atm marketplace

WHITE PAPER

Upgrade to EMV before your ATMs become a fraud target

By Robin Arnfield | Contributing writer, ATM Marketplace

Upgrade to EMV before your ATMs become a fraud target

By Robin Arnfield | Contributing writer, ATM Marketplace

SPONSORED BY:

National Cash systems

ATM deployers who haven't upgraded their ATMs to EMV by MasterCard's October 2016 deadline, risk becoming liable for card issuers' fraud losses at their terminals and could be disconnected from their processor's network.

"By October 2016, any ATM deployers who aren't EMV-ready could face much higher costs," says Judi Suzuki, president of Irvine, California-based National Cash Systems. "The cost of the fraud will fall back on the ATM deployer, so avoid liability costs and don't become another target when we already have the solution. Staying ahead of the game by being EMV-compliant will be more beneficial and cost-effective for ATM deployers and customers at the end of the day."

MasterCard's October 2016 liability shift for ATMs will be here very soon. Make sure your ATMs are EMV-compliant before you become a target for criminals and potentially become liable for card fraud losses. Also, your acquirer may disconnect your ATMs if they aren't EMV-compliant by the deadline.

“By October 2016, any ATM deployers who aren’t EMV-ready could face much higher costs. The cost of the fraud will fall back on the ATM deployer, so avoid liability costs and don’t become another target when we already have the solution. Staying ahead of the game by being EMV-compliant will be more beneficial and cost-effective for ATM deployers and customers at the end of the day.”

— Judi Suzuki, president of Irvine, California-based National Cash Systems.

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.

The U.S. has been forced to embark on EMV migration because card fraud has been moving to the U.S. from European countries that have already rolled out EMV technology. As the vast majority of U.S. ATMs can only accept mag-stripe cards, criminals have been making mag-stripe clones of European EMV cards and using them in the U.S.

Another reason for EMV migration is the fact that criminals have been targeting U.S. ATMs, particularly non-bank ATMs, with fraud attacks such as card skimming.

Rising U.S. ATM fraud

According to statistics published by analytic software firm FICO, the number of U.S. ATMs compromised by criminals rose 546 percent from 2014 to 2015. FICO said that figures for 2015 were the highest ever recorded by its FICO Card Alert Service, which monitors hundreds of thousands of ATMs in the U.S.

Non-bank ATMs accounted for 60 percent of all compromises, up from 39 percent in 2014. Convenience stores were especially hard-hit, with compromises up ten-fold year over year, FICO said.

T.J. Horan, FICO’s VP of fraud solutions, said that criminals are targeting non-bank ATMs, which are more vulnerable than FI-owned ATMs. He said ATM operators should increase the frequency of their inspections, looking carefully for any signs of tampering.

Although the chip on an EMV card can't be cloned, EMV cards will remain vulnerable to skimming as long as they contain mag-stripes. So, as part of their EMV migration, ATM deployers need to install EMV-compliant card readers that contain anti-skimming technology.

According to an atmAToM.com blog by Darryl Cornell, president and CEO of Long Beach, Mississippi-based ATM vendor Triton Systems, retail ATM owners need to prioritize investment in anti-skimming card readers and EMV upgrades. Otherwise, the recent surge in fraud means retail ATM owners risk seeing a damaging erosion in consumer confidence in the security of their terminals.

"Customers are becoming increasingly aware of the value that a secure transaction holds," says Suzuki. "Sophisticated customers will try to avoid the less secure mag-stripe swipe method for using their card whenever possible and will prefer EMV transactions."

Canada proves EMV cuts ATM fraud

Canada completed its migration of credit and debit cards, POS terminals and ATMs by 2012.

Cornell wrote in an atmAToM.com blog that Canada saw positive results from its migration to EMV. Citing statistics from Interac, Canada's domestic debit card scheme, he wrote that Canadian domestic debit fraud at ATMs averaged nearly C$2,400 ($1,912) per terminal in 2009.

"By 2014, two years after Canada's migration to EMV, that figure had been slashed to a mere C$33 ($26) per terminal," Cornell wrote. "An interesting aside is that all non-EMV ATMs were turned off by Interac in December 2012 — a reduction of nearly 1,000 terminals."

Deadlines

As part of their EMV migration roadmaps, Visa and MasterCard have established deadlines for counterfeit card fraud liability shifts for U.S. ATM acquirers.

On October 1, 2016, counterfeit card fraud liability will shift to U.S. ATM acquirers whose ATMs have not been migrated to EMV and are unable to accept MasterCard-branded EMV cards.

From October 1, 2017, counterfeit card fraud liability will shift to ATM acquirers that don't accept Visa-branded EMV cards at U.S. ATMs.

Once MasterCard's and Visa's 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 non-EMV-compliant ATM.

Risk of disconnection

According to an atmAToM.com blog by Cornell, non-EMV-compliant U.S. retail ATMs could be shut off in large numbers by the end of 2016.

"While bank- and large ISO-owned ATMs will be largely EMV-ready by October (2016), smaller ISO- and merchant-owned ATMs will not," Cornell wrote. "This means that as many as half of all U.S. ATMs will be 'mag-stripe only' at the October MasterCard liability shift deadline. Unlike POS devices, ATMs are prime targets for fraudsters. Using fistfuls of cloned mag stripe cards, international crime rings will easily exploit non-EMV ATMs as fraud bypasses EMV ATMs. Liability shift chargebacks will quickly reach the six-figure levels we saw in Canada (after its EMV migration deadline) by year-end.

"Presumably, sponsor banks are already busy evaluating the ability of ATM-owning ISOs and merchants in their own networks to absorb these levels of financial losses. Those who elect not to upgrade and who cannot absorb the projected financial losses will, as we saw in Canada (after its EMV migration deadline), simply be turned off. Many of these ATMs will be subsequently upgraded or replaced, others will not. In the interim, expect a significant contraction in active U.S. ATMs in late 2016."

U.S. EMV deadlines

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

From April 2015, all U.S. ATM third-party acquirers/processors and sub-processors must be able to support EMV chip data, Visa says.

From October 2015, counterfeit card fraud liability shifted to U.S. acquirers that don't accept EMV cards at U.S. POS terminals, according to MasterCard and Visa.

MasterCard said in March 2016 that 67 percent of U.S.-issued MasterCard-branded consumer credit cards feature chips and that consumers can use their chip cards at 1.2 million U.S. merchant locations whose POS terminals are EMV-enabled.

On October 1, 2016, counterfeit card fraud liability will shift to ATM acquirers that don't accept MasterCard-branded EMV cards at U.S. ATMs.

From October 1, 2017, counterfeit card fraud liability will shift to ATM acquirers that don't accept Visa-branded EMV cards at U.S. ATMs.

From October 2017, U.S. automated fuel dispensers must be EMV-compliant.

EMV migration

Migrating an ATM network to EMV involves three processes.

Firstly, ATMs must contain EMVCo-approved Level 1-compliant EMV 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.

Secondly, an EMVCo-approved EMV Level 2-compliant software kernel must be added to the ATM's application software provided by the ATM vendor.

EMV Level 2 is the standard for the application software resident in the terminal which processes EMV transactions.

Thirdly, 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.

After installing EMV card readers and EMV kernel software, individual ATM deployers must carry out testing and certification with their processor.

More information on EMV migration can be found in the ATM Marketplace guide "EMV at the ATM: The race to compliance."

Mag-stripe versus EMV

Magnetic Stripe Transaction	EMV Transaction
Card is swiped, inserted, or dipped, and is returned to cardholder after magnetic stripe data has been read	Card must be inserted and remain in the terminal for the duration of the transaction
There is no interaction between card and terminal after magnetic stripe has been read	Data is exchanged between card and terminal to initiate the transaction
Card does not generate a cryptogram	Chip card generates a unique cryptogram which is sent to the host for verification
Online request message contains no EMV-specific data	Online request message contains additional EMV-specific data
Host does not perform any EMV-related processing	Additional processing is required by host to verify request cryptogram, generate response cryptogram, and interrogate additional EMV-specific fields in the request message
Online response message contains no EMV-specific data	Online response message contains additional EMV-specific data
There is no interaction between card and terminal at the end of the transaction	Data is exchanged between card and terminal at the end of the transaction

"Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community" by the EMV Migration Forum and Smart Card Alliance, 2015.

Recommendations

"While the odds of any single terminal being hit by a fraudster are rather low, as soon as a terminal is identified as non-EMV compliant, it will become a repeated target until the merchant upgrades," says Suzuki. "Any funds withdrawn via a fraudulent card at a non-EMV terminal merchants should consider an immediate loss, in addition to fines by the card networks for having to investigate the cardholder's inevitable claim. Merchants need to weigh the fixed cost of upgrading versus the variable cost that comes with potential fraud."

ATM deployers need to perform an inventory of their fleet to determine which ATMs can be upgraded to EMV, and which cannot so will have to be replaced, notes the EMV Migration Forum whitepaper "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community."

In an ATM Marketplace article, *Randy Vanderhoof, the EMV Migration Forum's director, made the following recommendations:*

- Work closely with your payment network representatives and make sure you understand the EMV requirements of the individual payment networks;
- Work closely with ATM vendors, and solicit their input and recommendations. Be aware of each vendor's plans and roadmaps, upgrades, re-certifications and other updates;
- If working with a processor, be aware of their EMV-readiness. This includes both testing and certification of the processor's platform and end-to-end testing to ensure compatibility between the processor and each make and model of ATM;
- Allow extra time for all tasks that involve external vendors. A delay is likely to have a domino effect because so many external entities (such as vendors and payment networks) are involved;
- If you wait to certify, you will undoubtedly find yourself in a queue with others who are also trying to certify. This may cause significant delays in getting EMV-compliant ATMs into production;
- Though it might be tempting to make further changes such as software upgrades, attempting multiple changes simultaneously could prove to be unmanageable. Focusing only on EMV will allow for a more efficient and effective migration.

About the sponsor:

Since 1997, Irvine, California-based National Cash Systems has established many successful relationships with thousands of merchants nationwide and helped them fulfill their customized business ATM needs. The company's successful track record in providing clients with turnkey ATM and comprehensive payment solutions has earned it a reputation for delivering top-quality ATM equipment while exhibiting financial stability and expertise. For more information, visit www.nationalcash.com