing their rival common EMV debit AID solutions to the U.S. debit networks. The EMV Migration Forum is working on a common debit AID framework that would be accepted by Visa and MasterCard, as well as by all the U.S. debit networks. Using this framework, an acquirer would check the AID against its database to determine which debit network the merchant wants to use for transaction routing.

ATM vendors already are shipping ATMs with EMV-capable card readers and software in the U.S. Once a common debit AID framework is agreed to by the networks, these card readers will need to be field-upgraded with new software.

Shaun King, Triton Systems vice president of international sales, says ATM deployers should not postpone deploying EMV card readers until a common debit AID solution is finalized.

Evaluation

According to a blog post by Daryl Cornell, Triton president and CEO, on the company’s [ATMatom website](#), ISOs must carry out an evaluation of their ATM fleet.

“Which ATMs can be upgraded through installation of an [EMV conversion kit](#)?” Cornell wrote. “Which ATMs can be [refurbished by manufacturers and upgraded for EMV](#)? Which ATMs can be traded to the manufacturer for [credit against the purchase of new gear](#)? Which ATMs need to be culled



“Knowing what your processor’s EMV migration strategy is and when it plans to upgrade its switches to EMV will be critical.”

— Daryl Cornell, president and CEO of Triton Systems

based on lackluster performance and age? How many kits and ATMs will I need, and over what timeframe do I need to budget this expense?”

Once the ISO has performed this asset-management exercise, it can make educated decisions about timing and rollout, Cornell said.

“Ensure your project schedule allows time for budget approval, and for ordering and installing new parts or devices,” says the ATM Marketplace white paper, “EMV Implementation for Acquirers,” by payments software testing firm [Paragon Application Systems](#).

Communications protocol

In its white paper “Modifying Your ATM to Support EMV,” Paragon Application Systems says ATM deployers need to review their current communications protocol. “Some older protocols cannot handle the longer EMV messages,” it says. “You might want to use this opportunity to upgrade to TCP/IP, which isn’t required for EMV, but does facilitate other functions at the ATM.”

Processors

According to Cornell, it is vital for deployers to communicate with their processors as part of their EMV preparations.

“Talk to your processor,” Cornell recommends in his blog. “Find out how your processor plans to handle EMV conversion. When do they plan to upgrade their switches to support EMV? When will they be ready to begin supporting EMV transactions? Does your processor expect ISOs to pay for fraud claims from issuers? Will your processor be turning off high-risk terminals in advance of liability shift deadlines? How will your processor treat non-EMV terminals after the liability shift?”

Cornell recommends that ISOs talk to their internal and external field service providers to see if they plan to add field service technicians to accommodate EMV upgrades and replacements. He says ISOs should ask their vendors the following questions: “What will ATM lead times swell to as we approach liability shift? What are upgrade kit lead times? Which ATM models are upgradeable? What are trade values for certain makes and models? Can I get discounts for early purchases of kits and ATMs?”

Paragon Application Systems says ATM deployers must obtain written confirmation from their hardware vendors that they have passed EMVCo Level 1 and Level 2 certification for each combination of make, model and EMV software kernel their ATMs will be using.



About the sponsor:

Since 1997, National Cash Systems has established many successful relationships with thousands of merchants nationwide. The company's successful track record in providing clients with turnkey ATM and comprehensive payment solutions has earned it a reputation for delivering quality products while exhibiting financial stability and expertise. For more information, visit www.nationalcash.com.

Windows 7

On April 8, 2014, Microsoft ceased to provide updates for Windows XP. This means that ATMs that haven't migrated to Windows 7 will not receive Microsoft security patches. They will face greater risks from malware and network intrusions and will be in breach of the Payment Card Industry Data Security Standard, which requires ATM deployers to keep their operating systems updated with security patches that protect against known vulnerabilities.

ATM deployers who still are running XP should consider running their EMV and Windows 7 migration projects in tandem to achieve operational efficiencies and cost savings. Also, they are unlikely to receive certification from their processor for their EMV kernel software if they still are running XP.

Dip card readers

As ATMs in the U.S. commonly incorporate dip card readers, ATM owners will need to decide whether to replace their mag-stripe dip card readers with EMV-compliant dip card readers or with EMV motorized readers.

Diebold recommends EMV motorized readers for full-service ATMs where customers carry out a variety of transactions, as they will provide a better customer experience than dip card readers, said Jim Pettitt, Diebold senior director of advanced solutions product management.

However, replacing a mag-stripe dip card reader with an EMV motorized card reader might mean changing the ATM's fascia.

Since U.S. cardholders are used to swiping mag-stripe cards quickly through ATM dip card readers, they will need to be informed about leaving the EMV card in the reader until it has read and written to the chip. U.S. ATM deployers should provide directions on their ATM screens explaining how to use EMV dip card readers. A notice attached to the ATM fascia also might be advisable.